D5.2 - TELECOM USE CASE VALIDATION

Work Package	WP5 – Platform Validation
Lead Author	Sébastien Canard (ORA)
Contributing Author(s)	Ala Sarah Alaqra (KAU), Jérémy Chotard (ORA), Simone Fischer-Hübner (KAU), Bridget Kane (KAU), Stéphane Guilloteau (ORA), Dominique Le Hello (ORA), Elin Nilsson (KAU), John Sören Pettersson (KAU), Bastien Vialla (ORA)
Reviewers	Eleonora Ciceri (MCI), Boris Rozenberg (IBM)
Due date	30.04.2021
Date	30.04.2021
Version	1.0
Dissemination Level	PU (Public)

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767. The content and results of this deliverable reflect the view of the consortium only. The Research Executive Agency is not responsible for any use that may be made of the information it contains.

Revision History

Revision	Date	Editor	Notes
0.1	15.03.2021	Sébastien Canard (ORA)	TOC definition, initial contribution
0.2	06.04.2021	Sébastien Canard (ORA)	Adding inputs from contributors
0.3	13.04.2021	Sébastien Canard (ORA)	Finalizing first version for internal review
0.4	23.04.2021	Sébastien Canard (ORA)	Correction after first internal review
1.0	27.04.2021	Sébastien Canard (ORA)	Correction after second internal review
1.1	30.04.2021	Orhan Ermis (EURC), Melek Önen (EURC)	Quality check completed

Table of Contents

List of Tables

List of Figures

Executive Summary

One main purpose of the PAPAYA project is to show how the PAPAYA technology can serve concrete use cases. In this document, we focus on the ones related to the telecom world. We more precisely focus on three different aspects that may interest telecom related companies: the way individuals are moving using their smartphone, the way individuals are using the apps in their smartphones, and the way to detect security threats in a network traffic. The work presented here follows the one coming from WP2 on use case specifications, the one from WP3 on privacy-preserving techniques and the one on WP4 about the PAPAYA platform. It has been carried out in Task T5.2 titled “Validation through Telecom UC”.

This deliverable reports the validation process of the three telecom use cases, namely, *Privacy-preserving mobility analytics* (UC3), *Privacy-preserving mobile usage statistics* (UC4), and *Threat detection* (UC5). This validation is given by several means and we provide

- adherence to the initial specifications of the use cases, as defined in Deliverable D2.1 [1];
- adherence to the requirements defined in Deliverable D2.2 [2];
- validation through the identified stakeholders.

This document, when complemented with the outcomes of T5.1 and T5.3, serves as a tool for validating the outcome of the PAPAYA project, in terms of adherence to the initial design and applicability to real-world scenarios.

Glossary of Terms

AI	Artificial Intelligence
BF	Bloom Filters
DST	Data Subject Tool
FG	Focus Group
GDPR	General Data Protection Regulation
IMSI	International Mobile Subscriber Identity
PaaS	Platform as a Service
PP	Privacy Preserving
SaaS	Software as a Service
TP	Third Party
TPC	Third-Party Customers
UC	Use Case
UI	User Interface

1 Introduction

1.1 Purpose and Scope

The purpose of this deliverable is to provide an evaluation and validation of the PAPAYA's telecom use cases w.r.t. use case requirements, privacy requirements, and stakeholders' expectations. The results are combined to provide an integrated evaluation and validation of the project results. Evaluation determines whether PAPAYA meets the desired requirements and measures quantitative information of the key performance indicators related to the three studied telecom use cases. The goal of validation is to check whether the PAPAYA solutions are appropriate for the PAPAYA telecom use cases, meet requirements and perform as expected.

More precisely, this deliverable reports the validation process of the three telecom use cases, which full description is given in Deliverable D2.1 [1]. In a nutshell, we have:

- *Privacy-preserving mobility analytics* (UC3), which target some Orange's Third-Party customers interested in analytics based on individuals' mobility. For example, mobility analytics can be profitable to several kinds of Third Parties such as tourism development agencies, tourist offices, amusement parks, hotels, exhibition centres, stadiums capable of hosting all types of events (e.g.: festivals); etc. Indeed, the provision of insights on the visitors/tourists and their mobility patterns have strong implications for such organizations. Understanding these patterns could help those Third Parties managing infrastructure planning, enhance visitors' experience or tailor tourism offerings, in order to increase their revenues and better satisfy visitors' needs;
- *Privacy-preserving mobile usage statistics* (UC4), which gives the possibility, for Third Parties, to conduct privacy-preserving mobile data usage statistics that will prevent any inference or re-identification risks. In this use case, individuals give their consent and express privacy preferences before data collection by Orange. Individuals then encrypt their (private and sensitive) data before sending them to the Orange data processor which executes the analytics requested by the Third Party. The latter is eventually the only capable of obtaining the result of the statistics;
- *Threat detection* (UC5), which, unlike other user cases, does not necessarily apply to personal data that fall under the GDPR legislation, but focuses on business-sensitive data, whose confidentiality is of paramount importance for companies. Hence, the threat detection use case tackles the problem of detecting threats in systems or networks via dedicated analytics algorithms while respecting the confidentiality of the data used during detection.

Each use case is validated in three different ways. Firstly, we show that the use case specifications, described in Deliverable D2.1 [1], are correctly verified. More precisely, we consider the way we have covered the use case, how we have fulfilled the privacy requirements, the way we have integrated the PAPAYA components and the interface. In a second step, taking Deliverable D2.2 [2] as an input, we explain the way the requirement specifications are also validated. This includes on the one hand privacy requirements, and on the other hand Human Computer Interaction (HCI) demands. We finally explain how we have worked in order to obtain a validation of the UC by stakeholders (more precisely, authorities and end-users).

1.2 Structure of the Document

The rest of the document is organized as follows:

- **Section** Error! Reference source not found. provides the validation of UC3 on privacy-preserving mobility analytics;
- **Section 5** provides the validation of UC4 on privacy-preserving mobile usage analytics;
- **Section** Error! Reference source not found. provides the validation of UC5 on threats detection;
- We conclude the deliverable in **Section** 7.

For each UC related section, we first provide a short recall of the use case. We then give the way the specifications of the use case have been validated, we then explain the way the requirement specifications are now considered as validated and we finally talk about stakeholders' view on the way we have worked on the UC.

1.3 Telecom Use Cases and PAPAYA Platform

PAPAYA privacy-preserving technical solutions could be used both inside a PaaS (Platform as a Service) and a SaaS (Software as a Service) solution. In the telecom case, we have illustrated both, depending on the studied use case.

For UC3 and UC4, integrating the PaaS PAPAYA solution would have been very complex since we had to make the integration of the PAPAYA components (PP counting using Bloom filters or functional encryption, Data Subject Tools 1 and 4) in an existing architecture in Orange, in which a platform already exists. Therefore, in both cases (UC3 and UC4), we have then considered PAPAYA as a SaaS solution, only integrating the useful components. This has permitted us to validate the use of SaaS solutions and their interoperability features within another platform.

For UC5, we have been able to directly integrate the PAPAYA platform, taking advantage of the PaaS solution developed during the PAPAYA project. In this case, we have been able to validate the use of the PaaS solution.

2 UC3: Privacy-preserving mobility analytics

In this chapter we present the validation activities carried out for the first use case in the Telecom scenario, namely, the *Privacy-preserving mobility analytics* use case.

2.1 Use case description in a nutshell

The *privacy-preserving mobility analytics* use case targets some Orange's Third-Party Customers (TPC) interested in some analytics based on the way users are moving when using their phone. Indeed, using the probe data related to the telecom antennas that are displayed all over a specific country, Orange, as any telecom operator inside this country, is continuously collecting, thanks to some dedicated probes, triplets containing:

- the unique identifier (the IMSI) of each individual making a call;
- the geographic location of the antenna collecting this call;
- the precise timestamp for this call.

Such triplet (id, location, date) is of great value for tourism actors, territory planning, event planning, etc. since it permits those actors to know (i) where people are, and (ii) how people are moving from one location to another. Based on that, TPC can propose so-called studies by giving one or several time intervals and one or several geographical locations. More precisely, as described in D2.1 [1], two kinds of analytics are considered in UC3.

1. **Audience measurements**: it consists in counting the number of people in one or several areas of observation during a period of observation. This type of analytics permits to count the number of individuals at one specific location, but also the number of individuals that have been at two specific different locations during the period of observation.
2. **Trajectories analysis**: it extracts information on mobility patterns, that is, information on how people travel from an origin O to a destination D, and the amount of people flowing on each trajectory.

Such type of analysis is very useful in understanding how people participate and move during some specific events. This can have very significant benefits in a whole bunch of areas such as tourism or transport.

But if a telecom operator has the right, and the obligation, to collect such data for billing and legal needs, it has no right to use such data for any other purpose. The consequence is that if we plan to use such a triplet for any other means, we need to define a new legal basis for such new data processing. As there is no easy possibility to obtain a user consent (especially for roaming people), one possibility is to make use of the real time techniques (such as anonymization, pseudonymization or encryption), which permits to transform any sensitive data into a less-sensitive one, if the process is fast enough. But to do so, we need for that to find the most appropriate data processing. The purpose of such processing is then to preserve the privacy of the underlying individuals to prevent re-identification of the resulting “non-sensitive data”. But the way to treat the two aforementioned analytics is different.

1. For audience measurements (see also a simplified description of the interaction in Figure 1), UC3 is based on an existing Orange service that is based on this concept. The main idea of such service is to put each entry of the probe into a structured data set such as a Bloom filter (BF). A Bloom filter has the good property of permitting to easily obtain the number of entries in a given filter, and to make unions and intersections of filters so as to count them. Using a secret key, the dissemination of such a resulting set is no more sensitive since nobody, except Orange, can make the link between one individual (an IMSI) and one entry in the Bloom filter. But the fact that Orange can make such a link poses a problem of replaying the process to test if an individual belongs or not to the data set. The consequence is that such resulting Bloom filters cannot be stored at the end of the process. The idea is then to make use of PAPAYA primitive to perform those operations in the encrypted domain. If Orange doesn’t have the key to decrypt the resulting Bloom filter, then the re-identification is no more possible even for Orange. The resulting (encrypted) set can then be stored longer to obtain more statistics. This has been done using homomorphic encryption.
2. For trajectory analysis (see also a simplified description of the interaction in Figure 2), the idea is to start from the probe data, to encrypt it, and then to execute a trajectory clustering algorithm on encrypted data. We have studied two different ways to treat this case: either using Multi-Party Computation with the Traclus algorithm [3], or using homomorphic encryption with the MinHash algorithm [4].

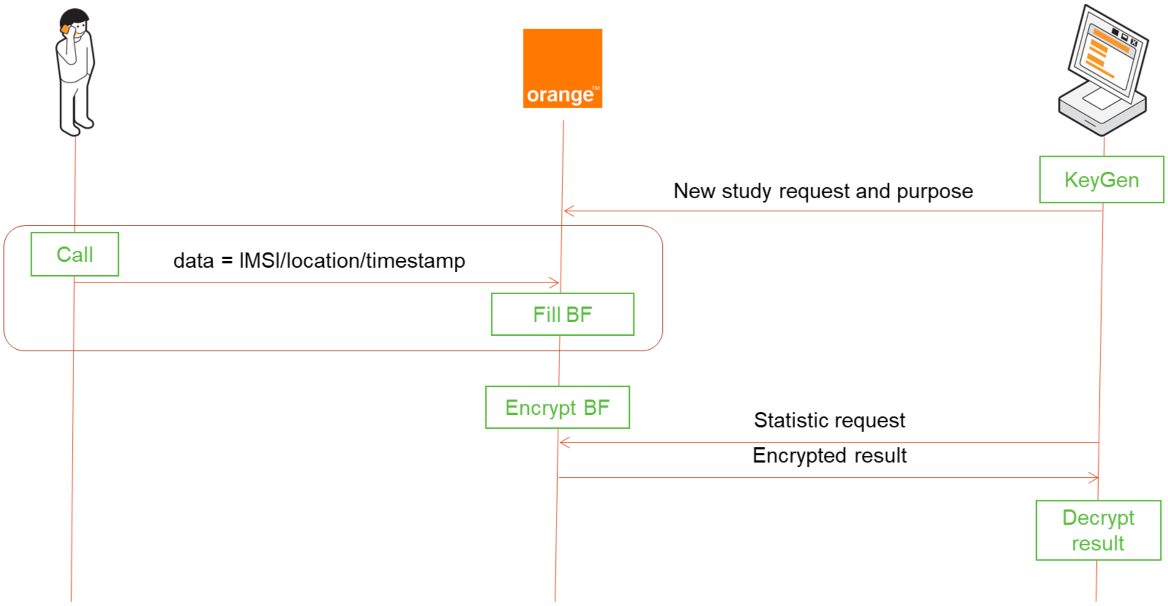
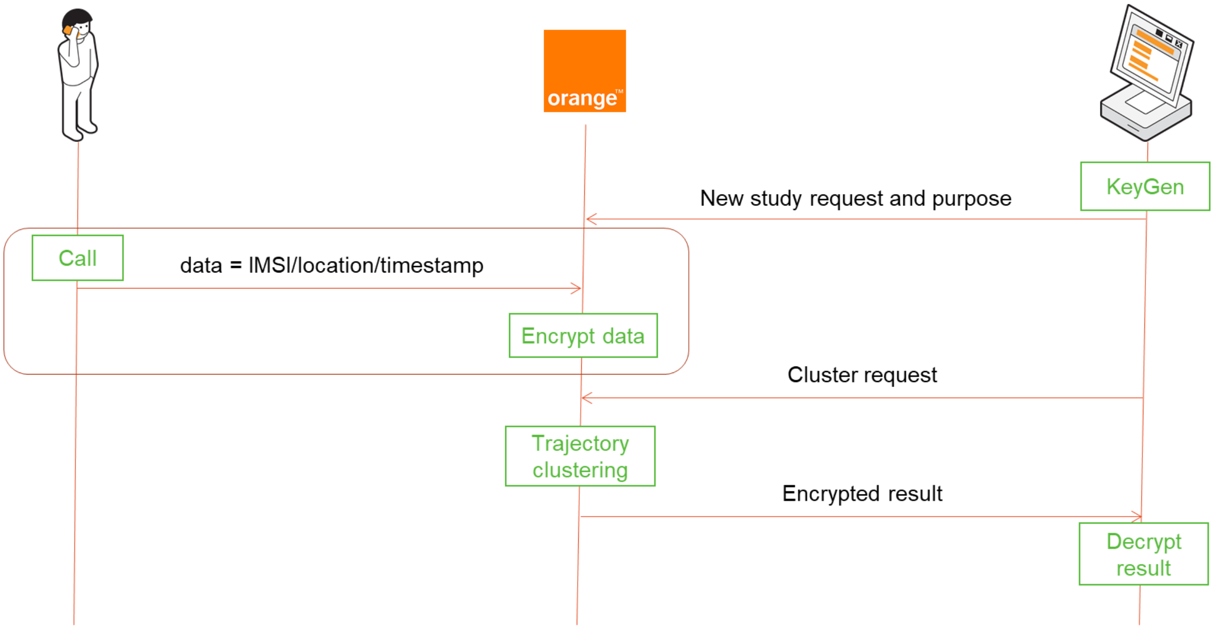


Figure 1 Interactions between actors in UC3 – Audience measurements



PAPAYA 2nd Project Review Meeting, Remote, 22 June 2020

Figure 2 Interactions between actors in UC3 – Trajectory analysis

2.2 Use cases specification validation

In this section we validate the implementation against the use case definition as specified in Deliverable D2.1 [1].

2.2.1 Coverage of use cases

In the following we present the coverage Table 1 for the use case specifications presented in Deliverable D2.1 [1]. For each entry, we give the current status and sometimes give some explanations. As there are some differences between audience measurements and trajectories analysis, we differentiate both.

