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

D8.1

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: 31/05/2021
Actual submission date: 31/05/2021

31/05/2021

Version 1.3

Responsible partner: CEA
Editor: Thanh-Hai Nguyen
E-mail address: thanhhai.nguyen@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: Thanh-Hai Nguyen (CEA), Stefano Sebastio, Shane Daly, Amine Lamine (UTRC), C. Plappert (FhG), Gianpiero Costantino (CNR)

Approved by: Thanh-Hai Nguyen (CEA), Ruisong Han (WIT)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	16-Feb-2021	T.-H. Nguyen, S. Sebastio	CEA, UTRC	Initial table of content
0.2	22-Mar-2021	C. Plappert	FhG	First draft of Task 8.5
0.3	06-Apr-2021	G. Costantino	CNR	Integration of CNR contribution
0.4	08-Apr-2021	T.H Nguyen	CEA	Integration of FHE technology
0.5	09-Apr-2021	T.H Nguyen	CEA	Integration of UTRC contribution
0.6	12-Apr-2021	T.H Nguyen	CEA	Integration of FhG contribution
0.7	14-Apr-2021	T.H Nguyen	CEA	Update UTRC contribution FhG contribution
0.8	15-Apr-2021	T.H Nguyen	CEA	Update FhG contribution & CEA contribution
0.9	29-Apr-2021	S. Daly, S. Sebastio	UTRC	Contribution to Task 8.2
1.0	29-Apr-2021	A. Lamine	UTRC / CNR	Contribution to T8.1
1.1	09-May-2021	T.H Nguyen	CEA	Merge
1.2	12-May-2021	T.H Nguyen	CEA	Integration component designs & validation
1.3	29-May-21	T.H Nguyen	CEA	Internal review

Executive Summary

This deliverable is the first output of Work Package 8, "Advanced Security Services Requirements and Architecture" due at M12 and its main aim is to report the requirements of the components of the E-CORRIDOR Framework reference architecture (defined in D5.1 and, for the convenience of the readers, reported in Section 2) that will be developed in WP8 by leveraging on the tools and technologies that are provided by the E-CORRIDOR partners. Hence, this deliverable reports a description of each of the provided technologies and tools, specifying the state of the art, the current status and whether they have been developed within a previous EU project. Another important contribution of this deliverable is that it also specifies which of the security components of the E-CORRIDOR Framework reference architecture can exploit the tools provided by the E-CORRIDOR partners for its implementation. In addition, this deliverable specifies the requirement of these components. It starts from the general requirements that have been defined in D5.1, and it specifies which of them relates to each of the components provided by the E-CORRIDOR partners. Finally, for each of these requirements, this deliverable specifies which is already satisfied by the current version of the tool and which, instead, is partially or not satisfied at all, thus requiring a maturation of the component in order to be adopted to implement the E-CORRIDOR Framework.

Table of contents

Executive Summary 3
1. Advanced Security Services 6
1.1. Advanced Security Services Architecture Overview 6
2. Privacy Aware Seamless Multimodal Authentication – Task 8.1 10
2.1 Multi-Biometric and Multi-Factor Authentications 10
2.1.1 State of the Art 10
2.1.2 Proposed Approach/Technology 11
2.1.3 Data Format Requirement 12
2.1.4 Platform Requirements 12
2.1.5 Application to Pilots 12
2.1.6 Potential Synergies with Other Components 13
3. Continuous Behavioral Authentication – Task 8.2 14
3.1 Federated authentication based on eIDAS 14
3.1.1 State of the Art 14
3.1.2 Proposed Approach/Technology 15
3.1.3 Data Format Requirement 18
3.1.4 Platform Requirements 18
3.1.5 Application to Pilots 19
3.1.6 Potential Synergies with Other Components 19
4. Privacy Aware Interest-Based Service Sharing – Task 8.3 20
4.1 State of the Art 20
4.1.1 Two-Party Computation (2PC) 20
4.1.2 Fully homomorphic encryption based service sharing 20
4.2 Proposed Approach/Technology 21
4.2.1 Two-Party Computation (2PC) 21
4.2.2 Fully homomorphic encryption based data sharing service 22
4.2.3 Data Format Requirement 23
4.2.4 Platform Requirements 23
4.2.5 Application to Pilots 24
4.2.6 Potential Synergies with Other Components 24
5. Privacy Aware Authorization – Task 8.4 26
5.1 Federated model for attribute based encryption 26
5.1.1 State of the Art 26
5.1.2 Proposed Approach/Technology 26
5.1.3 Data Format Requirement 27
5.1.4 Platform Requirements 27

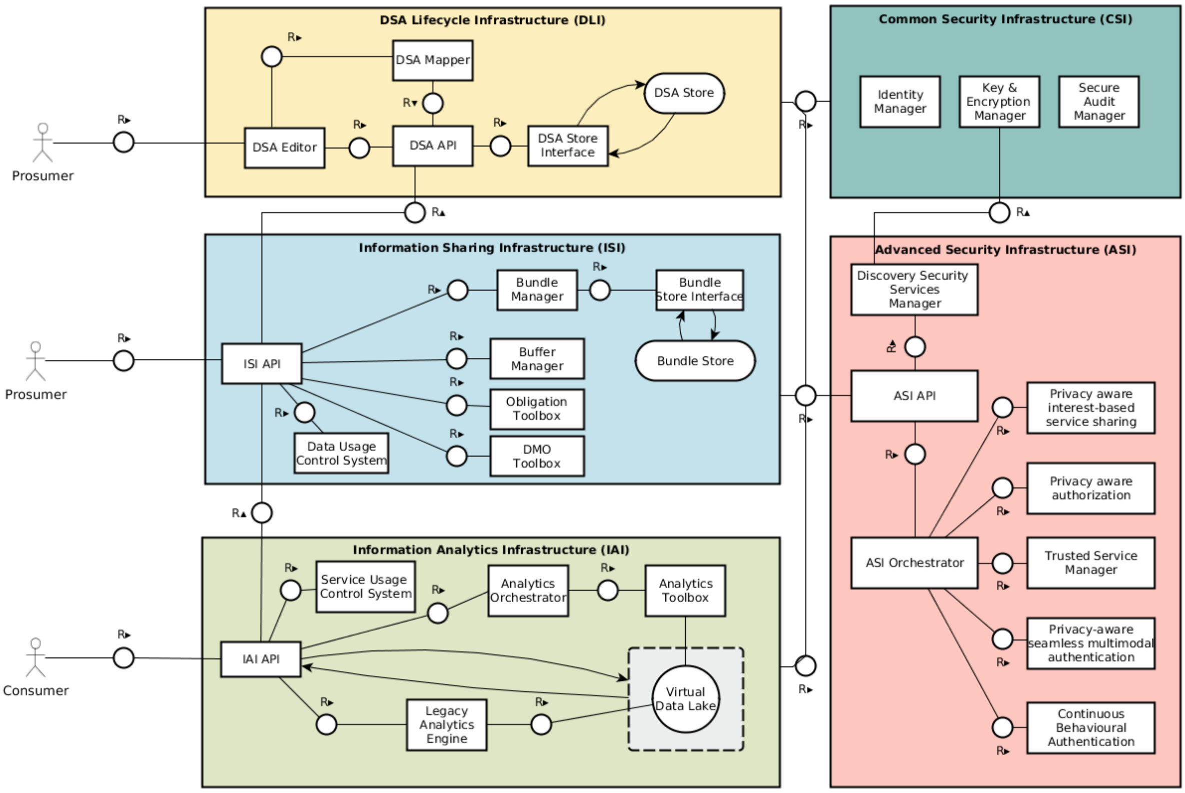
5.1.5 Application to Pilots 27
5.1.6 Potential Synergies with Other Components 27
6. Secure Identity Management / Trusted Identity Manager – Task 8.5 28
6.1 Trusted Identity Provider (TrIP) 28
6.1.1 State of the Art 28
6.1.2 Proposed Approach\Technology 29
6.1.3 Expected Data Format 33
6.1.4 Platform Requirements 33
6.1.5 Application to Pilots 34
6.1.6 Potential Synergies with Other Components 35
7. Conclusions 36
Reference 37
A. Appendix 40
A.1 Definitions and Abbreviations 40

1. Advanced Security Services

This deliverable is the first output of Work Package 8, “Advanced Security Services Requirements and Architecture” due at M12 and its main aim is to report the requirements of the components of the E-CORRIDOR Framework reference architecture (defined in D5.1 and, for the convenience of the readers, reported in Section 2) that will be developed in WP8 by leveraging on the tools and technologies that are provided by the E-CORRIDOR partners. Hence, this deliverable reports a description of each of the provided technologies and tools, specifying the current Technology Readiness Level (TRL) and whether they have been developed within a previous EU project. Another important contribution of this deliverable is that it also specifies which of the security components of the E-CORRIDOR Framework reference architecture can exploit the tools provided by the E-CORRIDOR partners for its implementation. In addition, this deliverable specifies the requirement of these components. It starts from the general requirements that have been defined in D5.1, and it specifies which of them relates to each of the components provided by the E-CORRIDOR partners. Finally, for each of these requirements, this deliverable specifies which is already satisfied by the current version of the tool and which, instead, is partially or not satisfied at all, thus requiring a maturation of the component in order to be adopted to implement the E-CORRIDOR Framework.