Table 1 Coverage of use cases related to "Privacy-preserving mobility analytics"

Use case:	Audience measurement status	Trajectories analysis status:
PRE-1 The TPC forms an analytics' request specifying the area and the period of observation	DONE. However, this is done by running a PAPAYA module on Orange's premises.	DONE. However, this is done by running a PAPAYA module on Orange's premises.

PRE-2 Orange registers to the PAPAYA platform	DONE. However, this is done by running a PAPAYA module on Orange's premises.	DONE. However, this is done by running a PAPAYA module on Orange's premises
PRE-3 Instance of (dedicated to Orange) PAPAYA service performing statistics on BFs is running on PAPAYA platform.	DONE. However, this is done by running a PAPAYA module on Orange's premises.	DONE. However, this is done by running a PAPAYA module on Orange's premises.
PRE-4 PAPAYA agent is running on Orange premises.	NOT COVERED, see remark below and Section 3.3.	NOT COVERED, see remark below and Section 3.3.

As explained in Section 3.3, we only consider PAPAYA as a SaaS solution instead as a PaaS solution, and have not integrated the whole PAPAYA platform.

2.2.2 Coverage of privacy requirements

In the following we present the coverage table for the privacy requirements presented in Deliverable D2.1 [1].

Orange encodes the sets of identities in Bloom filters and stores them encrypted, using TCP's public keys. Orange may later apply processing using the properties of the homomorphic encryption. We proceed similarly for trajectory clustering using directly the probe data. These methods provide several guarantees regarding the user's privacy.

Table 3 summarizes the coverage of the privacy requirements for UC3, as specified in Deliverable D2.1 [1].

Table 2 Coverage of privacy requirements for "Privacy-preserving mobility analytics"

Requirements:	Status:
Likelihood to re-identify a user counted in the Bloom Filters must be close to null	DONE. Bloom filters are automatically encrypted with a key that is not known by Orange.
Likelihood to infer information about a user counted in the Bloom Filters must be close to null	DONE. Bloom filters are automatically encrypted with a key that is not known by Orange.
Likelihood to single out a user in a cluster of trajectories must be close to null	DONE. Probe data are automatically encrypted with a key that is not known by Orange.

Likelihood to re-identify a user in a cluster of trajectories must be close to null	DONE. Probe data are automatically encrypted with a key that is not known by Orange.
Likelihood to infer information about a constituent user of a cluster of trajectories must be close to null (for example if, at a given moment, all users living near antenna A are going near antenna B and that antenna B is close to a place of worship, we can infer with a high probability the religion of people leaving living near A)	DONE. The result of the clusters are only given if the k-anonymity is verified, so that it is not possible to single out individuals in their habits.
Orange has to check how to apply the right of information to respect transparency. For example by an SMS to inform data subjects. For example by a « welcome message » in the case of roaming. Orange could be able to exercise the right to object.	NOT DONE. This UC is related to a currently deployed Orange product. We are currently in contact with Orange lawyers but it takes time and at the time of redaction of this deliverable, we have not yet a validated answer to provide. Indeed, this does not invalidate PAPAYA solutions.

2.2.3 Integration with PAPAYA platform

In this section we describe the integration activities performed in task T5.2. Firstly, we list the PAPAYA components that were used (and thus, integrated) for UC3. Then, we present an architectural view of the integrated solution.

We should notice here that the whole PAPAYA platform is not used in this use case. To suit our own internal restrictions at Orange, we have preferred to take the different PAPAYA components we need (see below) and put them in our own architecture. See Section 3.3 for some details.

2.2.3.1 Integrated PAPAYA components

This use case necessitates to embed and execute one or several PAPAYA components, as explained in D2.1 [1]. More specifically, the ones we are using for UC3 are given in Table 3.

Table 3: Integrated PAPAYA component for "Privacy-preserving mobility analytics"

PAPAYA components:		Status:
PP count using Bloom Filters	advanced cryptographic mechanisms to protect individuals' data	DONE

Trajectory clustering	advanced cryptographic mechanisms to protect individuals' data	In progress. We face some difficulties regarding the efficiency of the result (see deliverable D3.3 [5] for details[1]), so it is today difficult to integrate it. We will probably have to wait 1 to 3 years before having enough maturity.

The fact that the trajectory clustering status is today not valid is not a big issue. The main negative consequence is that we cannot today answer some of the requests, coming from third parties, about the way individuals are moving from one place (the origin) to another one (the destination). For this reason, we consider that UC3 is validated as a whole.

2.2.3.2 4.2.3.2 Integrated architecture

The UC3 global architecture is structured with different independent parts, each of them communicating with the others. More precisely, we have:

- The Orange back-end that manages the requests from third parties. It obtains the data (corresponding to a triplet (IMSI, location, timestamp)) from individuals. For audience measurement, it fills one or several BF, depending on the received requests from Third-Party Customers. At the end of each defined period, it encrypts the resulting BF. Orange then simply stores the encrypted BF. For trajectories analysis, Orange directly encrypts a pseudonymized version of the triplet. When necessary, depending on TP's requests, Orange makes the trajectory clustering on encrypted data;
- a TP frontend application, which takes the form of a Web application inside a browser. It manages the creation of a new study and the display of the finally obtained statistics for a given study;
- individuals are not really part of this architecture, as they are not requested to do something particular. It's just that their data are used (in a privacy-preserving manner).

Table 4 gives the way the PAPAYA components are used by each above party (Orange backend and TP frontend, as this is not relevant for individuals, as just explained).

[1] For PP Trajectory Clustering based on 2PC, we can cluster up to 800 line segments if we use only Boolean shares, ~1000 line segments if we use Yao's Garbled Circuits and Arithmetic shares and ~1200 line segments if we use Arithmetic shares. In real-life scenario, it should be possible to cluster ~70000 line segments.

Table 4: PAPAYA component and UC3 actors

PAPAYA components:	Orange backend:	TP frontend:
PP count using BF	✓	✓
Trajectory clustering	✓	✓

Finally, the main interactions between the three actors and the PAPAYA components are given in Figure 3 and Figure 4.

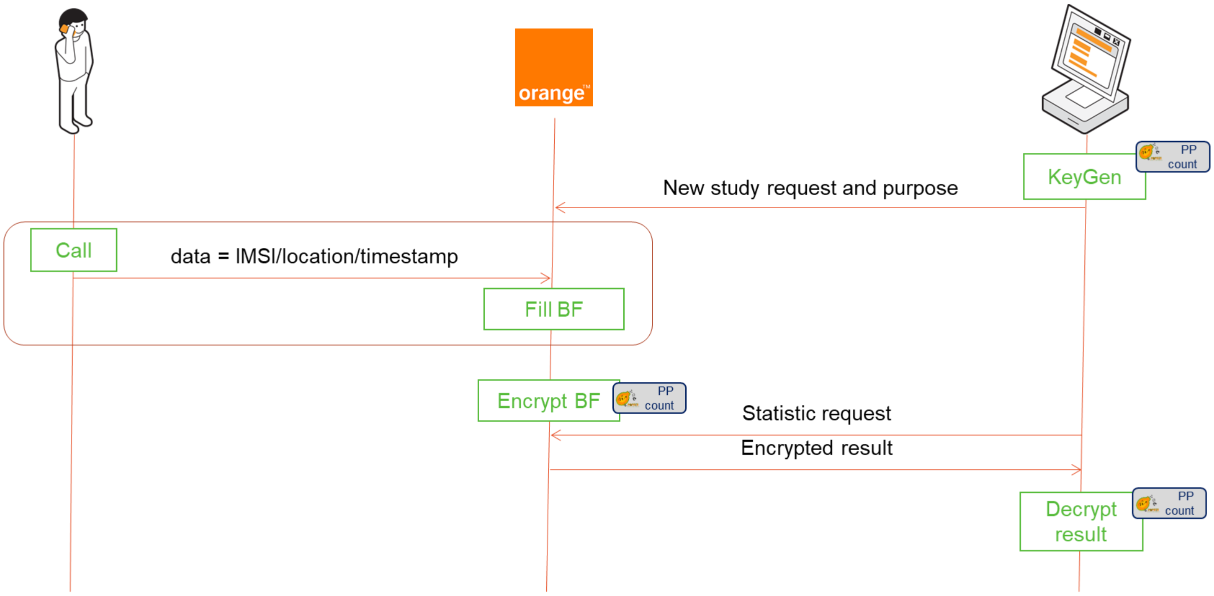


Figure 3 Interactions with PAPAYA components on UC3 – Audience measurements

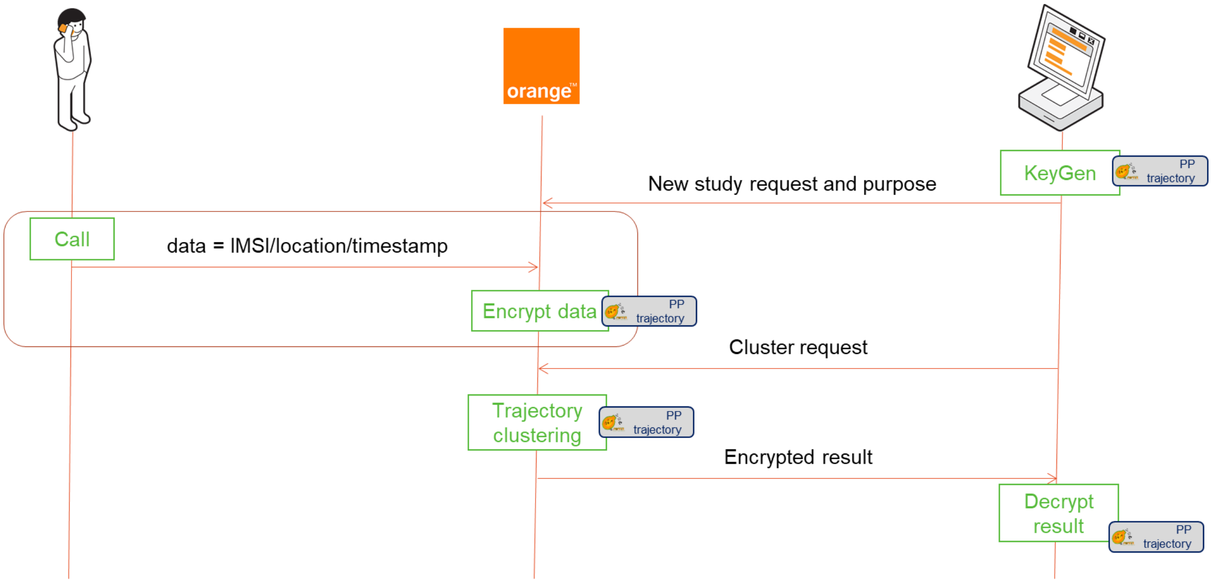
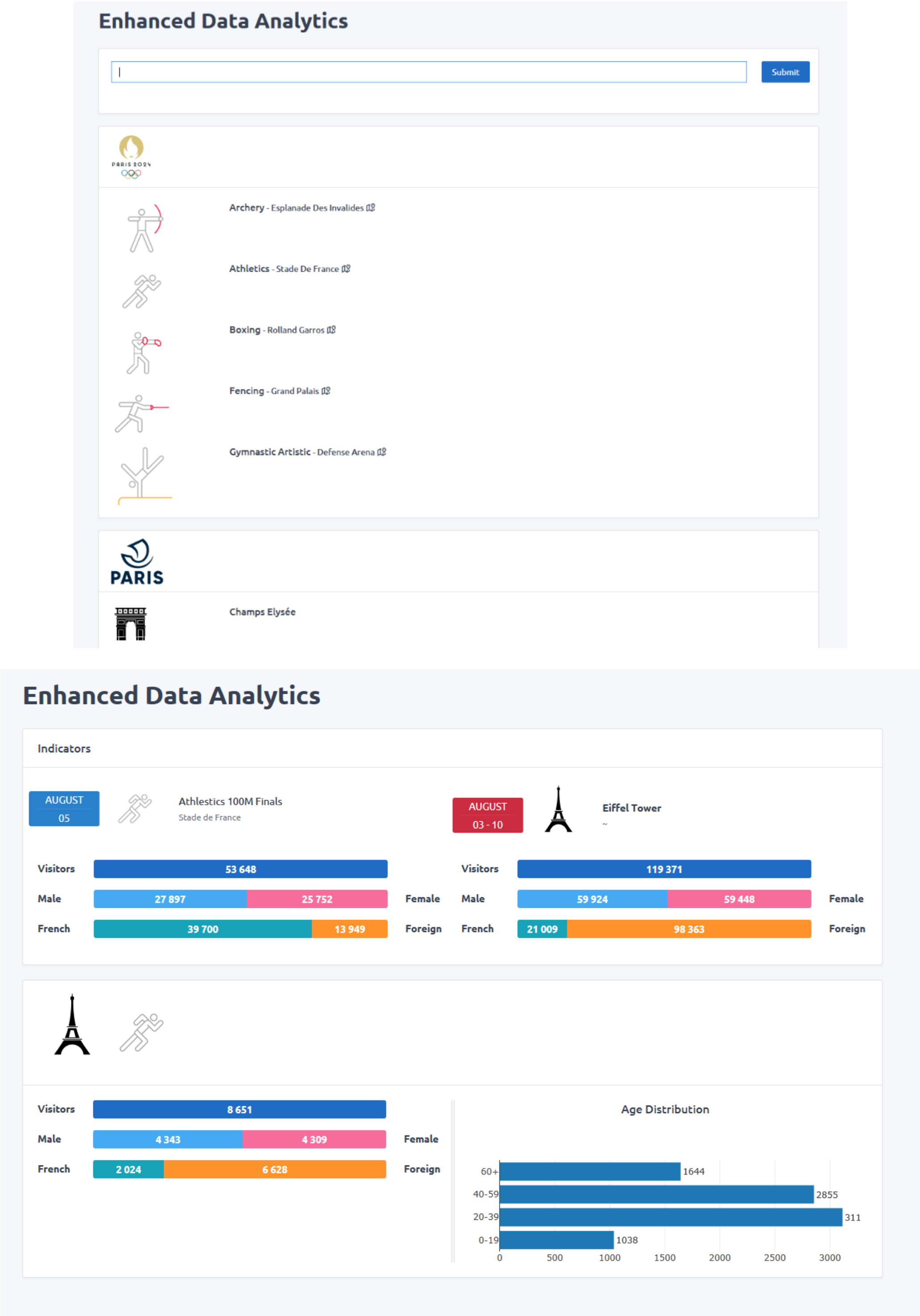


Figure 4 Interactions with PAPAYA components on UC3 – Trajectory analysis

2.2.4 Applications implementation: interfaces

Herein this section, we present main interfaces related to Third Parties. In Figure 5, we show a possible illustration of what can be shown to TP in the case of the Paris 2024 Olympic Games. The first screenshot gives the interface to choose a set of competitions for which one wants to obtain statistics. The second one shows the obtained result. A video presenting the whole system is also available with this deliverable (available in the PAPAYA website).



Enhanced Data Analytics

Archery - Esplanade Des Invalides

Athletics - Stade De France

Boxing - Rolland Garros

Fencing - Grand Palais

Gymnastic Artistic - Defense Arena

Champs Elysée

Enhanced Data Analytics

Indicators

AUGUST 05 Athlestics 100M Finals
Stade de France

Visitors	53 648		
Male	27 897	25 752	Female
French	39 700	13 949	Foreign

AUGUST 03 - 10 Eiffel Tower
~

Visitors	119 371		
Male	59 924	59 448	Female
French	21 009	98 363	Foreign

Visitors	8 651		
Male	4 343	4 309	Female
French	2 024	6 628	Foreign

Age Distribution

60+	1644
40-59	2855
20-39	311
0-19	1038

Figure 5 Screenshots for UC3

2.3 Requirements validation

In this section we validate the implementation against the requirements specified in Deliverable D2.2 [2]. The chosen ones are based on the study that has been done during the redaction of D2.2 for each use case (see the deliverable for details).

We start by giving the main Table 5 for legal privacy requirements pursuant to the GDPR and ePrivacy regulation.

Table 5 Status of privacy requirement in UC3

ID:	Title:	Use case:	Status:	Comment:
C.EUR.L.10	Data minimisation	Common	DONE	Orange manipulates probe data during a short time, then only manipulates individual's data both pseudonymized (using BFs) and encrypted. Moreover, Orange does not know the cryptographic key permitting to decrypt the BF or the probe data.
C.EUR.L.12	Data security	Common	DONE	User data are either manipulated during a short period of time (to fill BFs), or stored pseudonymized (using BF) or encrypted.
C.EUR.L.13	Accountability	Common	DONE	Role of DPO inside Orange.
C.EUR.L.19	Enabling the right to rectification, restriction and erasure	Common	DONE	Orange only manipulates and stores individual's data in an encrypted form.
C.EUR.L.22	Data processing agreement	Common	DONE	Role of DPO inside Orange. Conform to Orange policy
C.EUR.L.23	Adequacy principle	Common	DONE	Conform to Orange policy.

As explained above and in D2.1 [1], there is no human computer interaction in this use case. Then, the Human Computer Interaction (HCI) and usability requirements are not relevant.

2.4 Validation by stakeholders

In this section, we give the different actions and conclusions we have obtained to validate our concept with several specific stakeholders.

We had a meeting with CNIL during the first part of the project, especially on UC3 (see D2.2 [2] for details). The important point is to assess if we can discover that a person's data are in a base or a set of data and the main question to solve is "Is it still possible to single out an individual?".

Using Bloom filters is a first step as it permits data pseudonymization. If one entity obtains a Bloom filter after a security breach, it cannot re-identify any individual inside this structured data set as it does not know how to test whether someone is in the Bloom filter or not. For this, such an entity has to additionally obtain the way the Bloom filter has been created: the used hash functions, and the internal secret key used in those hash functions. Using those secret data and the IMSI of an individual, anyone can easily test whether this identifier is in the Bloom filter or not, using the properties of such a structured data set. The task of an attacker is then much harder. However, this is not impossible, as those secret data can also be stolen from Orange's premises. In particular, using one IMSI as an entry, Orange can itself test whether someone is in a Bloom filter or not.

Adding an encryption layer permits to limit such an attack. A compromised Bloom filter is now still encrypted and since the attacker does not have the decryption key, it will not be able to re-identify any individual inside the Bloom filter. This implies that Orange does not know the decryption key. Our approach consists then in directly encrypting the Bloom filters using the keys of the TPs. As this approach is compatible with homomorphic encryption, we obtain a system that protects better individuals' privacy.

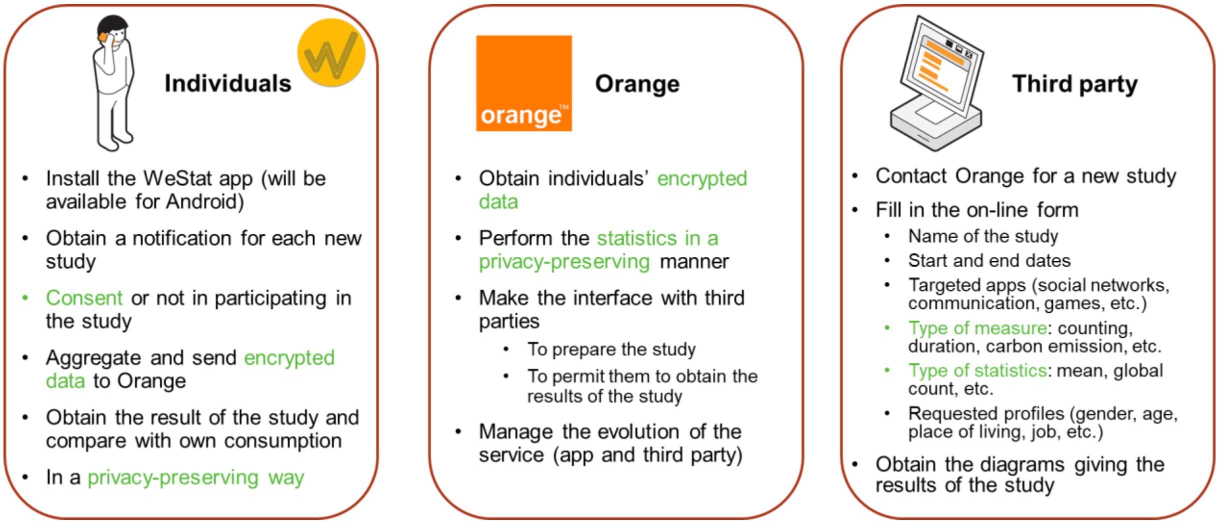
It however remains to validate such approach with Orange legal department, and to more precisely know how long the encrypted data can be stored. Indeed, this use case is related to a currently deployed Orange product. We are currently in contact with Orange lawyers but it takes time and at the time of redaction of this deliverable, we have not yet a validated answer to provide. We plan to obtain most of the answers in a couple of months.

3 UC4: Privacy-preserving mobile usage statistics

In this chapter we present the validation activities carried out for the second use case in the Telecom scenario, namely, the *Privacy-preserving smartphone usage analytics* use case (named Anonym-TRIP in previous deliverables and now called WeStat).

3.1 Use case description in a nutshell

Orange's *privacy-preserving smartphone usage analytics* mobile application, called *WeStat*, is designed to produce statistics on the use of mobile phone applications while scrupulously respecting the privacy of the participating users. According to Deliverable D2.1 [1], there are three main actors in this use case: users/individuals, Orange as an Aggregator and Third Parties (TP). A detailed view of actions and rights for each party is given in Figure 1.



Individuals

- Install the WeStat app (will be available for Android)
- Obtain a notification for each new study
- Consent or not in participating in the study
- Aggregate and send encrypted data to Orange
- Obtain the result of the study and compare with own consumption
- In a privacy-preserving way

Orange

- Obtain individuals' encrypted data
- Perform the statistics in a privacy-preserving manner
- Make the interface with third parties
  - To prepare the study
  - To permit them to obtain the results of the study
- Manage the evolution of the service (app and third party)

Third party

- Contact Orange for a new study
- Fill in the on-line form
  - Name of the study
  - Start and end dates
  - Targeted apps (social networks, communication, games, etc.)
  - Type of measure: counting, duration, carbon emission, etc.
  - Type of statistics: mean, global count, etc.
  - Requested profiles (gender, age, place of living, job, etc.)
- Obtain the diagrams giving the results of the study

Figure 6 WeStat actors and main roles

The main interaction between all those actors are given in Figure 7, and some details will be given further. On one side, a TP is interested in obtaining insights on mobile usage. It requests Orange to collect and analyze mobile usage data from users that consent to participate in a study and to share their data. Orange performs the requested analytics and returns the result to the TP.

On the end users side, the *WeStat* mobile app (OMA as per Orange Mobile Application in D2.1 [1]) collects usage data depending on user's habits, encrypts them and sends the encrypted aggregated data to the *WeStat* backend in charge of the computation of statistics on encrypted data. The encrypted results are then sent to TP, who has requested the statistical survey. The TP will eventually obtain the result in plain.

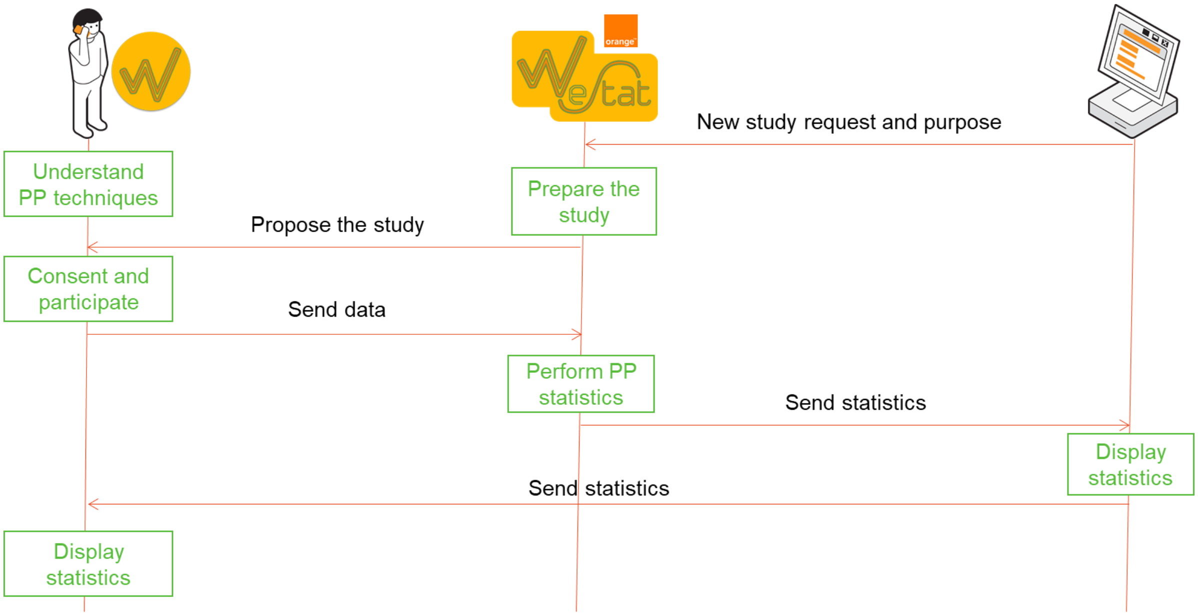


Figure 7 Interactions between actors in UC4

Each study is given by a set of information:

- name of study and start/end dates;
- targeted apps (within different categories such as social network, games, communication);
- type of measure such as counting, duration or carbon emission;
- type of statistics such as global counting, mean, linear regression;
- the requested profile (range of age, place of living, etc.).

This level of details that is accepted by the individual regarding his/her profile can be parametrized using the Privacy Engine tool [6].

The *WeStat* back office is a generic application offering a framework for specific statistical needs to be set up on a case by case basis, for both Third Parties (thanks to a web application) and individuals (thanks to the *WeStat* app).

3.2 Use cases specification validation

In this section we validate the implementation against the use case definition specified in Deliverable D2.1 [1].

3.2.1 Coverage of use cases

In the following we present the coverage Table 6 for the use case specifications presented in Deliverable D2.1 [1]. For each entry, we give the current status and sometimes give some explanations.

Table 6: Coverage of use cases related to “Privacy-preserving smartphone usage analytics”

Use case:	Status:
PRE-1 Orange registers to the PAPAYA platform.	DONE
PRE-2 Instance of (dedicated to Orange) PAPAYA service performing statistics is running on PAPAYA platform.	DONE
PRE-3 Orange and the TP define a business relationship between each other where Orange provides an analytics service to the TP.	DONE
PRE-4 The TP forms an analytics request specifying the period of observation, the attributes to collect and the type of statistics.	DONE
PRE-5 Orange validates the technical feasibility of the requested analytics.	DONE
PRE-6 The users install the *WeStat* app, which integrates an instance of the PAPAYA client side platform.	DONE
PRE-7 The users give their consent to the collection and processing of their usage data	DONE
POST-1 A report for the TP produced by Orange, is available for its download.	DONE
Initialisation-1 TP sends to Orange an analytics request that specifies the period of observation, the attributes to collect and the statistics to compute.	DONE
Initialisation-2 Orange studies the technical feasibility of the analytics request, depending on the attributes, the analytics, and the available encryption mechanisms, in accordance with operative legal requirements. If the conclusion is that this is not possible, the process is stopped.	DONE
Initialisation-3 Orange sends an invitation and a consent request to a panel of users to participate to TPC’s study by forwarding the analytics request (via the *WeStat* app).	DONE
Initialisation-4 Users respond to the invitation and give their consent to the collection and purpose of processing.	DONE
Initialisation-5 Users respond to a questionnaire prepared by the Privacy Engine (embedded in the *WeStat* app).	DONE
Initialisation-6	DONE

The Privacy Engine extracts privacy preferences from the users' answers to the questionnaire.	
Initialisation-7 The *WeStat* app generates keying material for the user, by calling the dedicated module in the PAPAYA client-side agent (embedded in the WeStat app).	DONE
Statistics phase-1 During the observation period specified in the analytics request, the *WeStat* app collects the data (the attributes) listed in the request.	DONE
Statistics phase-2 *WeStat* app performs a local aggregation of the collected data.	DONE
Statistics phase-3 Aggregated data is enriched with other kind of data (phone and sociodemographic data).	DONE
Statistics phase-4 *WeStat* app calls the PAPAYA client-side agent to encrypt the enriched aggregated data and sends it to Orange.	DONE
Statistics phase-5 Orange aggregates data received from the users actually participating to the study.	DONE
Statistics phase-6 Orange invokes the dedicated module of the PAPAYA platform which performs the statistics operation specified in the query.	DONE
Statistics phase-7 Orange sends the results to the TP.	DONE
Exception-1 No consent received from the user for the collection and processing of her usage data for the statistics purpose. OMA does not collect data from the unenrolled users.	DONE
Exception-2 Orange deems that the requested analytics is not feasible regarding the available cryptographic mechanisms. Orange sends this conclusion to TPC and stops the process.	DONE

3.2.2 Coverage of privacy requirements

In the following we present the coverage Table 7 for the privacy requirements presented in Deliverable D2.1 [1].

Table 7: Coverage of privacy requirements for “Privacy-preserving smartphone usage analytics”

Requirements:	Status:
Users give consent to mobile app CGU	DONE
Users give consent for each study	DONE
Users data are encrypted on mobile phone	DONE
Encrypted data are sent to backend	DONE
Encrypted data are aggregates on backend side before performing statistics	DONE

3.2.3 Integration with PAPAYA platform

In this section we describe the integration activities performed in task T5.2. Firstly, we list the PAPAYA components that were used (and thus, integrated) for UC4. Then, we present an architectural view of the integrated solution.

We should notice here that the whole PAPAYA platform is not used in this use case. To suit our own internal restrictions at Orange, we have preferred to take the different PAPAYA components we need (see below) and put them in our own architecture. See Section 3.3 for some details.

3.2.3.1 Integrated PAPAYA components

This use case necessitates to embed and execute one or several PAPAYA components, as explained in D1.2. More specifically, the ones we are using for UC4 are given in Table 8.

Table 8: Integrated PAPAYA component for “Privacy-preserving smartphone usage analytics”

PAPAYA components:		UC4 status:
DST1	UIs for consent form and explaining used privacy-preserving techniques.	DONE
DST4	Privacy Preserving Manager for user preferences	DONE
PP count	Advanced cryptographic mechanisms to protect individuals’ data	DONE

3.2.3.2 Integrated architecture

The UC4 global architecture is structured with different independent parts, each of them communicating with the others. More precisely, we have:

- a *WeStat* backend application which performs statistics on encrypted data and make interface with users and Third Parties;

- a user frontend application, which takes the form of the WeStat smartphone app. It manages notifications (for new studies), users' consents for each study, internal data aggregation, data encryption, and ciphertext sending to *WeStat* backend application;
- a Third Party frontend application, which takes the form of a web application inside a browser. It manages the creation of a new study and the display of the finally obtained statistics for a given study.

Each part makes use of one several of the PAPAYA components, such as given in Table 9.

Table 9: PAPAYA component and UC4 actors

PAPAYA components:	WeStat backend:	WeStat app:	WeStat TP frontend:
DST1		✓	
DST4	✓	✓	
PP count	✓	✓	✓

Finally, the main interactions between the three actors and the PAPAYA components are given in Figure 8.