1.1. Advanced Security Services Architecture Overview

This section briefly recalls the high-level E-CORRIDOR Framework reference architecture (shown in Figure 1) that has been defined at Month 12. The main aim of this section is to give a quick overview of the main components of the architecture and a brief description of their main functionalities. A very detailed description of the components of the architecture, of their functionalities, of their interactions, and of the workflow of the main operations of the E-CORRIDOR Framework can be found in D5.1. The main aim of recalling the E-CORRIDOR



DSA Lifecycle Infrastructure (DLI)
DSA Mapper
DSA Store
DSA Editor
DSA API
DSA Store Interface
Prosumer
Common Security Infrastructure (CSI)
Identity Manager
Key & Encryption Manager
Secure Audit Manager
Information Sharing Infrastructure (ISI)
Bundle Manager
Bundle Store Interface
Bundle Store
Buffer Manager
ISI API
Obligation Toolbox
Data Usage Control System
DMO Toolbox
Prosumer
Advanced Security Infrastructure (ASI)
Discovery Security Services Manager
ASI API
Privacy aware interest-based service sharing
Privacy aware authorization
ASI Orchestrator
Trusted Service Manager
Privacy-aware seamless multimodal authentication
Continuous Behavioural Authentication
Information Analytics Infrastructure (IAI)
Service Usage Control System
Analytics Orchestrator
Analytics Toolbox
IAI API
Virtual Data Lake
Legacy Analytics Engine
Consumer

Figure 1: E-CORRIDOR architecture overview

Framework reference architecture here is that in the following, we describe each of the tools that are being provided by the E-CORRIDOR partners, and for each of them, this document specifies which of the components shown in Figure 1 can benefit of such tool.

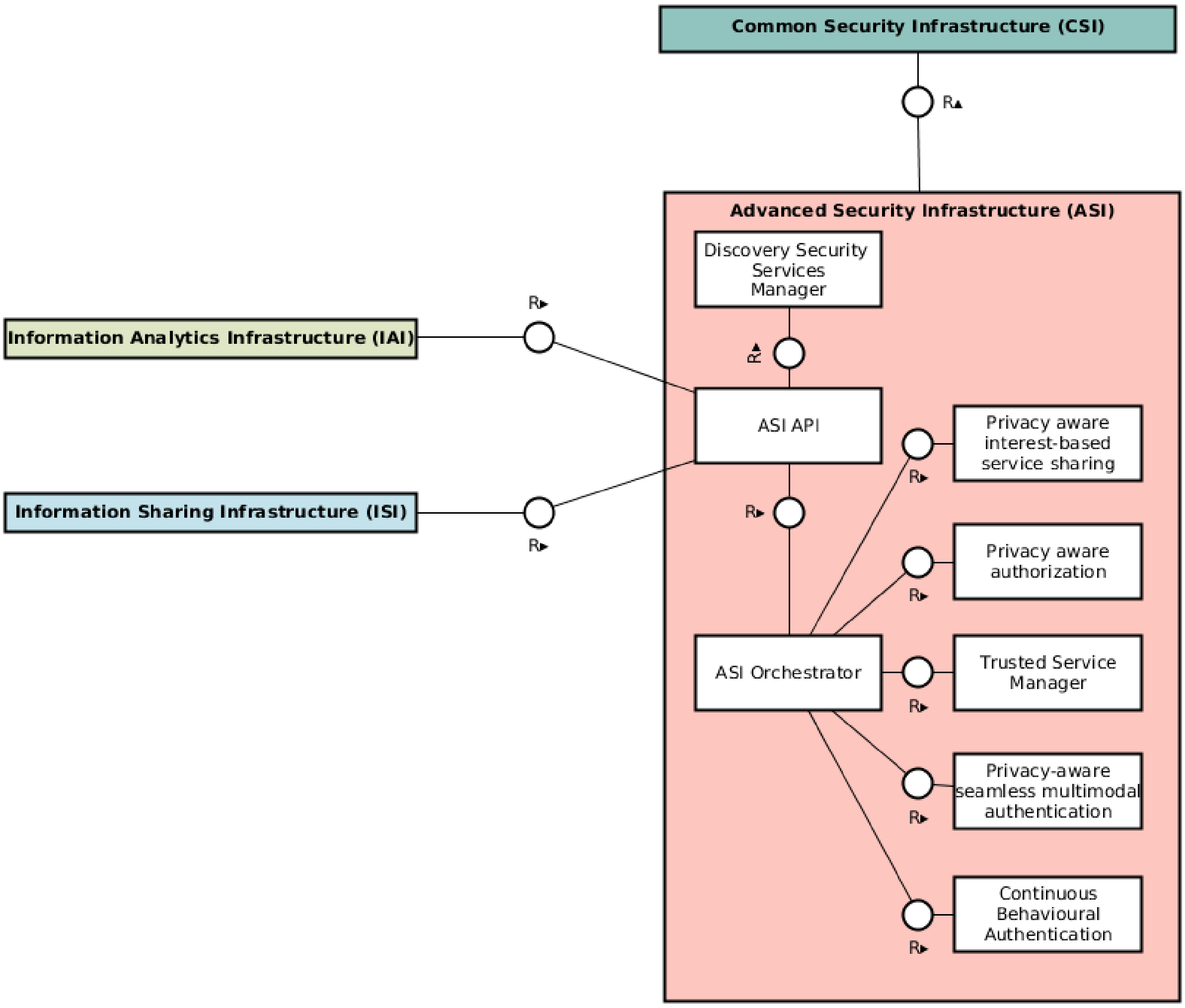

Common Security Infrastructure (CSI)
R
Advanced Security Infrastructure (ASI)
Discovery Security Services Manager
R
Information Analytics Infrastructure (IAI)
R
ASI API
Privacy aware interest-based service sharing
R
Information Sharing Infrastructure (ISI)
R
R
Privacy aware authorization
R
ASI Orchestrator
Trusted Service Manager
R
Privacy-aware seamless multimodal authentication
R
Continuous Behavioural Authentication
R

Figure 2: Security Infrastructure Architecture Overview

As shown in Figure 2, the E-CORRIDOR Advanced Security Service architecture is composed of the following main subsystems:

Discovery Security Service Manager: This component proposes a discovery service which is responsible for detecting whether **a security service** is on or off status. The information about RESTfull connection endpoint this service can collect facilitate **ASI (Advanced Security Infrastructure) Orchestrator** service to interact with available security services hosted in ASI. **ASI API** is an exposed OpenAPI which allows other Infrastructure or components in E-CORRIDOR Framework to invoke.

Regarding to Advanced Security Services, E-CORRIDOR partners proposes the following services:

Privacy aware seamless multimodal authentication: This component proposes a privacy aware Multi Factor Authentication (MFA) scheme that is designed to scale quickly in the multi-modal transport pilot's system by applying adaptive device and user context into the system. Legacy authentication mechanisms such as hardware tokens, PIN/passwords, voice biometrics, behavioral biometrics, and other wearable authentication approaches such as data from smart watches will be leveraged to build an MFA system, which exploits thus both Biometric and Behavioral Authentication. From multi-modal transport perspective, the dynamic access policies around particular transport use-case like airport (passport or E-passport), car-sharing (driving license validity) and other user-centric attributes like role, location, and device information will be identified. Once risky behavior is detected, the system can enforce those policies automatically with step-up authorization or access denial, protecting identity and access to data. To enable privacy in seamless authentication systems, this component leverage Multi Party Computation (MPC) that is used for security reasons against typical privacy adversarial models, offering various security levels, from computation to perfect security. In addition, we incorporate Fully Homomorphic Encryption (FHE) and the paradigm of using of FHE – based analytics in heterogeneous cloud infrastructure with FHE-friendly APIs analysis programming for the main purpose: efficient execution with further easy evaluations in the encrypted domain.

Considering the airport pilot's scenario, this component develops a context-aware multi-factor authentication mechanism that assures the security and privacy preserving of passenger information, while facilitating the seamless flow of passenger journey with the help of Single Token technologies.

Continuous behavioural authentication: This component proposes a privacy aware continuous behavioural authentication system and develops a behavioural ID/profile which will be unique to each transport entity and defined through behavioural fingerprinting such as data collected from accelerometers and gyroscopes for action recognition, voice and video analysis and the original ID type of information using machine learning and deep learning approaches. Specifically, behavioural ID constructed by capturing the state, context of transport entities with a spatio-temporal fingerprinting methodology. The system gains knowledge over the time of the golden communication channel between transport entities. Moreover, we adopt an adaptive risk-based model that applies device and user context through an adaptive approach and performs continuous authentication of a user based on behavioral ID/profile under different devices and different environments. This component also address to eWallet Sharing token authentication problem for both user and device pattern to authenticate a right transaction and prevent to any fraud money attempt.

Privacy aware interest-based service sharing: This component aims to provide a privacy-aware protocol and framework of data sharing that allow stakeholders having a common service interest to share their client data with respect to data privacy constraints. These constraints will be clearly defined in Data Sharing Agreement, which is established between them, fully and transparently controllable in data exploitation and analysis. Privacy-preserving data mining techniques based on homomorphic encryption and anonymization technologies will be applied to ensure the respect of these data sharing constraints. 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. It's a nice solution for supporting the development of cross-border pan-European multimodal transport.

Privacy aware authorization: This component will lead to the definition of the functional methodology for privacy aware authorization. The system will be based on the attributed-based encryption federated model and will interact with this framework, to provide a holistic solution for security provisioning. This component will result in a layered modular structure, accommodating the various functional blocks aimed at implementing the required functionalities and respecting privacy by design rules. Furthermore, 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: This component aims to develop a secure identity management system for both eWallet Sharing and continuous authentication token checking for both passenger and baggage. This 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. 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.

2. Privacy Aware Seamless Multimodal Authentication – Task 8.1

This task aims at performing a privacy-aware multi-factor authentication (MFA) by exploiting multi-biometric, behavioral, location and contextual information of the user (either driver or passenger). The MFA provided by the E-CORRIDOR core framework will allow a context-aware authentication able to assure privacy (through a token-based system) while enhancing the security of the authentication mechanism itself. The latter goal is achieved thanks to the use of multiple sources of information to identify and authenticate the users.

2.1 Multi-Biometric and Multi-Factor Authentications

The problem of person detection, monitoring and localization has been at the center of many studies with the increasing demand for more accurate mechanisms for identifying and authenticating the users. Multi-biometric systems utilizing this principle are referred as *sensor fusion* [1], [2]. With this process the information produced by several sources is optimally combined to improve recognition with respect to simpler authentication process relying on legacy authentication mechanisms such as hardware tokens, passwords or a single biometric.

2.1.1 State of the Art

Many applications of the sensor fusion principles for identification and authentication systems have been proposed. An authentication approach based on a multi-biometric system fusing gait features from ground reaction force and video data of the walking subject has been proposed in [3]. Efficient extraction techniques were considered to identify and generate the characteristic features. The proposed solution consists of one classifier based on the ground reaction force and three classifiers based on visual features. They proposed an approach based on the Bayes risk criterion which subsequently integrates the multiple classifiers. The proposed authentication system significantly increases recognition robustness and reliability with respect to more classical approaches.

To enhance the privacy protection of smartphones, [4] proposes a context-aware implicit authentication, which is a scheme to improve the robustness of the authentication by introducing a context awareness module. The proposed scheme fuses multi-sensor data, including accelerometer, gyroscope, magnetometer, timestamp, pressure and touch size. To characterize touch actions of the user, the multi-sensor data are captured in a fine-grained manner. Then, gesture and touch features are extracted using both statistical method and distance measurement method. A context is defined as the body posture of the user when a touch action happens. In each context, a weighted sum fusion rule was defined to consider the results of different features. The proposed method can effectively improve the reliability and practicability of *implicit authentication* (i.e., mechanisms that are unobtrusive for the user).

In [5], authors provide an approach to identify patients in the healthcare environment by using a fusion of biometrics and information systems. In particular, they investigate the biometric system and the authentication process using periocular biometrics (i.e., the region of the face around the eye). The approach fuses the periocular biometrics and the electronic master patient index in healthcare information systems to identify patients. A comparative analysis of different periocular biometric recognition methods is conducted and assessed against various traditional and deep learning-based methods proving the applicability of the proposed methodology.

To detect, localize and track multiple people, [6] proposes a system to fuse multi-camera computer vision with effective identity information provided by a radio-based localization system. The approach is able to perform tracking analysis for identification, propagating identities while the people move in the environment. Experimental results show that the fusion approach significantly outperforms systems separately using computer vision or radio.

2.1.2 Proposed Approach/Technology

In the E-CORRIDOR core framework, multiple data analytics are in charge of performing driver and passenger identification. This component will leverage these analytics (such as computer vision platforms based on deep learning and multi-camera, a Bluetooth-based localization and gait analysis from sensors available in the user's smartphone) to perform authentication of numerous passengers. Other sensors and data sources (like the RFID data contained in the electronic passport) could be also included in the data fusion to provide one a stronger authentication mechanism.

The proposed continuous authentication system based on the fusion of multi-factor and multi-biometric data is composed by the following modules (similarly to [7]):

1. Data Collection: data are collected either directly from different sensors or from other user identification components available in the analytics toolbox of the E-CORRIDOR framework (e.g., computer vision, Bluetooth-based localization system or gait analysis from smartphone's sensors). In the proposed system, during the passenger operation and movements, the data collection module records the instantaneous readings in x_1, x_2… x_n axes of the n sensors or the output of the identification performed by the other analytics. Then, the collected data are used by the feature extraction module.

2. Feature Extraction: the feature extraction module consists of three sub-modules (i) feature design (ii) feature fusion, and (iii) feature selection.

   i) *Feature Design:* in the feature design module, the data collected by sensors and generated by the identification analyses are segmented by time periods or time windows. In each of these, statistics and frequency features are extracted from each axis of sensors.
   ii) *Feature Fusion:* feature fusion merges multiple features from the same or different input data including the results of the user identification analytics. By combining features from multiple sources, accuracy and reliability (i.e., whereas some sensors could have shadow zones other may work correctly) of the authentication system can be enhanced.
   iii) *Feature Selection:* from the combined features, the ones with the maximum mutual information are selected for each user. Features can be fused according to a parallel or a serial strategy *[8]*.

3. Classifier: a machine learning-based classifier is built by processing the features for training, testing and validation.

4. Authentication: the classifier is used to provide a robust multi-biometric and multi-factor authentication.

To improve the quality of the data, the component could also consider data and analysis from a ground truth created during an *enrollment phase*. Each user will be requested to perform some natural and simple tasks in the enrollment stage (e.g., walking on a pre-defined path prepared in the airport). Therefore, the identification component can build a user profile for all the sensors and simplify the authentication process in the subsequent stages. In such a way, the authentication accuracy can be improved with a minimal to null effect on the user experience.

2.1.3 Data Format Requirement

This component will consider in input mainly the output of the user identification analytics of the IAI analytics toolkit of the E-CORRIDOR framework, but will be potentially enriched with additional sensors and data such as the RFID read of the electronic passport. The sensor fusion analysis will output strong secure authentication credentials.

2.1.4 Platform Requirements

Below we provide the list of requirements in order to fulfil the platform requirement from D5.1

ID	Priority	Requirement	In order to fulfil Platform Requirement(s) of D5.1
E-CORRIDOR-ASI-MFA-001	MUST	Sensor network data and results of the user identification analytics are shared among multiple security areas and mode of transportations (stakeholders) to reduce shadow zone and increase the reliability of the authentication in the multi-modal environment.	E-CORRIDOR-DA-04 E-CORRIDOR-DA-05 E-CORRIDOR-DA-06
E-CORRIDOR-ASI-MFA-002	MUST	Stakeholders managing the distributed sensor networks have to share data and expose analytics results in a standard way.	E-CORRIDOR Ope-04
E-CORRIDOR-ASI-MFA-003	SHOULD	In presence of sensors collecting a large amount of data (e.g., images from cameras) the user identification analytics should be able to provide results in a timely fashion to the MFA module to allow a frictionless experience for the user.	E-CORRIDOR Per-02 E-CORRIDOR Per-03

2.1.5 Application to Pilots

Pilot	Airport-Train pilot

Reference to Use cases or User stories	- *AT-US-03: Distributed and Combined Context Analysis in Sensor Network* - *AT-US-05: End to End Safe-Contact/Contactless Journey* - *AT-US-07: Document-free Secure Multimodal Travel Credential*
Brief description of the Use cases or User stories	The user stories refer to advanced authentication mechanisms allowing a frictionless experience for the passenger thanks to the adoption of multi-sensor data.
Match of the proposed approach/technology with the USs/UCs	MFA and multi-biometric allow a robust, more reliable and accurate user identification and authentication not possible with the use of a single approach.

Table 1. Task 8.1, Multi-Biometric and Multi-Factor Authentication application to Pilots

2.1.6 Potential Synergies with Other Components

Synergies with other components - Work package and Task	- *T7.1* - *T8.2*
Title/brief description of the task	T7.1 includes the user identification analytics provided by the E-CORRIDOR framework, whereas T8.2 allows a continuous authentication in federated domains.
Description of the potential synergy with risks and opportunities	The collected data are fused to achieve and enhance accuracy and reliability of the passenger authentication.
Dependencies on other components	T7.1

Table 2. Task 8.1, Multi-Biometric and Multi-Factor Authentication potential synergies with other tasks and components

3. Continuous Behavioral Authentication – Task 8.2

This task aims at performing a "*continuous and token-based*" authentication in a multimodal transportation domain. In the foreseen scenario, each transportation entity collects over time user information (driver in case of the S2C pilot, and passenger in case of the AT pilot) from the deployed sensors. In turn, the data analytics techniques (see the analytic toolbox in WP7) can build *behavioral fingerprints* (i.e., a token). While the user progresses in her/his journey and changes transportation modes (or simply moves to a different area), the E-CORRIDOR framework uses the information collected in the token to keep the passenger continuously authenticated with the transportation environment.

3.1 Federated authentication based on eIDAS

This advanced security service aims at performing a token-based authentication in a multi-stakeholder environment. In particular, the component exploits standard and widely adopted protocols (such as SAML) and the EU eIDAS for a pan-European identity management. Thanks to this component provided by the E-CORRIDOR core framework, EU citizens are continuously authenticated throughout their multi-modal journeys (e.g., consisting of public bus, car sharing, train, and airport as in the E-CORRIDOR pilots).

3.1.1 State of the Art

Federated Identity Management (FIM) is a set of standards, technologies and agreements that allows different services and applications to dynamically share user identities across a number of different security domains and obtain system interoperability [9]. This essentially allows users to use the same identification credentials such as email and password across multiple different domains to log in securely. An example of this would be using your Facebook account to log into another service such as Spotify, therefore less credentials must be remembered and a friendlier user experience is perceived. The federated identity model is constituted by a few logical components [9]: *user, service provider (SP) and identity provider (IdP)*. In such a model the service that the user wants to access doesn't have to take into account the authentication task. Therefore, the two providers are decoupled allowing better management and higher flexibility of the platform (as often the services have a more rapid evolution than the authentication systems).

By using an FIM system, users have a greater deal of control over what information, such as specific attributes, are shared across domains by service providers. Federations are based on multi-stakeholders agreements and can be realized in two ways [10]:

- *Multilateral*
- *Peer-to-peer (P2P) or bilateral*

Of the two, P2P federation is the simpler model to establish (as fewer parties are involved), but could bring to higher complexity in presence of a higher number of stakeholders as more contracts need to be specified (and more mapping among attributes of each domain have to be defined). However, both models can co-exist and also interoperate to provide the authentication [11].

In practice, a FIM system relies on a number of different protocols: OAuth, OIDC and SAML. These protocols allow different service providers to securely authorize users and pass information between different domains [12] [13].

Through the joint use of these protocols (or a subset of them), some works have created solutions: to grant access to IP-protected web resources with accounting capabilities [14], to perform delegation function with electronic certificates [15], to support authentication and authorization in the exchange of eCR (electronic Case Record) medical data [16], to realize chain of trust for federated cloud environments [17], [18], [19], and to federate non-web-based services [20]

SAML is an Oasis and ITU (ITU-T X.1141) open standard used for exchanging authentication and authorization credentials between security domains. It is an XML-based protocol and uses *security tokens* containing assertions to pass information. SAML 2.0 provides the foundations for building federated architectures [11]. It enables a web-based and cross-domain *single sign-on (SSO)* which reduces the administrative overhead. Thanks to SAML, only one set of credentials is required to log into many different websites (or domains) while maintaining a high level of security. The SAML's core is constituted by the *assertions,* i.e., XML messages containing information about the user's identifier, authentication status and attributes. These messages can be singed and also encrypted.