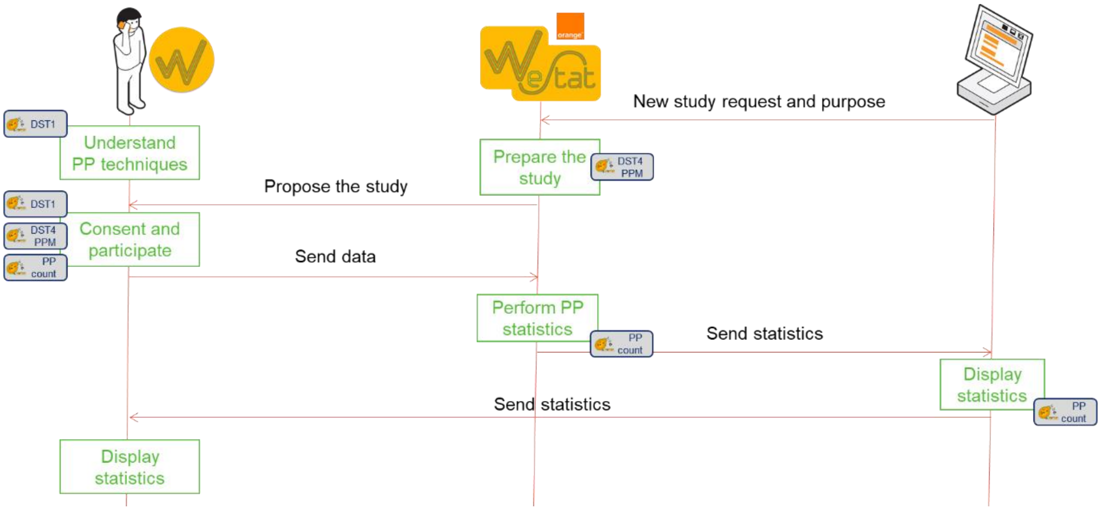
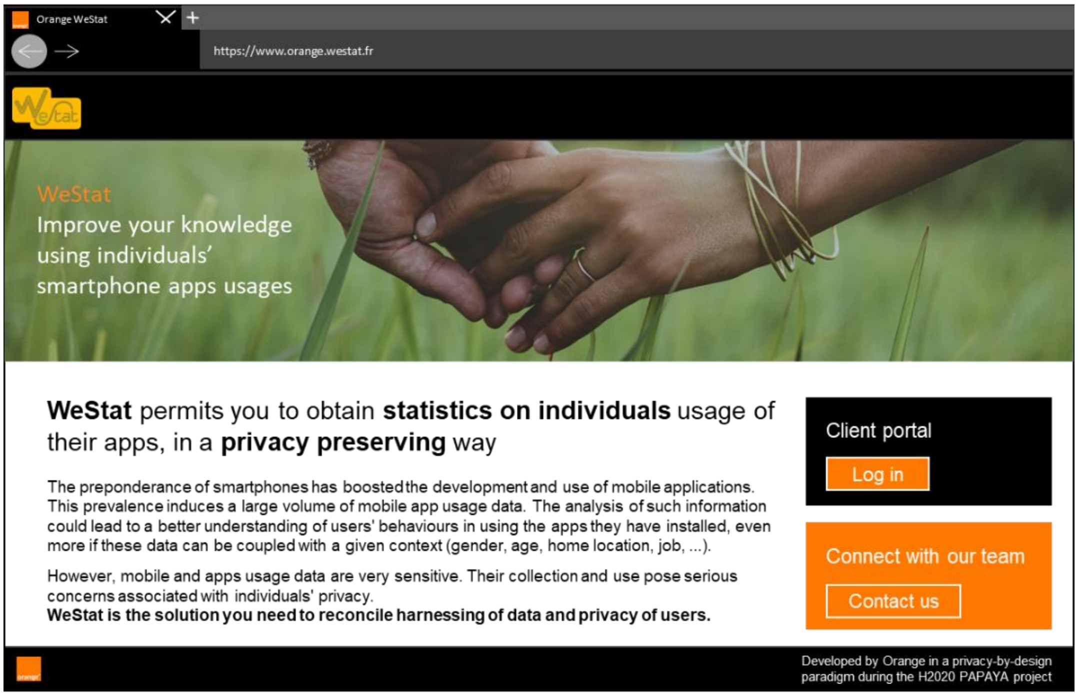


Figure 8 Interactions with PAPAYA components on UC4

3.2.4 Applications implementation: interfaces

In this section, we present the main interfaces related to both Third Parties (Web application, see Figure 9, Figure 10 and Figure 11 with at first the main Web page, then the form a Third Party has to fill to create a new study, and finally an example of statistics that are finally provided to the Third Party) and individuals (smartphone app, see Figure 12 and Figure 13 with at first a list of studies, then the way an individual can manage his/her profile, then the screen for the user to consent to participate to a study and finally the screen for him/her to send his/her data). A video presenting the whole system is also available in this deliverable (available in the PAPAYA website).



WeStat
Improve your knowledge using individuals' smartphone apps usages

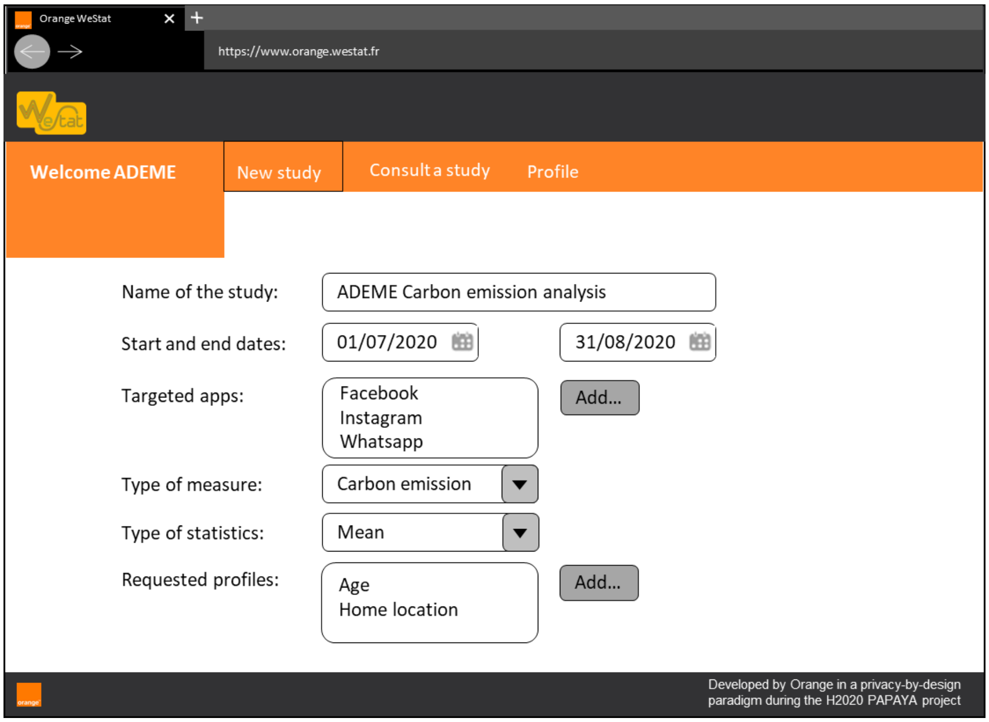
WeStat permits you to obtain **statistics on individuals** usage of their apps, in a **privacy preserving** way

The preponderance of smartphones has boosted the development and use of mobile applications. This prevalence induces a large volume of mobile app usage data. The analysis of such information could lead to a better understanding of users' behaviours in using the apps they have installed, even more if these data can be coupled with a given context (gender, age, home location, job, ...).

However, mobile and apps usage data are very sensitive. Their collection and use pose serious concerns associated with individuals' privacy.
WeStat is the solution you need to reconcile harnessing of data and privacy of users.

Developed by Orange in a privacy-by-design paradigm during the H2020 PAPAYA project

Figure 9 Screenshots for WeStat Third Parties


Orange WeStat
https://www.orange.westat.fr
WeStat
Welcome ADEME
New study
Consult a study
Profile
Add...
Add...
Developed by Orange in a privacy-by-design paradigm during the H2020 PAPAYA project

Name of the study: ADEME Carbon emission analysis

Start and end dates: 01/07/2020 31/08/2020

Targeted apps:
Facebook
Instagram
Whatsapp

Type of measure: Carbon emission

Type of statistics: Mean

Requested profiles:
Age
Home location

Figure 10 Screenshots for WeStat Third Parties

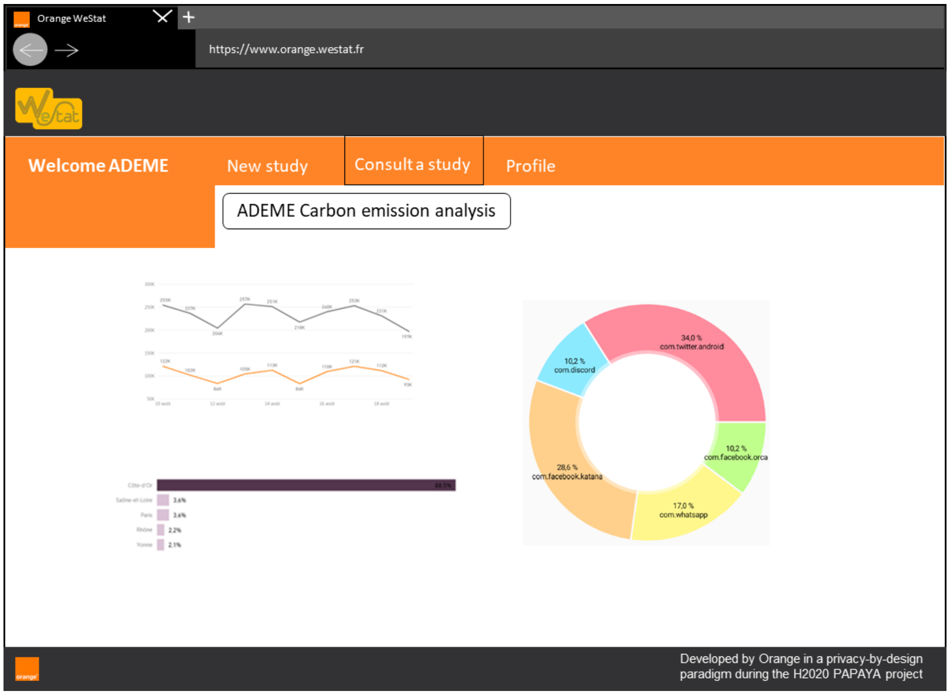
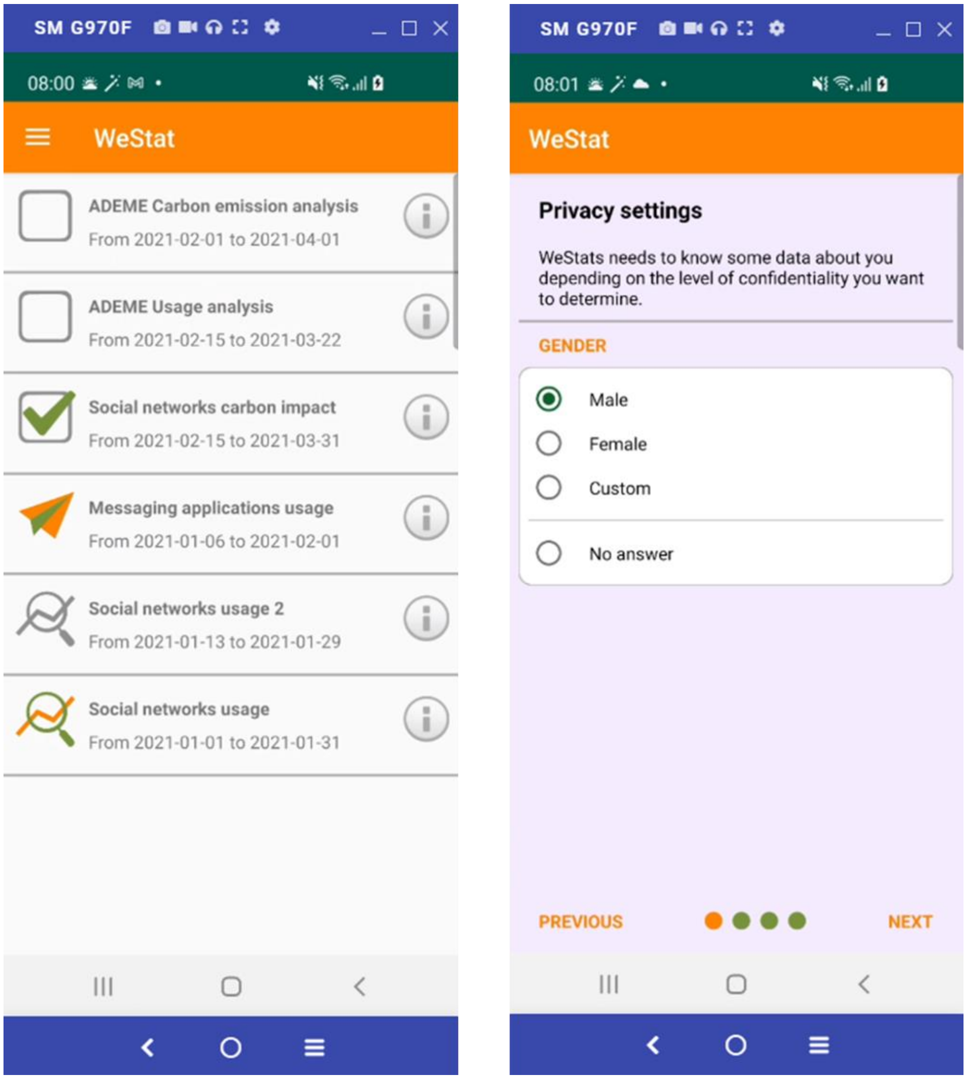


Figure 11 Screenshots for WeStat Third Parties



SM G970F

08:00

WeStat

□ ADEME Carbon emission analysis
From 2021-02-01 to 2021-04-01

□ ADEME Usage analysis
From 2021-02-15 to 2021-03-22

☑ Social networks carbon impact
From 2021-02-15 to 2021-03-31

Messaging applications usage
From 2021-01-06 to 2021-02-01

Social networks usage 2
From 2021-01-13 to 2021-01-29

Social networks usage
From 2021-01-01 to 2021-01-31

SM G970F

08:01

WeStat

Privacy settings

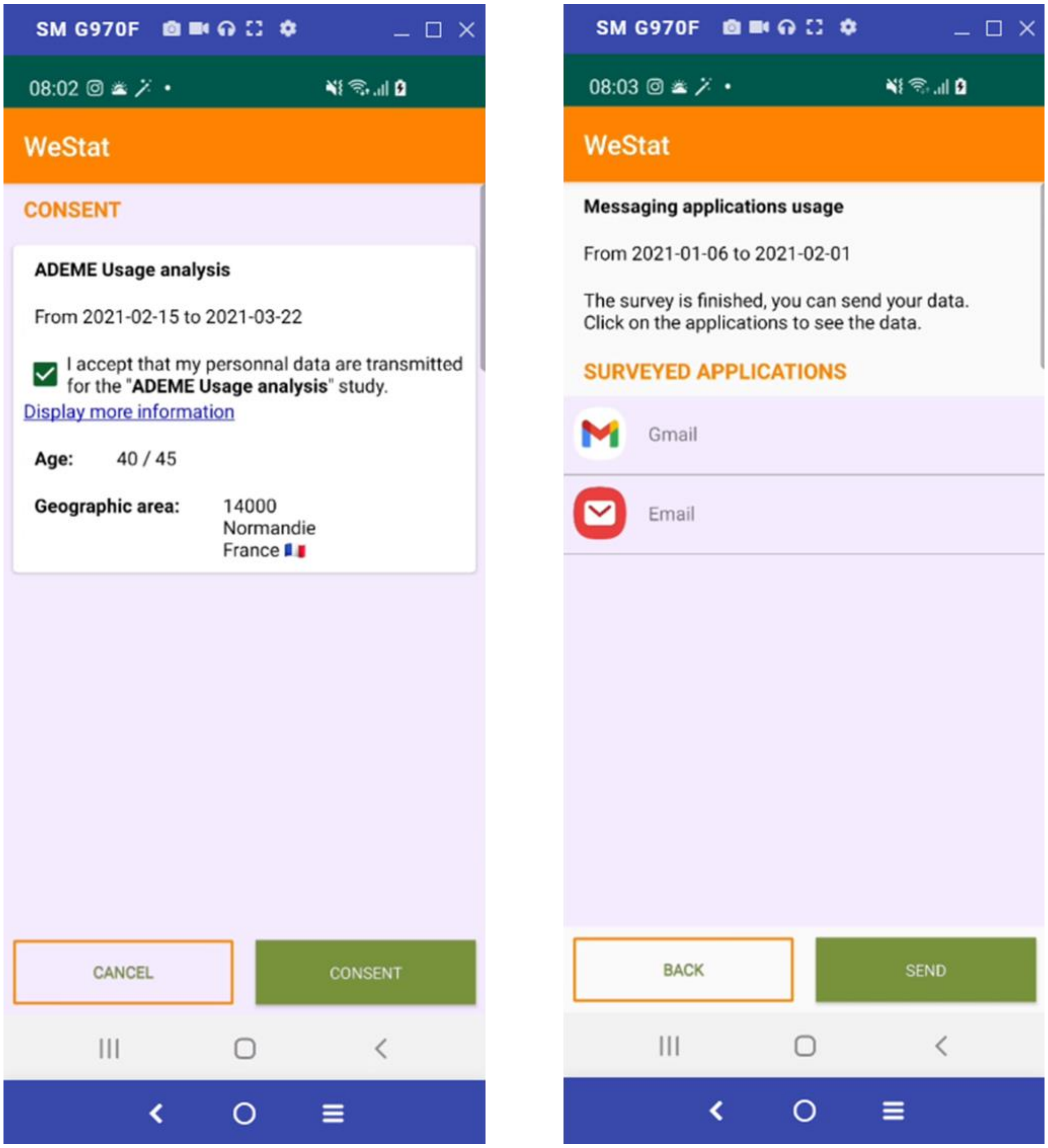
WeStats needs to know some data about you depending on the level of confidentiality you want to determine.