OAuth is an industry-standard protocol often used in FIM systems. OAuth is an open standard used for *access and authorization delegation* [21]. This means that OAuth is used to grant user access to other websites or applications without the use of passwords. Typically, this method is used to share information with third-party applications or websites. Essentially OAuth allows access tokens to be issued to third party clients by an authorization server with the approval of the resource owner.

Open ID Connect OIDC is a simple identity layer built on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end-user and exchange basic user attributes based on the authentication performed by an authorization server. It gathers and transmits basic profile information on the user (*digital identity*) in a REST-like manner. OIDC allows a range of clients, including web-based and JavaScript clients to request and receive information about authenticated users [22].

3.1.2 Proposed Approach/Technology

Multi-modal transportation domains are constituted by different stakeholders each of which in charge of managing its own security domain. From the user point of view (passenger or driver), the seamless access to the services of each requires that the user is continuously and automatically authenticated. If that goal is achieved, a frictionless experience is perceived by the user while approaching the transportation services. In the E-CORRIDOR core framework, this is attained thanks to a token-based federated identity management exploiting the eIDAS protocol. The authentication token will be generated by each security domain according to user behavior and contextual information. Then, thanks to the eIDAS protocol, these authentication tokens are exchanged among stakeholders through SAML assertions.

eIDAS (Electronic Identification, Authentication and trust Services) is an EU regulation on electronic identification and trust services for electronic transactions within the European Single Market [23]. eIDAS is used to oversee electronic identification and trust services for electronic transactions within the European Union. eIDAS has also created standards for electronic signatures, qualified digital certificates, electronic seals, timestamps and other proof for authentication mechanisms to enable electronic transfers with the same legal standing as transactions performed on paper.

There are a number of different components of the eIDAS framework, each providing their own specific purpose for authentication. Some EU Member State have already adopted the eIDAS framework for services of the public administration (e.g., SPID in Italy [24], NemID in Denmark [25] and the German eID in Germany [26]).

1. *Identity Provider (IdP):* This institution stores and manages digital identities, which verifies the citizen's identity and issues the user with an electronic ID. A user would enter their credentials on a service, and these credentials would be sent as a request to the IdP. The second step involves the IdP verifying the users' credentials to determine if the user can be granted access and what services they can access. The final step either grants or denies the user access to the service after having verified their credentials
2. *Service Provider (SP):* The SP provides access to users to a number of online services. These services can be either public or private. The service provider will receive a request from the external member state or security domain (SAML Request) and will then grant the user access to the services.
3. *eIDAS Node:* An eIDAS-Node is an application component that can assume two different roles depending on the origin of a received request.
    a. *eIDAS Node Connector:* An eIDAS node will assume this role when it is located within the Service Provider's Member State. The Node will receive a request from the Service Provider asking for authentication. The connector receives the authentication requests and forwards it to the eIDAS-Node of the citizens' country.
    b. *eIDAS Node Proxy Service:* The eIDAS node will assume this role when it is located within the citizens Member State. In this case, the node is sending the request. The eIDAS Node Proxy Service receives authentication requests from an eIDAS-Node of another Member State (Node Connector). The Proxy Service also has an interface with the national eID infrastructure and triggers the identification and authentication of a citizen at an identity and/or attribute provider *[27]*.

In the E-CORRIDOR project, the eIDAS framework will be adopted using the Identity Federation and Federated Authentication approach and will take input from the data analytics components in charge of performing the user identification (see D7.1 for a detailed description of the analytic toolbox in E-CORRIDOR). Federated Identity Management (FIM) is based on business, technical and policy agreements that allow organizations to interoperate based on shared identity management. By using FIM a secure, trusted environment for multiple organizations can be created to give users SSO (Single Sign On) and SLO (Single Log Out) capabilities within the circle of trust (CoT) [11].

The image below (Figure 3) shows the process that the eIDAS framework follows using the SAML protocol. To better exemplify one of the applications in the E-CORRIDOR project the two entities represent the stakeholders in the AT pilot (i.e., SNCF for the train station and ADP for the airport). The process is explained as follows:

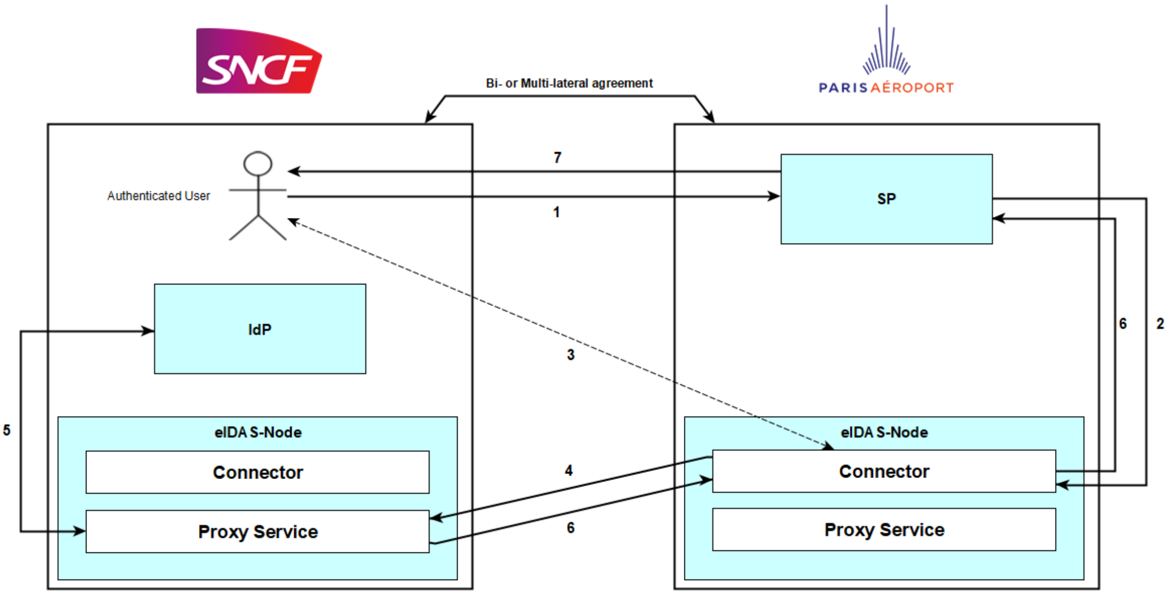


Figure 3 eIDAS infrastructure in a multi-stakeholder environment (adapted from [28] for the AT pilot of the E-CORRIDOR project)

1. An user authenticated at SNCF (e.g., through the data analytics components for user identification available in the E-CORRIDOR analytic toolbox) requests access to the services provided by Paris Airport (ADP);
2. ADP then sends the request for services to its own eIDAS connector;
3. On receipt of the request, the connector asks the user for the domain of origin (or this is automatically identified according to the user context). In such a way the correct IdP that has authenticated the passenger at SNCF is identified;
4. When the user selects the entity that has issued her/his credentials, the SAML assertion containing the user authorization (as remarked in Step 1, potentially representing the passenger's models generated thanks to the user identification analytics available in the E-CORRIDOR analytics toolbox) is forwarded from the Connector to the Proxy Service of the user's service provider;
5. The eIDAS-node proxy service sends the SAML assertion as a request to the identity provider for authentication, and a user is authenticated using the electronic identity. The identity is returned to the Proxy-Service. This enables seamless authentication of passengers between services within the federation (i.e., belonging to the same CoT).
6. The eIDAS-node proxy service sends a SAML assertion to the requesting connector, which forwards the response to the service provider.
7. The service provider grants access to the user.

Thanks to this workflow, passengers can be seamlessly authenticated and services such as eWallet use-case of S2C pilot can be used to automatically purchase the required ticket or charge the service fee.

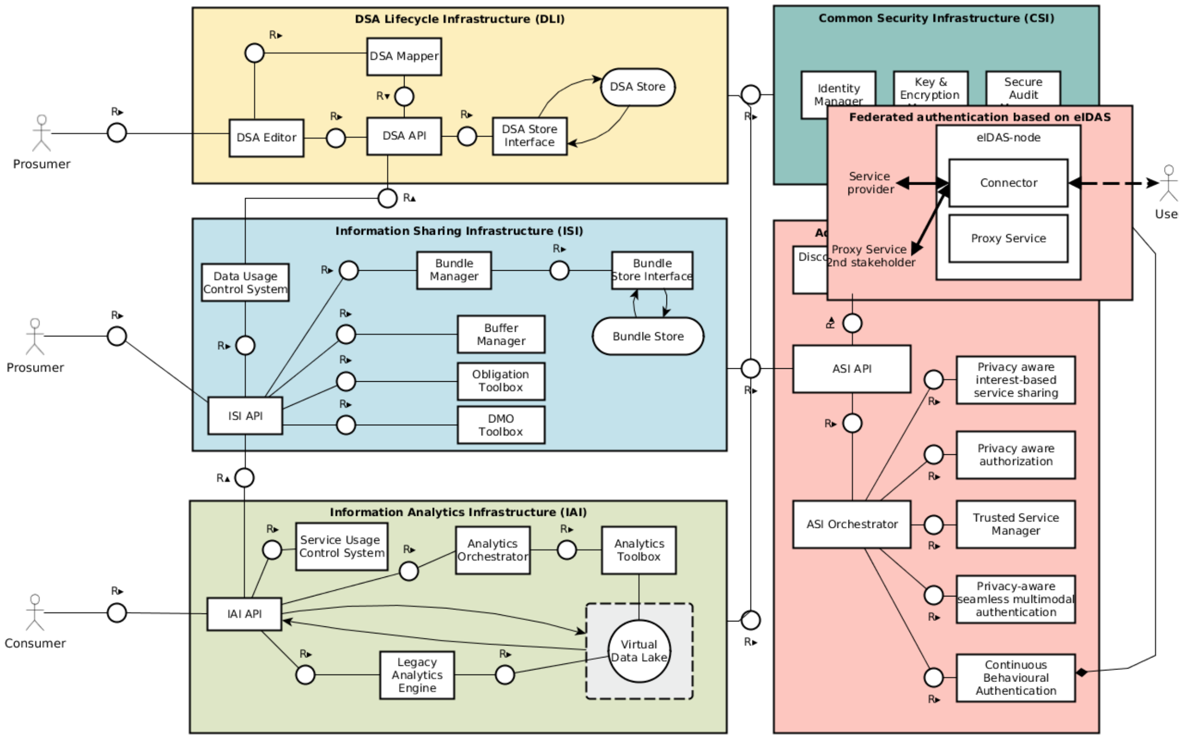

DSA Lifecycle Infrastructure (DLI)
DSA Mapper
DSA Editor
DSA API
DSA Store Interface
DSA Store
Prosumer
Common Security Infrastructure (CSI)
Identity Manager
Key & Encryption
Secure Audit
Federated authentication based on eIDAS
eIDAS-node
Service provider
Connector
Proxy Service
Proxy Service 2nd stakeholder
User
Information Sharing Infrastructure (ISI)
Data Usage Control System
Bundle Manager
Bundle Store Interface
Bundle Store
Buffer Manager
Obligation Toolbox
DMO Toolbox
ISI API
Prosumer
ASI API
Privacy aware interest-based service sharing
Privacy aware authorization
ASI Orchestrator
Trusted Service Manager
Privacy-aware seamless multimodal authentication
Continuous Behavioural Authentication
Information Analytics Infrastructure (IAI)
Service Usage Control System
Analytics Orchestrator
Analytics Toolbox
IAI API
Virtual Data Lake
Legacy Analytics Engine
Consumer

Figure 4: The federated authentication component based on eIDAS integrated in the ASI of the E-CORRIDOR framework

Figure 4 shows how the federated identity management eIDAS-based authentication component is integrated into the E-CORRIDOR framework and in particular in its Advanced Security Infrastructure (ASI). For more details of this architecture, the reader can refer to D5.2.

3.1.3 Data Format Requirement

User’s behavioral models and contextual information created by the analytics will constitute the authentication token. The latter will be encoded in a standard SAML assertion and exchanged among the stakeholders in the federation.

3.1.4 Platform Requirements

ID	Priority	Requirement	In order to fulfil Platform Requirement(s)
E-CORRIDOR-ASI-FA-001	MUST	Stakeholders adopt standard protocols for authentication and authorization in their own security domains (OIDC, OAuth, SAML).	E-CORRIDOR-Sec-IS-06 E-CORRIDOR Use-01
E-CORRIDOR-ASI-FA-002	MUST	Multi-modal transportations belong to the same Circle of Trust (CoT) created through bi-lateral or peer-to-peer agreements.	E-CORRIDOR Per-02

E-CORRIDOR-ASI-FA-003	MUST	The analytic-based user identification systems adopted by the stakeholder in their security domains need to expose models and information as SAML assertions.	E-CORRIDOR-Sec-IS-06 E-CORRIDOR Use-01

3.1.5 Application to Pilots

Pilot	Airport-Train (AT) pilot, Smart City and Car Sharing (S2C) pilot
Reference to Use cases or User stories	- *AT-UC-06* - *S2C-UC-01*
Brief description of the Use cases or User stories	The use cases aim at providing seamless authentication among different mobility operators.
Match of the proposed approach/technology with the USs/UCs	The adoption of standard authentication and authorization protocols and the creation of CoT among the transportation entities allow to perform continuous and automatic authentication.

Table 3. Task 8.2, Federated authentication based on eIDAS application to Pilots

3.1.6 Potential Synergies with Other Components

Synergies with other components - Work package and Task	- *T7.1* - *T8.1*
Title/brief description of the task	The data analytics components in T7.1 are in charge of performing driver and passenger identification. T8.1 performs multi-factor and multi-biometrics authentication in a single domain.
Description of the potential synergy with risks and opportunities	This component exploits identification and authentication performed by T7.1 and T8.1 in a single domain. Thanks to the adoption to standard protocols and the definition of CoT, the federated authentication component allows continuous and automatic SSO in multiple domains.
Dependencies on other components	T7.1 and T8.1

Table 4. . Task 8.2, Federated authentication based on eIDAS potential synergies with other tasks and components

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-Bases Service Sharing, which allows customers to match their interest with other without reveal their real interest and profiles, and vice versa. To limit the risk of privacy exposure, only minimum information about interest attribute of the users is extracted with prevention of real profile attributes. It is secure and almost prevent from hacking profile of users.

4.1 State of the Art

4.1.1 Two-Party Computation (2PC)

Privacy-aware service sharing will exploit the secure Two-Party Computation (2PC) technique to keep private participants' data private. Over the last ten years, researchers have proposed different 2PC frameworks to run private functions. FairPlay [29, 30] is a well-known framework that allows users to write functions using a high-level language, Secure Function Definition Language (SFDL), and to compile SFDL functions into garbled boolean circuits, which will mask the real inputs of both participants. Only a limited number of commands and operations are available in SFDL. For instance, it is not possible to use text values in a function, but only integers or simple types are allowed.

FairPlay has strong security properties in the context of two- party computation. The framework is shown to be secure against a malicious party; in particular *i)* a malicious party cannot learn more information about the other party's input than it can learn from a Trust Third Party (TTP) that computes the function; and *ii)* a malicious party cannot change the output of the computed function. New versions of this framework are FairplayMP [31], which is the extension of Fairplay that works with more than two parties, and MobileFairplay [32], which is the version of Fairplay ported to Android Smartphones.

More recent 2PC frameworks are: MightBeEvil [33] and CBMC- GC [34]. Both have the similar goal, namely allowing people to easily write functions that can be run in a private way. CBMC-GC is composed of two main parts: the compiler that translates functions written in "C" into garbled circuits, and the interpreter 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. Moreover, CBMC-GC implements an optimization phase during the compilations phase that allows the framework to use less memory than other 2PC frameworks.

4.1.2 Fully homomorphic encryption based service sharing

Homomorphic encryption (HE) is a recent cryptographic method allowing performing computation 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 to preserve the privacy of each user, their data are 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 functions 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 to switch 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 *13ms* to perform a gate evaluation) techniques 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.

4.2 Proposed Approach/Technology

4.2.1 Two-Party Computation (2PC)

The technology will be accessed by actors through smartphone apps as well as infotainment system apps. Actors will have the opportunity to define themselves an app, for instance, by indicating the interests, personal information and so on that will be evaluated in a privacy-preserving way. Data employed in the services will not be disclosed with other parties unless actors did not declare how to share, for instance data-sharing after pseudo-anonymization.

To provide privacy-preserving service sharing, we leverage the secure Two-Party Computation (2PC) idea proposed by [2PC]. 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 to securely compute g(x, y) without the need of a TTP.

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

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

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

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

4.2.2 Fully homomorphic encryption based data sharing service

In the E-CORRIDOR project, FHE technology will allows 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 licence, e.g a proof that the driving licence 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.