GENDER

● Male
○ Female
○ Custom
○ No answer

PREVIOUS ● ● ● ● NEXT

Figure 12 Screenshots for WeStat smartphone app



ADEME Usage analysis

From 2021-02-15 to 2021-03-22

☑ I accept that my personnal data are transmitted for the "**ADEME Usage analysis**" study.

Display more information

Age: 40 / 45

Geographic area: 14000
Normandie
France 🇫🇷

Messaging applications usage

From 2021-01-06 to 2021-02-01

The survey is finished, you can send your data.
Click on the applications to see the data.

Figure 13 Screenshots for WeStat smartphone app

3.3 Requirements validation

In this section we validate the implementation against the requirements specified in Deliverable D2.2 [2].

3.3.1 Privacy requirements

We start by giving in Table 10 the legal privacy requirements pursuant to the GDPR and ePrivacy regulation.

Table 10: Status of privacy requirement in UC4

ID:	Title:	Use case:	Status:	Comment:
C.EUR.L.8	Fairness and Transparency	Common	DONE	UIs from DST1, see below and validation by stakeholders.
C.EUR.L.9	Purpose limitation	Common	DONE	Used cryptographic primitive limits what can be done by Orange and Third Parties (see [7] for details)
C.EUR.L.10	Data minimisation	Common	DONE	Used cryptographic primitive limits what can be done by Orange and Third Parties (see [7] for details)
C.EUR.L.11	Data accuracy	Common	DONE	Constant modification of aggregated data inside the user smartphone. Users can always modify their profile in the *WeStat* app. Nothing is sent outside the smartphone before users' acknowledgment.
C.EUR.L.12	Data security	Common	DONE	User data are either stored on the user's personal smartphone, or sent/stored/used in an encrypted form.
C.EUR.L.13	Accountability	Common	DONE	Role of DPO inside Orange.
C.EUR.L.1	Lawfulness	Common	DONE	User consent using DST1. See stakeholder's validation.
C.EUR.L.2	Consent	Common	DONE	User consent using DST1. See stakeholder's validation.
C.EUR.L.7	Transparent Information	Common	DONE	User consent using DST1. See stakeholder's validation.
C.EUR.L.15	Policy Icons	Common	DONE	User consent using DST1. See stakeholder's validation.
C.EUR.L.16	Enabling the Right of Access	Common	DONE	DST1 UIs to explain used techniques to protect the data. See stakeholder's validation.

C.EUR.L.17	Enabling the right to withdraw consent	Common	DONE	Users can stop participating in a specific study at any time, no data are then sent outside the smartphone and all data that has been aggregated inside the smartphone is deleted. Once the user has sent his/her data, the data on Orange backend are automatically deleted. After the computation of the statistics, users' data on Orange backend are automatically deleted, and the study result is anonymous.
C.EUR.L.18	Enabling the right to data portability	Common	DONE	Conform to Orange policy on data portability.
C.EUR.L.19	Enabling the right to rectification, restriction and erasure	Common	DONE	Users can stop participating in a specific study at any time, no data are then sent outside the smartphone and all data that has been aggregated inside the smartphone is deleted. Once the user has sent his/her data, the data on Orange backend are automatically deleted. After the computation of the statistics, users' data on Orange backend are automatically deleted, and the study result is anonymous.
C.EUR.L.20	Enabling the right to object	Common	DONE	User consent.
C.EUR.L.21	Enabling the right not to be subject of fully automated individual decision making	Common	DONE	User consent.
C.EUR.L.22	Data processing agreement	Common	DONE	User consent, and additional button for users to send their data in the encrypted domain.
C.EUR.L.23	Adequacy principle	Common	DONE	Conform to Orange policy.
C.EUR.L.24	Metadata processing	UC4	DONE	User consent and data encryption.

3.3.2 Human Computer Interaction requirements

We then focus on the Human Computer Interaction (HCI) and usability requirements, such as given in D2.2 [2].

3.3.2.1 General Human-Computer Interaction

We start with the C.EUR.HCI.1 one, focusing on “General Human-Computer Interaction" (HCI). Indeed, the General Human-Computer Interaction requirement (C.EUR.HCI.1) specified in Deliverable D2.2 [2] calls for three independent expert evaluations to be conducted against the usability principles presented in the deliverable (see Appendix 1). For the acceptance criteria of the requirement to be met the three evaluators had to agree to the adequacy of the applications usability (see first line of Table 11). The rest of this subsection explains how comments from the expert evaluations have been used for the refinement of the user interface for validation by stakeholders.

Each of the three evaluators were given a usability expert evaluation guide defining the principles and the evaluation process. In the guide the evaluators were instructed to go over the mock-up images and evaluate them against the principles and to note down any conflicts. After the completion of the evaluation of the multi-layered policy notice and consent form user interfaces presented below (see Figure 14, Figure 15 and Figure 16, these belong to design development work reported in Deliverable D3.4 [8]), evaluators agreed it could be confusing for the user to navigate among the pages of the application with a risk of the user getting “lost”. Breadcrumbs were suggested as a possible solution to this issue to ensure the users recognize their location among the pages, to enable quicker and flexible movement through the application as well as return to a previous page without repeated clicks. Consequently, breadcrumbs were introduced to the mock-up after the end of the evaluations.

Some changes to the placement and text of some buttons were made to improve the internal consistency of the application as well as to avoid the possibility of accidental presses. In particular, all “Back” buttons on 2nd, 3rd and 4th user interface (UI) layers were moved from the right-hand side to the left side at the bottom of the user interface screens, so that users that repeatedly press on “Back” from lower layer UIs would not by accident press on “Consent” button that is placed down on the right-hand side on the first UI layer.

Other issues mentioned by the evaluators were an issue regarding the contrast of the text in the PIA chart could be too low to meet the principle of “Add enough colour contrast” as well as evaluators mentioning that it might be good to include a page to confirm the consent, or a page where the consent to send the data is given. Solutions for these issues have not yet been implemented in the mock-ups that were used for our end user validation, as they were not strictly needed for testing our data subject tools, but they may be considered by the consent user interfaces in the final version of this use case.

For the page explaining functional encryption specifically (see **Error! Reference source not found.** below) the use of the colour blue to represent the study provider (SP), both in the text and the icons, was changed from blue to green to avoid this text causing confusion due to the similarity of the blue-coloured clickable links on previous pages. We did not change the colour of the word "you" to mimic the colour of the user icon (from red to orange), but this might be considered in the future. The whitespace in the formatting was improved upon on this page, as well as throughout the application. For the abbreviation *SP* for "study provider" might make some users think of "service provider". We did not change this wording in the mock-up, and no participant in the workshops described below ever used the term "service provider" when speaking about the SP. Other parts of the wording might be fine-tuned, such as starting by "If/Once you agree…" instead of "You agree…" to set the conditional state of the things described in the explanation, but the wording used in the mock-up is definitely sufficient for initial user evaluation.

Finally, while the experts validated the general usability of the UI there are some remarks from the evaluators that the essential function of these user interfaces is about informing users. Evaluating how successful this is to involve prospective users. This is part of the research on validation by stakeholders in Section 5.4 of the present deliverable.

3.3.2.2 UC Specific Human-Computer Interaction

We now give in Table 11 the main status and some comments for all the other HCI requirements.

Table 11: Status of HCI requirement in UC4

ID:	Title:	Use case:	Status:	Comment:
C.EUR.HCI.1	General Human-Computer Interaction	Validated for UC4	DONE	Three independent expert evaluations have agreed that the usability is adequate according to the heuristics mentioned in D2.2.
UC4.EUR.HCI.2	There exists an introduction when the app is installed	UC4	DONE	The subscription to the WeStat service (when the app is installed) gives explanation about the studies, GCUs. The way data are protected using DST1 is moreover always accessible to users.
UC4.EUR.HCI.3	Give the user time to think over the data request	UC4	DONE	The user obtains a notification for each new study and should consent to participate. Each study for which the user has not already consent is still in the

				list of studies for which the user can participate.
UC4.EUR.HCI.4	Offer alternative incentives	UC4	NOT COVERED	Incentives will not be implemented and are study dependent (see below).
UC4.EUR.HCI.5	Inform user about limitation in transferability	UC4	DONE	This is done in the user consent form; cf. the stakeholders' validation section.
UC4.EUR.HCI.6	Inform user about limits to the revocation rights	UC4	DONE	This is done in the user consent form; cf. the stakeholders' validation section.
UC4.EUR.HCI.7	Inform user that the incentive will be void if the user withdraws	UC4	NOT COVERED	Incentives will not be implemented and are study dependent (see below).
UC4.P.F.2	Basics Statistics	UC4	DONE	Done using PP counting using FE PAPAYA primitives. See [7] for details.

We will not directly implement the incentive part of the system. In fact, this is related to the commercial relation between Orange and the Third Party requesting the study. This will be done at the time the product will be fully commercialized by Orange.

3.4 Validation by stakeholders

In this section, we give the different actions and conclusions we have obtained to validate our concept with several specific stakeholders.

3.4.1 Validation by Public Authorities

We had a meeting with CNIL during the first part of the project, especially on UC4 (see Deliverable D2.2 [2] for details). It has been concluded that consent would be the legal basis for this use case, and that each study should lead to a specific consent, so that data subjects should have the option to consent to e.g., a processing for scientific research but not for marketing purposes.

We have moreover identified the Data Controller as Orange since, with the help of the Third Party, Orange validates the purposes and means of the processing of personal data. It is under Orange's responsibility to fulfill the requirement of an informed consent, as it is now proposed in the current version of WeStat.

Finally, regarding the cryptographic building block we are using, namely functional encryption, it has been raised during this first meeting with CNIL the question of the management of the master key. Indeed, if managed by a single entity, such key can be used to decrypt the data for a single entity. As shown in [7], the power of the master secret key is in fact given to all users, so that nobody can decrypt the data of a single individual.

We have planned a new meeting with CNIL but due to the current restrictions, related to the COVID-19 pandemic situation, this has not been possible before the redaction of this document.

3.4.2 Validation by End Users

In this section, we present the validation of the UC4 data subject tools with end users as stakeholders. The tools are evaluated in regard to the end users' comprehension and perceptions. For this evaluation, we consider and compare the perceptions and comprehensions of both crypto-experts and non-crypto-experts users.

3.4.2.1 Research Questions

Previous work on users' mental models of end-to-end encryption has shown that especially for lay users metaphors and technical details were most effective if they were functional (mediating what the system can do) rather than structural (explaining how the system works) [DSB+18]. Moreover Bai et al. report that users also found information about confidentiality, risks and weaknesses most useful [9].

Our data subject tools for explaining privacy by design approach based on functional encryption provides structural explanations, which can be complemented with functional explanations as part of multi-layered policy user interfaces (see below, further details will also be put in the upcoming Deliverable D5.4). Moreover, as part of this multi-layered user interfaces, users can also access information about risk reductions and remaining risks by presenting them the output of risk artifacts produced by the extended version of the CNIL Privacy Impact Assessment (PIA) tool presented in Deliverable D3.4 [10].

Our earlier work revealed differences in mental models and perceptions of privacy-enhancing crypto solutions for lay users versus expert users [11], [12]. We are therefore especially interested to analyze whether technical experts are interested in receiving more detailed structural information for establishing trust in the privacy-enhancing solutions and how far functional in combination with structural information and the risk artefacts can help to evoke comprehensive mental models for crypto-experts and non-crypto-experts users.

This has motivated the following three research questions that are investigated for users with different technical backgrounds (i.e. lay users vs. technical experts) and demographics:

RQ1: What are the users' comprehension of and interests in the information about the privacy by design approach and PIA results?

RQ2: What is the impact, preferences and perspectives of functional vs. structural explanations and metaphors on the users' mental models?

RQ3: How are clarifying limitations and remaining risks in comparison perceived and how can they contribute to develop comprehensive mental models?

In addition, we were also interested in the role of incentives for participating in studies within the scope of the Privacy-preserving smartphone usage analytics use case, which motivated our fourth research question:

RQ4: What incentives can motivate users to participate?

3.4.2.2 Methodology

We chose empirical qualitative methods, as our research is explorative with the objective of investigating and gaining a deeper understanding about the users' perceptions and comprehensions with the help of the multi-layered policy notice and consent form user interface (UI) mock-ups showing our data subject tools (see figures below). For the study, a scenario was chosen, in which the users are requested to contribute their age and social network usage data in "aggregated and securely encoded form" for analysis to TelecomAB on behalf of MediaSurvey Cooperation. An example of an incentive was used in the test, which was in the form of monetary incentive; a five-euro Amazon voucher. We held four focus groups (FG), totalling 13 participants, with three focus groups having three participants each, and one focus group with four participants (FG4) in March and in April 2021. In total, there were six male, five female, and two preferred not to say participants. Their age ranges were 18-29 (6), 30-39 (2), 40-49 (4), and 50-59 (1). Two focus groups had participants recruited as non-crypto experts/ lay users (FG1, FG3) and two focus groups recruited as crypto-expert users (FG2, FG4), who were however not experts in functional encryption.

Before the focus group, all focus group participants took part in individual UI mock-up walkthroughs, which allowed us to observe on which links the users were clicking and thus in what types of policy information they showed interest in. Additionally, it allowed the participants to familiarize themselves with the UI and use case individually before having the focus group discussion. The different UI screens were then discussed in the focus groups followed by individual post study questionnaires. All focus group sessions were moderated by the same moderator with at least one further researcher participating and taking notes. The individual UI mock-ups walkthrough sessions were conducted in parallel and moderated by different researchers. All sessions were recorded with Zoom with the participants' consent that was taken at the beginning either by audio or sent in written format by email. Table 12 provides an overview of the qualitative methods that we combined and the corresponding research question. All parts of the study took place online via the telco system Zoom and with support of the interactive Mentimeter presentation tool.