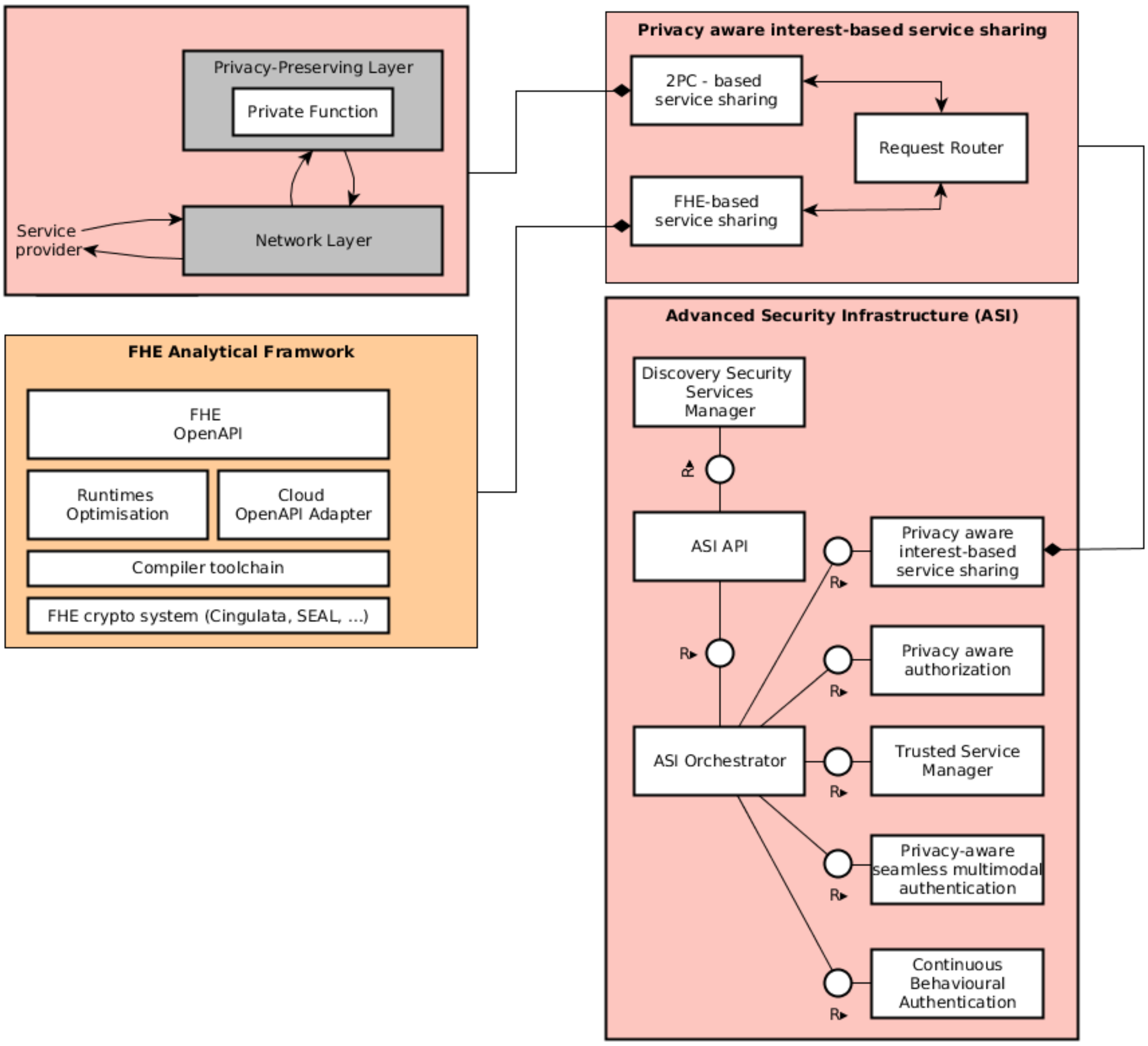

Privacy-Preserving Layer
Private Function
Network Layer
Service provider
Privacy aware interest-based service sharing
2PC - based service sharing
Request Router
FHE-based service sharing
FHE Analytical Framwork
FHE OpenAPI
Runtimes Optimisation
Cloud OpenAPI Adapter
Compiler toolchain
FHE crypto system (Cingulata, SEAL, ...)
Advanced Security Infrastructure (ASI)
Discovery Security Services Manager
ASI API
ASI Orchestrator
Privacy aware interest-based service sharing
Privacy aware authorization
Trusted Service Manager
Privacy-aware seamless multimodal authentication
Continuous Behavioural Authentication

Figure 5: The technology components 2PC and FHE for privacy aware interest-based service sharing integrated in the ASI of the E-CORRIDOR framework

Figure 5 shows how the Privacy Aware Interest-based Service sharing component with 2PC and FHE is integrated into the E-CORRIDOR framework and in particular in its Advanced Security Infrastructure (ASI). The Request Router component allows redirect request to right analysis service 2PC – based service sharing and FHE – based service sharing. In the 2PC – based service sharing feature, it composes 2 layers: Network and privacy preserving layers which interact between them. For the FHE – based service sharing feature, it composes a FHE analytics framework which 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.

4.2.3 Data Format Requirement

Data type will depend on the type of function to be run on the analytic. A relevant requirement of the 2PC technology is that data format should be composed by integer numbers and the function to be implemented should not too complex. This, in fact, may impact the performance of the working function.

Input data will depend on the use case and will be mostly related to the involved participants, i.e., smartphones or infotainment system of vehicles.

4.2.4 Platform Requirements

ID	Priority	Requirement	In order to fulfil Platform Requirement(s)
E-CORRIDOR-ASI-PA-001	MUST	Prosumers may require running analytics expressing conditions to preserve confidentiality over the shared data.	E-CORRIDOR-DS-09
E-CORRIDOR - ASI-PA-002	MUST	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.	E-CORRIDOR-DA-04 E-CORRIDOR-DA-05 E-CORRIDOR-DA-06
E-CORRIDOR - ASI-PA-003	SHOULD	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.	E-CORRIDOR-DA-11 E-CORRIDOR-DM-04
E-CORRIDOR - ASI-PA-004	MUST	Prosumers may require that some shared data, e.g., those ones that contain sensitive information, will be encrypted.	E-CORRIDOR-DM-03

E-CORRIDOR-ASI-PA-005	MUST	Privacy aware Interest-Based analytics will be available at the edge of the E-CORRIDOR framework.	E-CORRIDOR Ope-02

4.2.5 Application to Pilots

Pilot	Airport-Train, S2C, ISAC pilots
Reference to Use cases or User stories	• *AT-UC-04* • *AT-UC-09* • *AT-UC-11* • *S2C-US-08* • *S2C-UC-07* • *ISAC-UC-07*
Brief description of the Use cases or User stories	The above use cases refer to passenger movements in the airport to be monitored in a privacy-preserving way. To the possibility that actors can share data about access to their services in a privacy-preserving manner while preserving data ownership, for instance, passengers are informed by any disruption (e.g., service strike, delay, weather alerts, emergency state) they may incur during their journey. Finally, peers that can ask for analytics without compromising their privacy. For S2C pilot, passenger profiles could be in FHE format in order to check validity and behavior evaluation. For ISAC, this service can allow sharing notification data like IP in blacklist notification
Match of the proposed approach/technology with the USs/UCs	The adoption of technologies to provide privacy-preserving analytics will help prosumers sharing sensitive information without data leak.

Table 5. Privacy aware interest-based service sharing to Pilots

4.2.6 Potential Synergies with Other Components

Synergies with other components - Work package and Task	• *T7.1* • *T7.2* • *T7.3*
Title/brief description of the task	The above tasks refer to Driver DNA for Data Analytics for Driver Identification

Description of the potential synergy with risks and opportunities	This service aims to provide useful and customized services depending on the Pilot use cases.
Dependencies by other components	T7.1 and T7.2

Table 6. Privacy aware interest-based service sharing potential synergies with other tasks and components

5. Privacy Aware Authorization – Task 8.4

5.1 Federated model for attribute based encryption

The need to share information or compute specific function in a privacy-preserving manner is a relevant objective of the E-CORRIDOR framework. Through the privacy aware authorization service, we provide the technology to design and develop services that have the privacy of the participating actors as a requirement by design. Thus, analytics will share data without compromising actors' privacy. As an example, peers may share data based on their interests, and those ones will be matched without disclosing out the degree of interest. Analytics can be run from peers towards edge computing nodes as well as among peers themselves. This latter may allow information to be shared among peers that expressed a particular interest in getting the information. All the procedures that involve information service sharing will be done in a privacy-preserving way.

5.1.1 State of the Art

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Facebook. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services.

One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level. Suppose a particular user wants to grant decryption access to a party to all of its Internet traffic logs for all entries on a particular range of dates that had a source IP address from a particular subnet. The user either needs to act as an intermediary and decrypt all relevant entries for the party or must give the party its private decryption key, and thus let it have access to all entries. Neither one of these options is particularly appealing. An important setting where these issues give rise to serious problems is audit logs. Sahai and Waters [35] made some initial steps to solving this problem by introducing the concept of Attributed-Based Encryption (ABE). In an ABE system, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. The cryptosystem of Sahai and Waters allowed for decryption when at least k attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error-tolerant encryption with biometrics, the lack of expressibility seems to limit its applicability to larger systems.

For more details of Two-Party Computation (2PC) refer to section 4.1.1.

5.1.2 Proposed Approach/Technology

In E-CORRIDOR will develop a fine-grained access control for sharing data based on passenger's interests, which facilitates granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Common to the existing techniques (see, e.g. [36] [37] [38], and the references therein) is the fact that they employ a trusted server that stores the data in clear. Access control relies on software checks to ensure that a user can access a piece of data only if he is authorized to do so. This situation is not particularly appealing from a security standpoint. In the event of server compromise, for example, as a result of a software vulnerability exploit, the potential for information theft is immense. Furthermore, there is always a danger of “insider attacks” wherein a person having access to the server steals and leaks the information, for example, for economic gains. Some techniques (see, e.g., [39]) create user hierarchies and require the users to share a common secret key if they are in a common set in the hierarchy. The data is then classified according to the hierarchy and encrypted under the public key of the set it is meant for. Clearly, such methods have several limitations. If a third party must access the data for a set, a user of that set either needs to act as an intermediary and decrypt all relevant entries for the party or must give the party its private decryption key, and thus let it have access to all entries. In many cases, by using the user hierarchies it is not even possible to realize an access control equivalent to monotone access trees.

5.1.3 Data Format Requirement

Refer to Section 4.2.3

5.1.4 Platform Requirements

Refer to Section 4.2.4

5.1.5 Application to Pilots

Refer to Section 4.2.5

5.1.6 Potential Synergies with Other Components

Synergies with other components - Work package and Task	• *T7.1* • *T7.2*
Title/brief description of the task	The above tasks refer to Driver DNA for Data Analytics for Driver Identification
Description of the potential synergy with risks and opportunities	This service aims to provide useful and customized services depending on the Pilot use cases.
Dependencies by other components	

Table 7. Privacy aware interest-based service sharing potential synergies with other tasks and components

6. Secure Identity Management / Trusted Identity Manager – Task 8.5

In this task a secure identity management system (SIM) for both eWallet digital token (see eWallet use case of S2C pilot in D3.1) and the continuous authentication checking for the passenger and baggage 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 main features of this task are the secure distribution of credentials to establish strong identities in the participating entities. This includes the user identification with his token (e.g., smartphone or smartwatch), backend systems like the E-CORRIDOR backend, car sharing, or airport backend systems as well as the actual resources like vehicles in the car sharing pilot or passenger or baggage tracking in the continuous authentication use case in the airport pilot.

6.1 Trusted Identity Provider (TrIP)

In this sub-task, a Trusted Identity Provider (TrIP) is developed that utilizes roots-of-trusts (RoTs) to secure and manage identities in different components of the E-CORRIDOR system. It is intended to act as a service provider, e.g., to provide cryptographic keys, for higher-level identity management or authentication systems. Special focus is on the underlying trust architecture that enables verifiable trust relationships between participating components so that they can trust in the secure distribution, storage, and usage of credentials.

In this document, the generic approach is described that will be later instantiated for the specific use cases of the pilots.

6.1.1 State of the Art

Identity Management (IdM) comprises processes and systems for management and control of identities in computer and telecommunications systems. Among the most popular schemes for IdM solutions are the OASIS Security Assertion Markup Language (SAML) [40], OpenID Connect [41], Shibboleth [42] project or WS-Trust and WS-Federation [43] [44].

While these systems provide a variety of convenience functions and strong security on the communication layer, the underlying security guarantees, e.g., for a secure key storage or a verifiable system state, are typically not addressed by the standards. However, especially in systems where components are partially exposed to physical attackers (cars, registration terminals, personal devices), strong and verifiable security guarantees on the system level are crucial to establishing trusted relationships between all participating parties.

In summary, we could identify the following basic threats (T) for current state-of-the-art IdMs that are partially derived from [45]:

- T1: Typical user web based identity management systems using SSO credentials based on username and password are prone to phishing attacks [45].
- T2: For components that are physically accessible, an attacker may try to compromise the host system, e.g., by deploying malware, to gain privileged access rights to access stored credentials.
- T3: Lack of trust between user and service provider, which also affects entities' trust in taking part in collaboration and transaction [45].

These threats are addressed with the development of an edge-enabled Trusted Identity Provider (TrIP) that utilizes root of trusts (RoT) in the system. It allows instantiating strong and verifiable security guarantees in the communicating entities to enable solid trust relationships between the communicating parties.

Beginning from a RoT, a trusted system can be bootstrapped. RoTs are system elements that must be trusted since misbehavior is not detectable. In order to build a high trust relationship with the RoTs, their complexity is typically slim, and their correct implementation certified by a trustworthy party that ensures an appropriate EAL.

The Trusted Computing Group (TCG) that develops and standardizes various Trusted Computing technologies, e.g., measured boot or remote attestation, define three types of RoTs that constitute a trusted platform. These are:

1 Root of Trust for Measurement (RTM)

2 Root of Trust for Storage (RTS), and

3 Root of Trust for Reporting (RTR).

The RTM is a component that measures the software state. It is typically used to bootstrap a trusted system and acts as the trust anchor in a chain of trust. The RTM sends its measurements to the RTS that shields these measurements against unauthorized access. The stored measurements may be reported to a remote verifier with the help of the RTR that allows verifying that the measurements are indeed originating from the requested platform.

6.1.2 Proposed Approach\Technology

To mitigate against the identified threats of state-of-the-art IdM systems, we propose a Trusted Identity Provider (TrIP) as our security technology for the E-CORRIDOR framework. The proposed system implements roots-of-trust in the system as trust anchors to secure the provided identities and protocols. This enables the following security properties that directly address the identified threats.

1. SP1: Secure Storage (Addresses T1).
2. SP2: Integrity Verification (Addresses T2).
3. SP3: Report System State (Addresses T3).

With the SP1, security-sensitive data, e.g., credentials like cryptographic keys, can be stored in a securely instantiated shielded location of the component. This enables a 2-factor authentication scheme where the first factor is the key (knowledge) and the second factor is the device itself (possession). This mitigates against phishing attacks (T1). The establishment of cryptographic keys allows secure Machine-2-Machine communication.

With SP2, the system is able to verify its integrity to shield security-sensitive data from modified software states, e.g., by sealing sensitive data to the system state. This mitigates against privilege escalation attacks (T2).

Finally, with SP3, the measurement reports can be used together with the establishment of cryptographic keys to allow the participants to be assured of the trustworthiness of the communication partner (T3).

The approach of this task is structured into the following steps and detailed in the following:

1 Definition of functional and non-functional requirements for TrIP

2 Design of a generic trust architecture with high-level interfaces and protocols

3 Evaluation of the Trusted Platform Module (TPM) as appropriate RoT for TrIP instantiation

In the first step, a generic TrIP design is developed. Therefore, in the first step, the functional and non-functional requirements are defined. Based on the requirements, a generic trust architecture with according communication flows and high-level interfaces and protocols is defined. Next, the TPM is evaluated as appropriate RoT to implement the previously defined generic system design.

6.1.2.1 Definition of requirements for TrIP

The requirements for TrIP are structured in requirements derived from the E-CORRIDOR framework (ER), basic (BR) and advanced (AR) functional requirements. They are listed in Table 8 and described in the following.

Table 8 TrIP Requirements

ID	Priority	Requirement
TrIP-ER-01	MUST	Modular design of the TrIP and consistent interface
TrIP-BR-01	MUST	Secure (re-) provisioning
TrIP-BR-01-01	MUST	Secure distribution of credentials
TrIP-BR-01-02	MUST	Secure storage of credentials
TrIP-BR-02	MUST	Revocation of credentials
TrIP-BR-03	MUST	Basic support for selected high-level protocols
TrIP-AR-01	SHOULD	Verification of the Platform State
TrIP-AR-01-01	SHOULD	Integrity verification of crucial system components
TrIP-AR-01-02	SHOULD	Attestation of crucial system components

Requirements derived from the E-CORRIDOR framework are defined as ER. The framework character allows components of the E-CORRIDOR to be deployed in both the E-CORRIDOR Backend as well as (probably in a reduced instantiation) directly as edge layer in components of the pilots. Thus, TrIP-ER-01 requires that TrIP should be designed modular and with a homogeneous interface so that it can be consistently deployed and used across different platforms.

The basic functional requirements are defined as BR and define the basic requirements that TrIP must enable.

TrIP-BR-01 requires secure provisioning and re-provisioning of credentials. This requirement is crucial to the security of all system components relying on TrIP. Any unauthorized access to credentials may potentially lead to identity theft and thus a compromised system. The requirement is further subdivided into TrIP-BR-01-01 and TrIP-BR-01-02. In detail, TrIP-BR-01-01 demands that new credentials must securely be distributed even across untrusted networks, like Internet connections, to remote parties, while TrIP-BR-01-02 requires that the credentials securely stored on the remote device after distribution so that they cannot be read out even if an attacker has gained access to the platform.

In the case that credentials may have been leaked, there must be a mechanism in place to revoke credentials so that the threat of leak can be mitigated. This, TrIP-BR-02 requires such a mechanism for TrIP.

The last basic functional requirement is TrIP-BR-03. This requirement demands that TrIP should provide support to secure higher-level protocols like authentication services or secure channels, e.g., TLS, for example, by providing an interface for dedicated application keys.

Finally, TrIP should implement some advanced requirements that are denoted as AR. These deal with integrity measurements and attestation of the software state. In particular, TrIP-AR-01-01 requires that TrIP can verify its software state and may, e.g., refuse service if an unauthorized software manipulation occurs, and TrIP-AR-01-02 requires that the software state can be securely reported to a remote party.

6.1.2.2 Design of a Generic Trust Architecture

As required by TrIP-ER-01, TrIP should be designed modular so that it can be easily deployed in the E-CORRIDOR backend as well as edge component in the pilots. Thus, first a generic trust architecture is defined that can be instantiated on the heterogeneous components of E-CORRIDOR system. The generic trust architecture is depicted in Figure 1.

Bootstrapped from a RoT, an isolation layer is instantiated in the system that shields the untrusted host environment from a secured environment, a Trusted Execution Environment (TEE). Depending on the distinct platform, a different RoT implementation may be necessary that induces varying security guarantees. This will be further addressed when the system is instantiated for the pilots.

TrIP is developed as a module so that depending on the resource it is deployed on, it is used as an edge component (e.g., at vehicle or camera level) or as a full-fledged component in the E-CORRIDOR backend. In either case, TrIP is divided into a trusted component hosted in the TEE ((Edge) TrIP Core) and the untrusted component hosted on the untrusted host ((Edge) TrIP Service). The (Edge) TrIP Service provides an interface for other applications or directly to a backend service, e.g., for secure provisioning. The (Edge) TrIP Core provides the security features, e.g., shielded location for cryptographic keys (key store) and integrity values, or secure processes (cryptographic operations, provisioning algorithms).