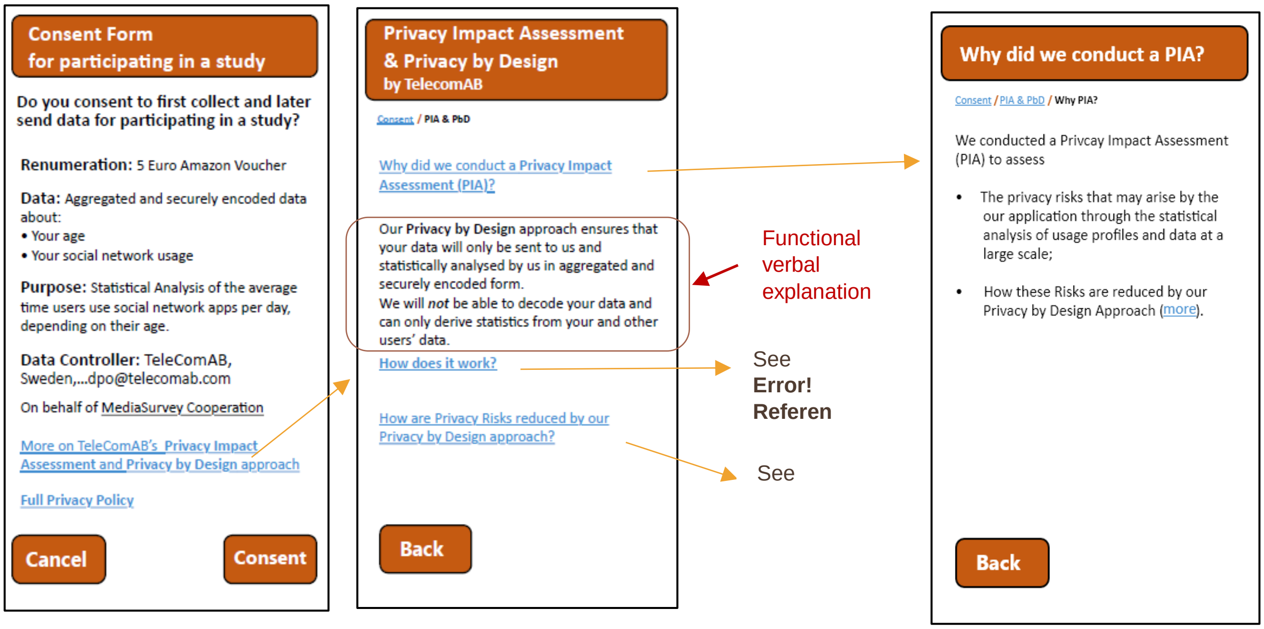
The study guide outlining of our study is presented in Appendix 3. Participants were recruited by the project partners, but were not part of the PAPAYA project. Furthermore, their participation was completely voluntary, and it was highlighted in the study. Appendix 2 presents the consent form that all participants agreed to. The study was evaluated and accepted by one of the ethical advisors at Karlstad University.

Table 12: Overview of the combination of qualitative research methods for the validation study

Parts of the Study:	Investigation of:
A. Individual UI mockups walkthrough	Interests in different elements of the UI (RQ1)
B. Focus groups workshop (3-4 in each group)	Perspectives on incentives, functionalities, trust and metaphors (all RQs)
C. Individual post study questionnaire	Demographics and technical knowledge (all RQs)

3.4.2.3 Mockups of a multi-layered policy notice and consent form

For evaluating the data subject tools for explaining functional encryption and presenting risk management artefacts for assessing the impact of privacy-preserving data analytics on privacy risks, we produced multi-layered policy notice and consent form user interface (UI) mockups, which includes explanation of functional encryption presenting its privacy functionality as well as a structural explanation of how functional encryption works. Moreover, it presents the result of a PIA that was conducted for the chosen scenario. PAPAYA Deliverable D5.4 will describe the user interfaces in more detail.



Consent Form
for participating in a study

Do you consent to first collect and later send data for participating in a study?

Renumeration: 5 Euro Amazon Voucher

Data: Aggregated and securely encoded data about:
- Your age
- Your social network usage

Purpose: Statistical Analysis of the average time users use social network apps per day, depending on their age.

Data Controller: TeleComAB, Sweden,...dpo@telecomab.com

On behalf of MediaSurvey Cooperation

More on TeleComAB's Privacy Impact Assessment and Privacy by Design approach

Full Privacy Policy

Cancel

Consent

Privacy Impact Assessment
& Privacy by Design
by TelecomAB

Consent / **PIA & PbD**

Why did we conduct a Privacy Impact Assessment (PIA)?

Our **Privacy by Design** approach ensures that your data will only be sent to us and statistically analysed by us in aggregated and securely encoded form.
We will *not* be able to decode your data and can only derive statistics from your and other users' data.

How does it work?

How are Privacy Risks reduced by our Privacy by Design approach?

Back

Why did we conduct a PIA?

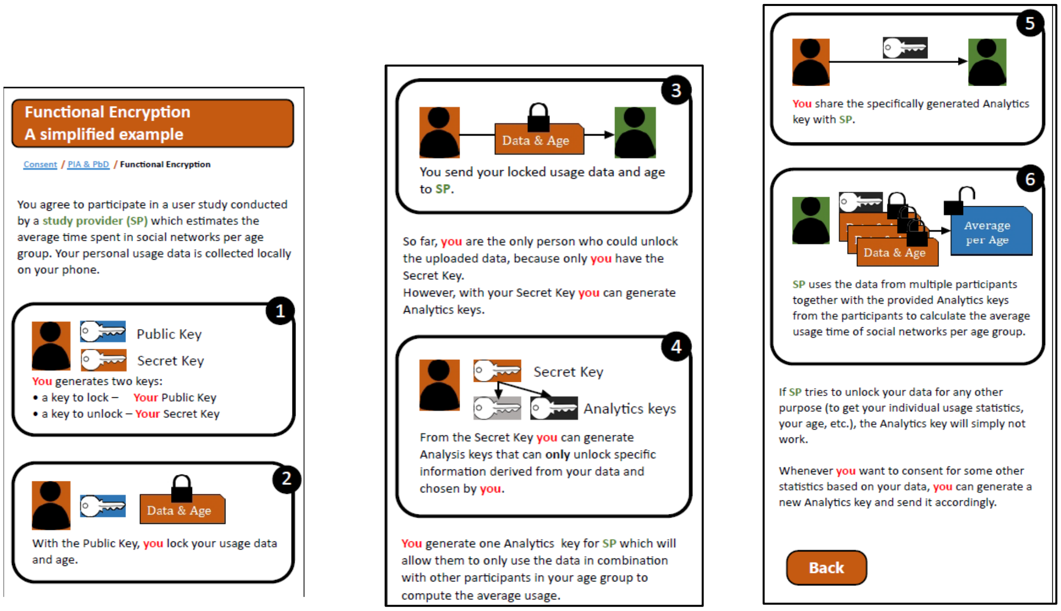
Consent / PIA & PbD / **Why PIA?**

We conducted a Privcay Impact Assessment (PIA) to assess

- The privacy risks that may arise by the our application through the statistical analysis of usage profiles and data at a large scale;
- How these Risks are reduced by our Privacy by Design Approach (more).

Back

Figure 14 Multi-layered policy notice and consent form. Functional explanations of functional encryption are provided on the 2nd layer. Clicking on "How does it work" on the 2nd layer leads to the structural explanation on a 3rd layer.



Functional Encryption
A simplified example

Consent / PIA & PbD / **Functional Encryption**

You agree to participate in a user study conducted by a study provider (SP) which estimates the average time spent in social networks per age group. Your personal usage data is collected locally on your phone.

1

You generates two keys:
- a key to lock – Your Public Key
- a key to unlock – Your Secret Key

2

With the Public Key, you lock your usage data and age.

3

You send your locked usage data and age to SP.

So far, you are the only person who could unlock the uploaded data, because only you have the Secret Key.
However, with your Secret Key you can generate Analytics keys.

4

From the Secret Key you can generate Analysis keys that can **only** unlock specific information derived from your data and chosen by you.

You generate one Analytics key for SP which will allow them to only use the data in combination with other participants in your age group to compute the average usage.

5

You share the specifically generated Analytics key with SP.

6

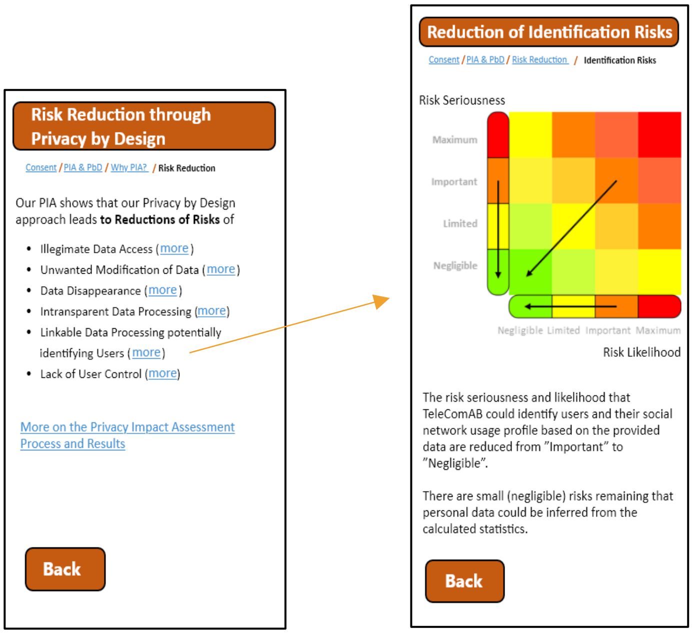
SP uses the data from multiple participants together with the provided Analytics keys from the participants to calculate the average usage time of social networks per age group.

If SP tries to unlock your data for any other purpose (to get your individual usage statistics, your age, etc.), the Analytics key will simply not work.

Whenever you want to consent for some other statistics based on your data, you can generate a new Analytics key and send it accordingly.

Back

Figure 15 Scrollable UI with the Data subject tool presenting high-level structural explanations of how Functional Encryption is working.



Risk Reduction through Privacy by Design

Consent / PIA & PbD / Why PIA? / Risk Reduction

Our PIA shows that our Privacy by Design approach leads **to Reductions of Risks** of

- Illegimate Data Access (more)
- Unwanted Modification of Data (more)
- Data Disappearance (more)
- Intransparent Data Processing (more)
- Linkable Data Processing potentially identifying Users (more)
- Lack of User Control (more)

More on the Privacy Impact Assessment Process and Results

Reduction of Identification Risks

Consent / PIA & PbD / Risk Reduction / Identification Risks

The risk seriousness and likelihood that TeleComAB could identify users and their social network usage profile based on the provided data are reduced from "Important" to "Negligible".

There are small (negligible) risks remaining that personal data could be inferred from the calculated statistics.

Figure 16 User Interfaces showing results of a conducted PIA in regard to the reduction of risks and remaining risks.

3.4.2.4 First Results

In this section, we summarise the main findings of our validation studies for each research question based on notes taken during the study and the recordings. The reader should note that these are first results based on notes taken and discussed after the studies. In parallel, we are also transcribing all recordings for a more in-depth follow-up analysis to be presented in an upcoming follow-up publication. Still, the results reported below were already eminent and clear based on the notes and observations from the studies and present interesting findings, which allows us to derive conclusions for future improvements of our data subject tools and our future work as presented and discussed below.

a) Results for RQ1

The individual walkthroughs of the mock-ups showed how far participants were interested in the PIA results and information about the Privacy by Design approach. Five of the six crypto-expert participants clicked on the link "More on TelecomAB's Privacy Impact Assessment and Privacy by Design approach" on the top layer and on the links on the subsequent layers – only one crypto-expert participant clicked directly "Cancel" on the top layer screen, with the stated reason that they would usually not participate in a study that pays for receiving user data. In contrast, non-crypto-expert participants (mostly) clicked directly on "Cancel" or "Consent" without showing interest in the information on the PIA and privacy by Design approach (only two out of seven).

They stated that they do usually not click on links for more policy information, as they avoid reading the long and complex text that they would expect to receive.

Hence, crypto-expert participants clearly showed more interest in the information about the PIA and privacy by design approach, and thus in our data subject tools, than non-crypto-expert participants.

b) Results for RQ2

Preference in terms of verbal metaphors in functional explanation:

We asked the focus group participants for their preferences of terms that should be meant for the general public/ different users to mediate that aggregated user data are protected by encryption: the verbal metaphors “securely encoded” and “securely protected” or the technically accurate term “securely encrypted”.

In FG1 (non-crypto experts), the verbal metaphor “securely protected” was agreed to be the preferred term – The metaphor “encoded” could be misunderstood, as it is also e.g. used for movie encoding and in that case the data is not confidentiality-protected, while they assumed that many lay users would not understand the technical term “encrypted”.

Participants of FG2 (crypto-experts) stated that for lay users, “protected” is a better term, even though “encrypted” is the accurate term. They thought that “aggregated” was a too difficult word for end users. The term “securely” made a rather suspicious impression to them, as the term “protected” should already comprise “secure”.

In FG3 (non-crypto experts), participants did not trust the term “protected” and preferred the exact technical term “encrypted”, which was to their opinion the professional term to use – Terms such as “aggregated” and “encrypted” should however include links that provide easy-to-understand definitions on another layer, such as the example provided in the study “That TelecomAB cannot read/access the user data in “clear text”. The information is first “summarized” then concealed by altering it so that it appears to be random data, e.g. “Password” is concealed as ““&t#dFF01”.". They also mentioned technical terms could be better represented with videos or links to a “Wikipedia” page if they need to access such details.

In FG4 (crypto experts), two participants preferred “encoded” as a suitable term for lay users. One thought that “encrypted” is too specific, and “protected” to be less suitable. The second thought that “encrypted” could be misleading and was not fond of the use of “securely” with “encoded”. However, the third member of FG4 favored the term “encrypted”, pointing out that the term is increasingly used by tools, such as WhatsApp, which lay users use, and that encoding does not necessarily comprise protection.

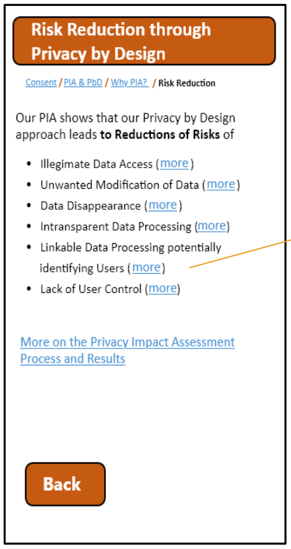
Suggested alternatives for verbal metaphors:

When asked for alternative verbal metaphors for “aggregated and securely encrypted” data, some of the participants provided suggestions including the following two suggestions by crypto-expert participants:

- “Unreadable data mixed with other users’ unreadable data. But can still have meaningful statistical information”
- “We are only collecting data that you agreed to share and they are not kept in clear, but more like a random sequence of character”.

Functional vs. structural explanations/metaphors:

Participants were asked whether they preferred the functional explanation (see **Error! Reference source not found.**) or the structural explanation ( ) for functional encryption.



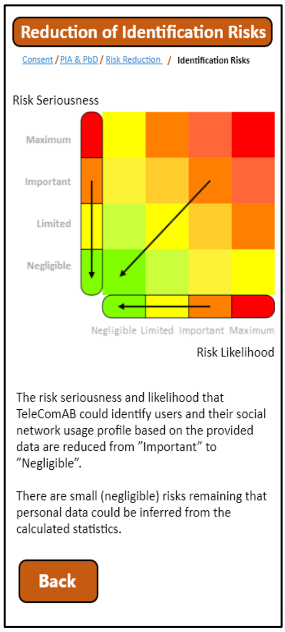
Risk Reduction through Privacy by Design

Consent / PIA & PbD / Why PIA? / Risk Reduction

Our PIA shows that our Privacy by Design approach leads **to Reductions of Risks** of

- Illegimate Data Access (more)
- Unwanted Modification of Data (more)
- Data Disappearance (more)
- Intransparent Data Processing (more)
- Linkable Data Processing potentially identifying Users (more)
- Lack of User Control (more)

More on the Privacy Impact Assessment Process and Results



Reduction of Identification Risks

Consent / PIA & PbD / Risk Reduction / Identification Risks

The risk seriousness and likelihood that TeleComAB could identify users and their social network usage profile based on the provided data are reduced from ”Important” to ”Negligible”.

There are small (negligible) risks remaining that personal data could be inferred from the calculated statistics.

One participant in FG3, two in FG1, and all participants (crypto-experts) in FG2 and FG4 stated that they preferred the structural explanations.

The graphical explanations and structure in six steps of the structural explanation was appreciated. They stated that it was in principle well understandable.

Crypto-expert participants appreciated the more technical details provided by the structural explanation. They would in any case like to have a more technical structural description of how the Privacy by Design approach works. One member in FG2 stated that it is beneficial to have both – a high level functional description plus a more detailed structural one – like diagnosis descriptions given by medical doctors to patients both in a high-level descriptive form and in a form using the exact medical terms.

In contrast, the most participants in FG3 were not interested in the structural explanation. Instead, the functional should be more to the point and address all their protection needs, e.g. also clearly state whether or how far the anonymity of users can be protected. To this end, a short video instead of the scrollable UI with the structural description would be preferred.

Comprehension and recall of explanations:

In the end, the focus group participants were asked questions for validating how far they understood and could recall the functional or structural explanations for functional encryption in the selected scenario.

In regard to the inquiry about whether anyone can decrypt or access the data that the users send, none of the participants in FG1 understood or could recall the protection properties of functional encryption. When reflecting on their answers, they stated that they simply thought that for conducting the data analysis the data must be available in clear text for TelecomAB.

However, all participants in FG2 responded to the protection properties correctly while reflecting on the structural descriptions provided.

In FG3, one participant understood it correctly, while two provided the wrong answer. When reflecting on the wrong answer, they stated that they anyhow would not trust the explanations that were made.

In FG4, two participants understood it correctly, while one assumed that the decryption key was sent by the user to TelecomAB for enabling the statistical analysis. The two participants that answered correctly stated that the structural explanation rather than the functional explanation was contributing to their understandings.

c) Results for RQ3

The risk artefacts presenting PIA results in terms of risk reductions and residual risks were differently perceived.

Participants of FG1 found the risk matrix confusing, as the arrows on the x/y axes point into the opposite directions than they commonly point in mathematical graphs.

Participants in FG2 liked the statement of remaining risks, but perceived the matrix as such not as useful.

Participants in FG3 found the information provided by the matrix and text not convincing enough – They requested details and information on what it means and additional assurance including information on who validated the PIA. One participant emphasized the need to show how the risks are being reduced, and not just the graph presenting the reduction of risks.

Two participants in FG4 stated that terms such as *risk seriousness* and *risk likelihood* used in the UI were confusing/unclear and needed to be defined. In contrast, one participant in FG4 thought that the matrix was similar to standard risk analysis result outputs and thus easy to grasp, however information why a risk reduction occurs and what controls contributed to the reduction could be added.

d) Results of RQ4

Almost all participants articulated different preferences in terms of incentives for participating in a study.

Vouchers or financial compensation was not considered as a strong incentive, even though some stated that it could be still justified to be reimbursed, especially if the study provider benefits financially. Many thoughts that a service or subscription related to TelecomAB is a more suitable incentive.

In general, the participants thought they would be more willing to share data if it is clear which data and what the study will result in, especially if there is a broad societal benefit from the data collection, e.g. if used for city planning.

Important incentives mentioned targeted sustainability goals and help for COVID-19 tracing. In addition, access to study results/ research data was also seen as important as well as an incentive to participate.

3.4.2.5 Discussion & Conclusions

The main results and their implications can be briefly summarised as follows:

Participants with no crypto expertise showed initially little interest in the data subject tools for explaining the Privacy by Design approach and PIA results (PAPAYA data subject tools) – but crypto expert participant showed interest by clicking on all links. This means that the transparency, provided by the information of PAPAYA data subject tools, mainly addresses the information-interests of crypto-expert users, while remaining a challenge to raise the interest of non-crypto expert/lay users.

Both functional and structural explanations are relevant to address different types of users (crypto and non-crypto expert users) – but need to be complemented. Crypto-expert participants request details of the technical functions with a preference of structural information explanation, which helps them to form mental models and build trust. Alternatively, non-crypto participants prefer shorter direct explanations. However, evoking the correct mental models and trust of non-crypto experts remains a challenge. Even when most non-crypto expert participants read the functional and structural explanations, stating that TelecomAB could not access the user data in clear text, they still assumed that TelecomAB could have access in order to calculate the statistics. However, for the crypto-expert participants the explanation was sufficient, as some stated that the structural explanation was the main contributor to their (correct) understanding.

Non-crypto expert participants highlighted the need for showing whether anonymity is ensured. Therefore, the functional explanation should be extended to state how far user anonymity is protected. It should be considered to use the technical terms “aggregated” and “encrypted” with links providing easy explanations of these terms for lay users. In addition, some of the alternative verbal metaphors suggested by study participants are worthwhile to test in another user study.

The risk matrix illustrations and used terms for illustrating risk reductions need improvements. The information about remaining risks was however appreciated. In addition, more details explaining how and why risks were reduced via functional encryption as well as additional information for increasing assurance of the PIA results could be added – these findings are partly in line with our previous research results [12].

Incentives contributing to broad societal benefits and sustainability goals as well as open research results and open research data can be important incentives for participating in studies.

4 UC5: Threat detection

In this chapter we present the validation activities carried out for the third use case in the Telecom scenario, namely, the *Threat detection* one.

4.1 Use case description in a nutshell

Orange designed an AI algorithm based on neural networks to detect malicious traffic on a company network. To put the model in practice into a product, the two basic and most widespread solutions have major drawbacks. One first solution is to send the traffic data to the server, so that the latter can execute its model on them. But this is not a viable solution since the internal network traffic of a company is a very sensitive information. That’s why another solution is to put the model on client’ servers. But this is also not acceptable since we would lose the control of the model, which one took months to be developed. Putting it on client’ side is to take the risk of it being stolen or retro-engineered by the client or an attacker against the latter.

This is why we introduced the idea of using the PAPAYA platform: it permits us to come up with a third option which seems to answer the issues of the two above solutions. In this scenario, the model is hosted on Orange servers. Through a frontend on client’ side, the traffic is encrypted with homomorphic encryption and sent to Orange server. Orange uses PAPAYA PETs to evaluate the network directly on encrypted data and send the encrypted result directly to the client. Hence, the model remains in Orange premises, remaining protected, and the sensitive traffic data from the client company is protected through encryption, and yet Orange does not learn anything about it.

Contrary to what was described in D2.1 [1], we no more consider the research phase where a new neural network is trained using some data coming from customers. Then, no contributing customer is now implied in UC5. In the sequel of this document, we then only consider a Third Party Customer, acting as a Client described above.

4.2 Use cases specification validation

In this section we validate the implementation against the use case definition specified in Deliverable D2.1 [1].

4.2.1 Coverage of use cases

In the following we present the coverage Table 13 for the use cases presented in Deliverable D2.1 [1].

Table 13: Coverage of use cases related to "Privacy-preserving smartphone usage analytics"

Use case:	Status:
PRE-1 Client and Orange have a contractual business relationship in which Orange offers a service and the Client pay for this service to obtain threat detection insights.	DONE
PRE-2 CCs and Orange have a contractual business relationship in which Orange improves its anomaly detection model based on CCs' data.	N/A since we no more consider the research phase, compare to D2.1 [1], see Section 6.1.
PRE-3 Orange runs an instance of the PAPAYA service for threat detection on the PAPAYA platform.	DONE
PRE-4 The Client runs an instance of the PAPAYA client-side agent.	DONE
POST-1 Orange prepares a report that gives the results of the threat detection procedure and sends it to the requesting Client.	DONE

4.2.2 Integration with PAPAYA platform

In this section we describe the integration activities performed in task T5.2. Firstly, we list the PAPAYA components that were used (and thus, integrated) for UC5. Then, we present an architectural view of the integrated solution.

4.2.2.1 Integrated PAPAYA components

As described above and in Deliverable D2.1 [1], Table 14 lists the PAPAYA tool we integrated for this use case.

Table 14: Integrated PAPAYA component for "Threat detection"

PAPAYA components:	UC4 status:

PP NN Classification (HE)	Module that implements the inference of a neural network using homomorphic encryption	DONE

4.2.2.2 Integrated architecture

As reported in Section 6.1, the solution is structured in the following way:

- the Orange backend is used to evaluate the neural network on the encrypted data using PAPAYA PP secure neural network inference module;
- the frontend application is hosted on the client' side. It oversees the encryption of the data, sends it to the PAPAYA platform, and decrypts the result whence it receives it.

Error! Reference source not found. shows the architectural representation of the integrated PAPAYA solution. The details on the way to use this part of the PAPAYA platform is given in Deliverable D4.3 [13].

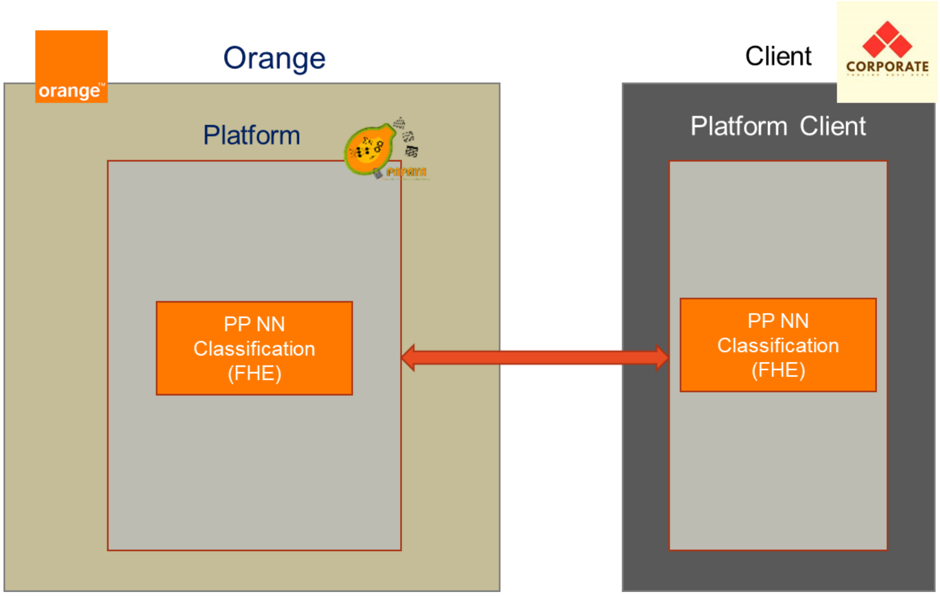


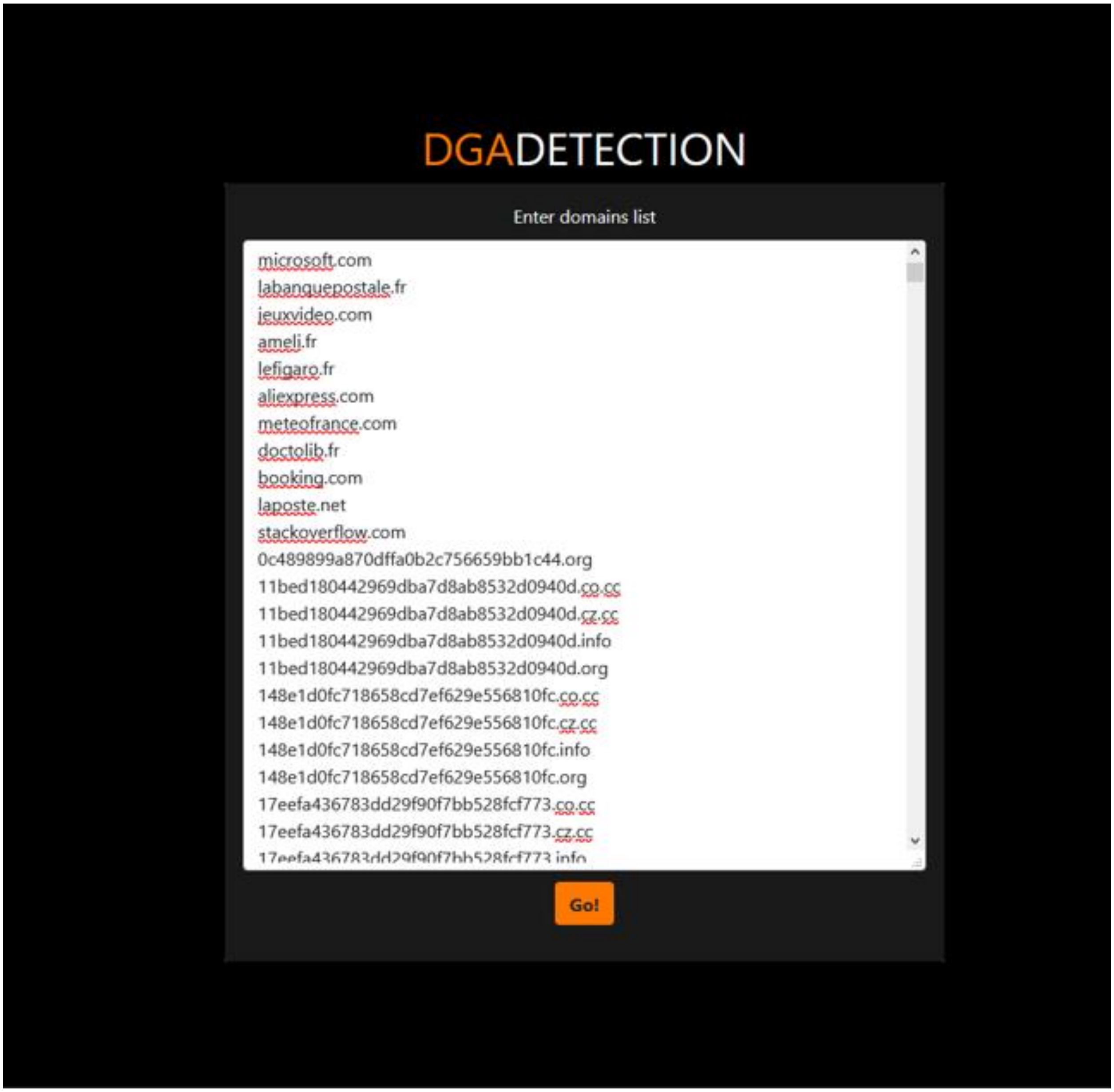
Figure 17 Architecture of the implementation of the threat detection use case

4.2.3 Applications implementation: interfaces

The client agent provides two means of interaction, a REST API and a visual interface. First, let us start with the visual interface. The Figure 18 shows the form on the client application. The user enters a list of at most 4095 website addresses that he wants to be classified. By clicking on *Go* the data is encrypted and sent to the server. The results page is shown in Figure 19. This page provides the probability for a given address to be malicious, and the result of the classification.