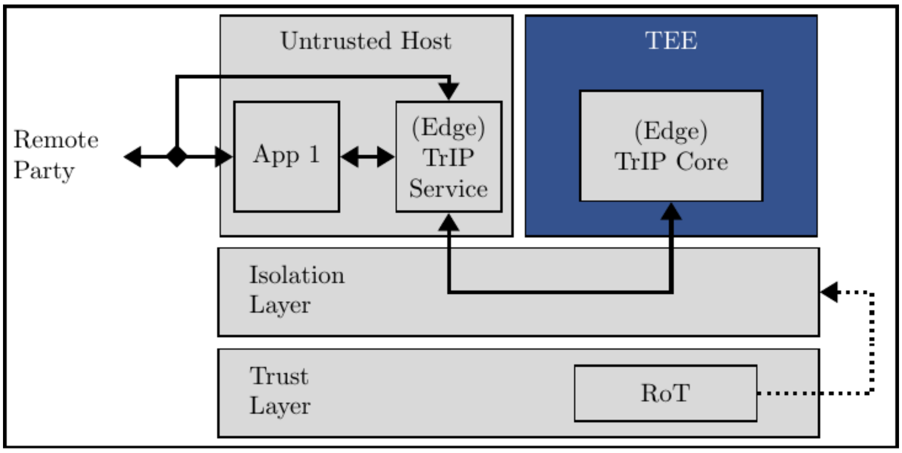


Figure 6: Generic Trust Architecture

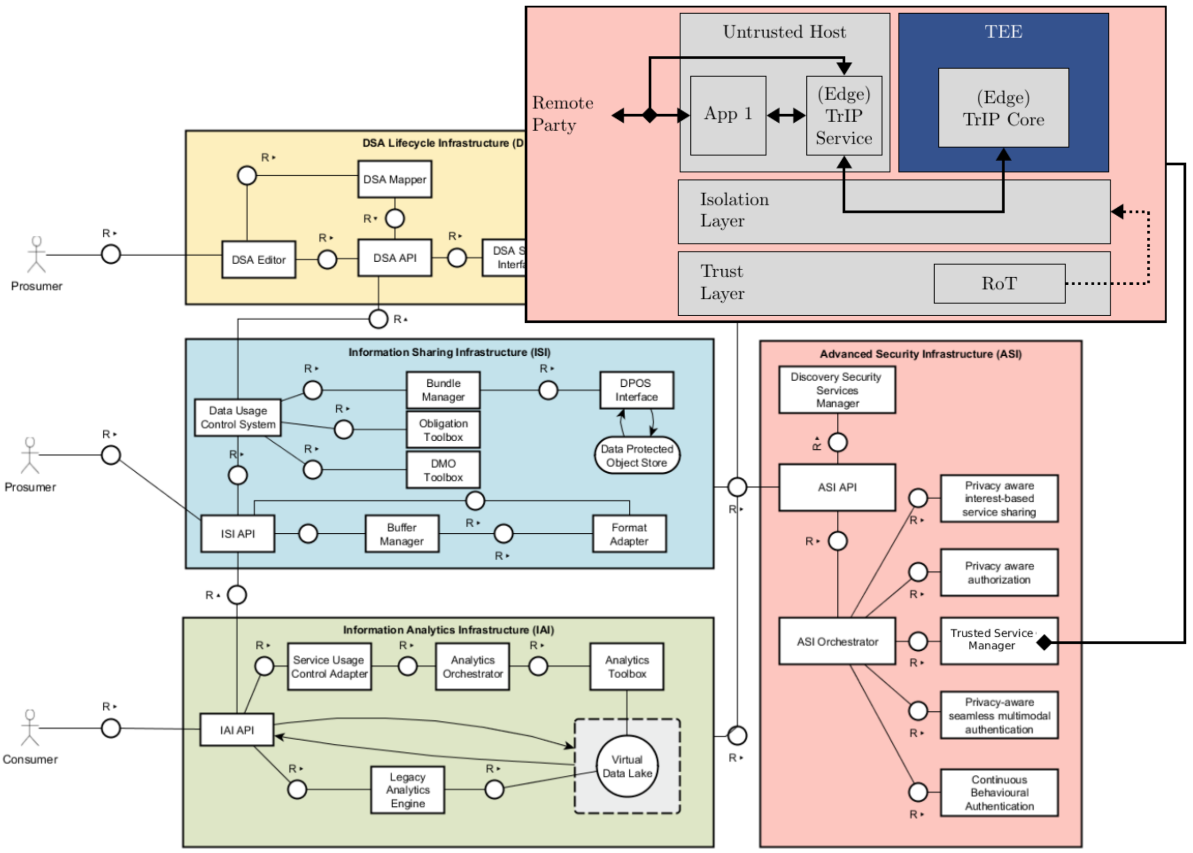

Untrusted Host
TEE
Remote Party
App 1
(Edge) TrIP Service
(Edge) TrIP Core
Isolation Layer
Trust Layer
RoT
DSA Lifecycle Infrastructure (D
DSA Mapper
DSA Editor
DSA API
DSA S Interfa
Prosumer
Information Sharing Infrastructure (ISI)
Bundle Manager
DPOS Interface
Data Usage Control System
Obligation Toolbox
DMO Toolbox
Data Protected Object Store
ISI API
Buffer Manager
Format Adapter
Prosumer
Information Analytics Infrastructure (IAI)
Service Usage Control Adapter
Analytics Orchestrator
Analytics Toolbox
IAI API
Legacy Analytics Engine
Virtual Data Lake
Consumer
Advanced Security Infrastructure (ASI)
Discovery Security Services Manager
ASI API
Privacy aware interest-based service sharing
Privacy aware authorization
ASI Orchestrator
Trusted Service Manager
Privacy-aware seamless multimodal authentication
Continuous Behavioural Authentication
R

Figure 7: Embedding of the Generic Trust Architecture into the E-CORRIDOR Framework

6.1.2.3 Embedding the Generic Trust Architecture of TrIP into the E-CORRIDOR Framework

Figure 7 shows how the generic trust architecture of TrIP is embedded into the E-CORRIDOR framework. It is hosted as module in "Secure Identity Management" component of the Advanced Security Infrastructure (ASI).

While the (Edge) TrIP Service can easily be provided as a container module, the (Edge) TrIP Core heavily depends on the component where it is instantiated. Thus, the suitability to roll it out as a container has to be further evaluated for the specific instantiation.

However, for the first iteration of TrIP we plan to deliver all functionality within a container and use a software-simulated RoT to provide the planned functionality.

6.1.2.4 Evaluation of the TPM as appropriate RoT for the TrIP

In this section, it will be evaluated how the TPM can be used as RoT for TrIP. Thus, first a background on the TPM is given and its features are evaluated regarding the previously defined requirements.

The TCG developed the TPM as a reference platform for their trusted platform architecture. It is designed as a security co-processor that is separated from the host system to which it provides security services. The TPM is a TEE featuring some advanced capabilities going beyond traditional key management functionality and provides tamper-proof cryptographic key storage that secures keys against all software attacks and, to some extent, even hardware attacks.

Its non-volatile memory is used to persist data, e.g., monotonic counters or keys, across boot cycles. A specific non-volatile memory region is dedicated to the Platform Configuration

Registers (PCR) that are used to securely store the platform's integrity measurements, e.g., for Trusted Computing concepts like a measured boot and remote attestation.

Key usage within the TPM may be secured with three different authorization mechanisms: passwords, HMAC, or policy sessions. The latter is also called Enhanced Authorization and allows to access keys by successfully processing a TPM policy. During authorization, the TPM will process presented policy commands sequentially and update an internal policy session digest with each processed policy. If the final digest matches the authentication value of the key, key usage is granted. Currently, 20 different combinable policy commands exist.

The TPM provides both RTS and RTR. Since the TPM can be trusted to prevent inappropriate access to memory, it can act as RTS and it provides functionality to report verifiable measurements from the RTS to external parties allowing it to act as RTR.

The TPMs suitability as RoT for TrIP is evaluated by mapping the basic and advanced requirements of Table 8 to the TPM features and providing the rationale for their fulfillment.

TrIP-BR-01: Secure (re-) provisioning: The secure (re-) provisioning is comprised of the secure distribution and storage of credentials. The TPM is designed as shielded location that has a key generator. By design, the TPM enforces that sensitive parts of the keys, e.g., a private part of an asymmetric key, cannot leave the TPM. Additionally, it can be proven (to a remote party) that a key is originating from a valid TPM and that is thus has never leaked to any unauthorized parties.

TrIP-BR-02: Revocation of credentials: Revocation is typically done by maintaining a revocation list. This list must be stored integrity-protected. The TPM can use its memory to secure such a list and enforce access control.

TrIP-BR-03: Basic support for selected high-level protocols: The TPM supports the typical RSA and ECC key encapsulation and signing operations and can execute them natively in its trusted execution environment. This allows, e.g., to establish a secure TLS connection where the keys are residing in the TPM. In case, a more specific algorithm needs to be executed that is not supported by the TPM, it can be at least store the key data and can further be used to bootstrap a secure software container where the operations can be done in software.

TrIP-AR-01: Verification of the Platform State: The TPM offers a dedicated memory region to securely store software state measurements, the PCRs. Additionally, it features a protocol to securely report the measurements to remote parties.

6.1.3 Expected Data Format

TrIP does not use any public datasets but provides an Application Programming Interface (API) to be used consistently across the components in the E-CORRIDOR framework. It is either instantiated directly in the backend or as edge layer in the components of the pilots.

6.1.4 Platform Requirements

ID	Priority	Requirement	In order to fulfil D5.1 Requirement(s)
E-CORRIDOR-TrIP-01	COULD	TrIP 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	E-CORRIDOR-Sec-IS-02

		be the instantiation of secure storage to store data encrypted at rest.	
E-CORRIDOR-TrIP-02	COULD	TrIP 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-03
E-CORRIDOR-TrIP-03	COULD	TrIP 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-04
E-CORRIDOR-TrIP-04	COULD	TrIP 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-05
E-CORRIDOR-TrIP-05	COULD	TrIP 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-Sec-IS-06, E-CORRIDOR-Use-01, E-CORRIDOR-Use-02

6.1.5 Application to Pilots

Table 9: Task 8.5, Trusted Platform Module application to Pilots

Pilot	Airport-Train pilot & Car Sharing pilot
Reference to Use cases or User stories	• *AT-US-02: Frictionless Multimodal Journey (Seamless/ Continuous Authentication)* • *S2C-US-01: Sign in eWallet*
Brief description of the Use cases or User stories	The above use case refers to a scenario where a passenger uses multiple modes of transportation (cars, trains, aircraft) during a trip without the need to re-authenticate at every single authentication point. This is done by either using the Seamless/ Continuous Authentication or the eWallet.

Match of the proposed approach/technology with the USs/UCs	TrIP enables strong identities in the participating entities (user, authentication terminals, access resources (cars, train, aircraft)).

6.1.6 Potential Synergies with Other Components

Table 10: Task 8.5, Trusted Platform Module potential synergies with other tasks and components

Synergies with other components - Work package and Task	• *T8.1 Privacy-aware seamless multimodal authentication*
Title/brief description of the task	The above task refers to a technology where legacy authentication mechanisms like different types of biometrics, hardware tokens, or wearable authentication approaches are leveraged to build a multi-factor authentication (MFA) scheme.
Description of the potential synergy with risks and opportunities	The Trusted Identity Provider provides strong (trust anchor-based) identities for the involved entities and thus provides trust functionality for the high-level MFA scheme.

7. Conclusions

This document presented the list of E-CORRIDOR advanced security services designed at M12 to successfully satisfy the pilot security requirements identified in three deliverables D2.1, D.31 and D4.1. A framework program for Advanced Security Infrastructure the E-CORRIDOR team is working for, expresses a representative cross section of the multi-modal transportation systems and is very interesting to define a proof of concept for frictionless passenger experience and improving the cyber-security toward a really integrated pan-European multi-modal transportation environment. All the advanced security services which are designed in ASI mainly focus to privacy-aware constraints, and there are developed from the state of the art.

The next period will be devoted to the refinement of the component features and technical requirements, as well as their development plan. Results on the first maturation of the data security services and the first integration in the E-CORRIDOR framework will be reported in the next deliverable (D8.2, "Advanced Security services first maturation") along with some preliminary demonstration.

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.

A. Appendix

A.1 Definitions and Abbreviations

Term	Meaning
AMB	Airport Managing Body
ASI	Advanced Security Infrastructure
BYOD	Bring Your Own Device
CBP	Customs and Border Protection
CoT	Circle of Trust
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
e-wallet	Digital wallet
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
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
TPM	Trusted Platform Module
TTP	Trust Third Party
UML	Unified Modelling Language
US	United States of America