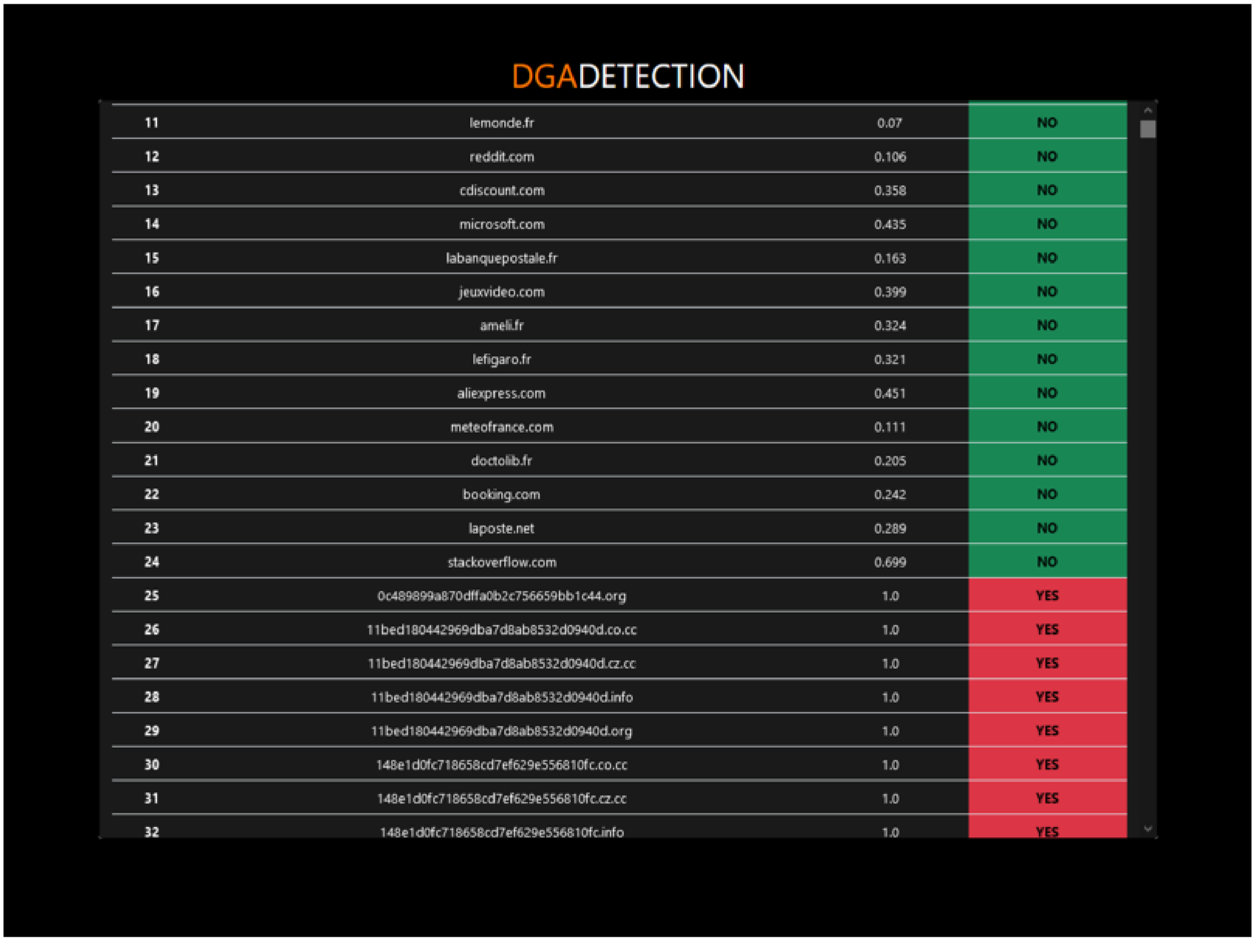
The client agent also provides a REST API that takes as input a list of addresses to classify. The results are sent as a response formatted as a JSON file. The REST API provides the same information as the visual interface, but it provides a means for the agent to be called upon with a programming language.

A video presenting the whole system is also available in this deliverable (available in the PAPAYA website).



microsoft.com
labanquepostale.fr
jeuxvideo.com
ameli.fr
lefigaro.fr
aliexpress.com
meteofrance.com
doctolib.fr
booking.com
laposte.net
stackoverflow.com
0c489899a870dffa0b2c756659bb1c44.org
11bed180442969dba7d8ab8532d0940d.co.cc
11bed180442969dba7d8ab8532d0940d.cz.cc
11bed180442969dba7d8ab8532d0940d.info
11bed180442969dba7d8ab8532d0940d.org
148e1d0fc718658cd7ef629e556810fc.co.cc
148e1d0fc718658cd7ef629e556810fc.cz.cc
148e1d0fc718658cd7ef629e556810fc.info
148e1d0fc718658cd7ef629e556810fc.org
17eefa436783dd29f90f7bb528fcf773.co.cc
17eefa436783dd29f90f7bb528fcf773.cz.cc
17eefa436783dd29f90f7bb528fcf773.info

Figure 18 Form to enter a list of web addresses to be classified



DGADETECTION

11	lemonde.fr	0.07	NO
12	reddit.com	0.106	NO
13	cdiscount.com	0.358	NO
14	microsoft.com	0.435	NO
15	labanquepostale.fr	0.163	NO
16	jeuxvideo.com	0.399	NO
17	ameli.fr	0.324	NO
18	lefigaro.fr	0.321	NO
19	aliexpress.com	0.451	NO
20	meteofrance.com	0.111	NO
21	doctolib.fr	0.205	NO
22	booking.com	0.242	NO
23	laposte.net	0.289	NO
24	stackoverflow.com	0.699	NO
25	0c489899a870dffa0b2c756659bb1c44.org	1.0	YES
26	11bed180442969dba7d8ab8532d0940d.co.cc	1.0	YES
27	11bed180442969dba7d8ab8532d0940d.cz.cc	1.0	YES
28	11bed180442969dba7d8ab8532d0940d.info	1.0	YES
29	11bed180442969dba7d8ab8532d0940d.org	1.0	YES
30	148e1d0fc718658cd7ef629e556810fc.co.cc	1.0	YES
31	148e1d0fc718658cd7ef629e556810fc.cz.cc	1.0	YES
32	148e1d0fc718658cd7ef629e556810fc.info	1.0	YES

Figure 19 Interface showing the results of the detection.

4.3 Requirements validation

The validation of the data privacy requirements is presented in Table 15.

Table 15: Coverage of the data security requirements for "threat detection"

ID:	Use case:	Status:	Comment:
Orange cannot get any information on TPC data.	UC5	DONE	Orange only manipulates the traffic data in an encrypted form.
TCP cannot get any information on Orange model	UC5	DONE	The model never goes outside Orange premises.

4.4 Validation by stakeholders

During internal remote meetings, we presented the current implementation, and related benchmarks, to the stakeholders inside Orange (Orange Cyber Defence team and some other research teams inside Orange Labs). The ability to protect the data and the model were very well received as this is a real need they have. Indeed, some of their potential customers are reluctant since they have to send sensitive information to Orange. However, the modifications made to the model, to be compatible with homomorphic encryption, led to a significant decrease of the accuracy. We are currently working on a new version of this model to solve this issue but this will not be ready before the end of the project as we need several months for that.

5 Conclusion

This document described the evaluation of the PAPAYA telecom use cases: privacy-preserving mobility analytics (UC3), privacy-preserving mobile usage statistics (UC4), and a threat detection system (UC5). This validation has been done by using several means. For each use case, we have first proven that the validated properties are adequate with the initial specifications of the use cases (as defined in Deliverable D2.1 [1]). We have then shown their adequacy with the general and specific PAPAYA requirements as defined in Deliverable D2.2 [2]. Finally, we have given some inputs coming from identified stakeholders: individuals (especially for UC4), public authorities (e.g. CNIL for UC3 and UC4) and potential commercial partners and clients (for UC5).

This PAPAYA evaluation and validation process showed fair maturity and performance levels for PAPAYA components and platform, with novel privacy-preserving elements that begin to be adopted even in the leading market solutions.

In this deliverable we showed that the PAPAYA components give the way to reach the objectives set at the start of the project for real-life applications in the telecom world: process high volume of data through various methods (counting, clustering, neural network), management of a multiplicity of data sources (single or multiple), being compliant with the GDPR regarding individuals’ data protection for multiple legal basis (user consent, real time anonymization / encryption).

References

[1] M. Mosconi, E. Ciceri, S. Galliani, M. Azraoui, S. Canard, D. Le Hello, A. Palomares Perez och M. Önen, *D2.1 Use Case Specification,* 2019.

[2] S. Fischer-Hübner, B. Kane, J. S. Pettersson, T. Pulls, L. Iwaya, L. Fritsch, B. Rozenberg, R. Shmelkin, A. Palomares Perez, N. Ituarte Aranda och J. Carlos, *D2.2 - Requirements Specification,* 2019.

[3] J.-G. Lee, J. Han och K.-Y. Whang, ”Trajectory clustering: A partition-and-group framework,” i *SIGMOD*, 2007.

[4] T. Bohman, C. Cooper och A. M. Frieze, ”Min-wise independent linear permutations,” *. Electr. J. Comb.,* 2000.

[5] S. Canard, B. Vialla, B. Bozdemir, O. Ermis, M. Önen, M. Barham, B. Rozenberg, R. Shmelkin, I. Adir och R. Masalha, *D3.3 - Complete Specification and Implementation of Privacy preserving Data Analytics,* 2020.

[6] B. Rozenberg, R. Shmelkin, B. Bozdemir, O. Ermis, M. Önen, M. Barham, M. Azraoui, S. Canard, B. Vialla och T. Pulls, *D4.2 - Progress report on platform implementation and PETs integration,* 2020.

[7] S. Canard, N. Desmoulins, S. Hallay, A. Hamdi och D. Le Hello, ”WeStat: a Privacy-Preserving Mobile Data Usage Statistics System.,” i *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics (IWSPA)*, 2021.

[8] S. Fischer-Hübner, M. T. Beckerle, J. S. Pettersson och P. Murmann, *D3.4 - Transparent Privacy preserving Data Analytics,* 2020.

[9] W. Bai, M. Pearson, P. G. Kelley och M. L. Mazurek, ”Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study,” i *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020.

[10] A. Demjaha, J. M. Spring, I. Becker, S. Parkin och M. A. Sasse, ”Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption.,” i *USEC*, 2018.

[11] A. Alaqra, S. Fischer-Hübner och F. E. , ”Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of

perspectives by medical professionals and patients,” i *Journal of medical Internet Reserach (JMIR)*, 2018.

[12] A. Alaqra, E. Ciceri, S. Fischer-Hübner, B. Kane, M. Mosconi och S. Vicini, ”Using PAPAYA for eHealth-Use Case Analysis and Requirements.,” i *IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)*, 2020.

[13] B. Rozenberg, R. Shmelkin, B. Bozdemir, O. Ermis, M. Önen, S. Canard, B. Vialla och T. Pulls, *D4.3 Final report on platform implementation and PETs integration,* 2021.

[14] B. Schneiderman, C. Plaisant, M. Cohen and S. Jacobs, Designing the User Interface: Strategies for Effective Human-Computer Interaction (6th ed.), New York: Pearson., 2016.

[15] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Seattle, Washington, USA, 1990.

[16] P. Stanley, ”Designing for accessibility is not that hard,” 2019. [Online]. Available: https://uxdesign.cc/designing-for-accessibility-is-not-that-hard-c04cc4779d94.

Appendix 1 Usability principles

We here give the list of usability principles for fulfilling C.EUR.HCI.1 as specified in [PAPAYA D2.2]. As written there, the principles are derived from the heuristics of Ben Schneiderman [14], Jakob Nielsen and Rolf Molich [15], and Stanley [16], which are regarded as broad principles in the design of technology and technological devices. The principles overlap each other and are summarised in the list below, along with some principles for accessibility

- Visibility of System Status
- Match between the system and the real world
- User control and freedom
- Consistency and standards
- Error Prevention
- Recognition rather than recall
- Flexibility and efficiency of use
- Aesthetic and minimalist design
- Help users to recognise, diagnose, and recover* from errors
- Help and documentation
- Enable frequent users to use shortcuts
- Offer informative feedback
- Design dialogue to yield closure
- Reduce short-term memory load
- Add enough colour contrast
- Do not use colour alone to make critical information understandable

Appendix 2 Consent form for KAU study participation

Here is the consent that was used by KAU during its interactions with users to validate UC4.

Consent form

I consent to participate in the study:
PAPAYA – Evaluation of user interfaces

I have been informed orally and in writing about this study and have had the possibility to put questions. I am allowed to keep the written information. I am aware of the fact that my participation is completely voluntary and that I can withdraw it at any time, without having to give any reason for doing so.

My signature below signifies that:
☐ I consent to participate in this study;
☐ I consent that the session can be audio and screen recorded;
☐ I consent to Karlstad University processing my personal data in accordance to GDPR and the information provided.

....
Signature

....	....
Clarification of signature	Location and date

Contact persons responsible for the research:

Prof. Dr. Simone Fischer-Hübner (simone.fischer-huebner@kau.se),
Prof. Dr. John Sören Pettersson (john_soren.pettersson@kau.se),
Ala Sarah Alaqra (as.alaqra@kau.se).
Karlstad University, Universitetsgatan 2, 65188 Karlstad, Sweden

Information about the study:
PAPAYA — Evaluation of user interfaces

Thanks for your interest to participate in a study by the EU H2020 PAPAYA project on “Platform for privacy preserving data analytics” conducted by Karlstad University (KAU).

The purpose of this study is to evaluate user interface mockups explaining how privacy-preserving data analysis is working with platforms developed in the project. Due to the pandemic, the session we invite you to participate in will be conducted remotely with the aid of a videoconferencing system.

In the videoconference session you will be asked to:

- Inspect and “walk through” some user interface mockups
- Give your opinion of the user interface and answer some questions while
- you use it
- Fill in a questionnaire
- Explain your general understanding of the content shown and your
- perception of the user interface mockups.
- Discuss with other participants your opinions and understanding of
- concepts and elements of the interface

If you give permission, the session will be audio and screen recorded. During the evaluation, we ask you to answer in general terms and not to reveal any sensitive personal data, such as data related to your personal health or stress situation. If any sensitive personally identifying data are stated by you during the interviews, we will interrupt and ask you to stop revealing such information, and we will not take any notes on that part and immediately delete any recording of that part of the session.

Participation in this evaluation as well as allowing recording are completely voluntary. Data will be collected and processed in compliance with the EU General Data Protection Regulation (GDPR) and no sensitive personal data will be asked or processed.

How your data will be processed

All your data including the notes and any recording that we take will be kept confidential, stored safely in a locked filing cabinet or on an encrypted partition of a computer hard drive, transcribed, pseudonymised as soon as possible and deleted after the archiving period of 10 years (required by Karlstad University for all original research data for preventing/detecting research fraud). The list matching participants’ names to pseudonyms will be kept separately from all other collected data at a secure place.

Karlstad University is the personal data controller. According to The General Data Protection Regulation, GDPR, you have the right to access all your data that has been collected without cost, and if needed have any errors corrected. You also have a right to ask for the deletion or limitation of the data, and to object to the processing of the data. It is possible to send a complaint to the Swedish Data Protection Authority. The contact information of the data protection officer at Karlstad University is dpo@kau.se.

Contact

Data controller:
Karlstad University, Universitetsgatan 2, 65188 Karlstad, Sweden (dpo@kau.se).

Contact persons responsible for the research:

Prof. Dr. **Simone Fischer-Hübner** (simone.fischer-huebner@kau.se),
Prof. Dr. **John Sören Pettersson** (john_soren.pettersson@kau.se),
Ala Sarah Alaqra (as.alaqra@kau.se).
Karlstad University, Universitetsgatan 2, 65188 Karlstad, Sweden.

Appendix 3 Study guide

We now give some details about the study guide that was used during KAU study for UC4 user validation.

Pre-study correspondence

We send out invitation letters containing the objective and description of the study. We also provide the consent form so that the respondent familiarizes themselves with the content.

Study part 1: UI mockups walkthroughs

1on1 interviews via zoom with workshop participants where we show the UIs from the use case mockups. Thereafter we have a discussion with other participants in the form of focus groups.

Protocol:

We welcome the respondent and introduce the study and setup: zoom, UI mockups links, and agenda of the study.

Introduction:

“Introduce myself and colleagues” Go around with pseudonym option, pronoun round.

“Welcome and thank you for participating in this study by the EU H2020 PAPAYA project which stands for “Platform for privacy preserving data analytics” conducted by Karlstad University (KAU). The purpose of this study is to evaluate user interface mockups explaining how privacy-preserving data analysis is working with the PAPAYA platforms developed in the project. We are interested in your opinions/perspectives; there are no right or wrong answers so feel free to express yourself in this study. All responses are voluntary.”

Agenda:

“This study will take approximately 2 hours in total to complete. There will be two parts:

Part1, which will be in parallel sessions: individual short UI walkthrough: we will show you UI mockups for the walkthrough, and then discuss with you few questions about your opinions and concerns.

--Screen sharing portion of the screen consent.

Part2, focus group workshop: a structured discussion with few other participants about opinions and perceptions of UI, consent, incentives, functionality, and mental models.”

Questions?

-------------*BREAKOUT ROOMS*-------------

Use case introduction:

"In this study, we have a use case, where a Telecom provider called TelecomAB, which offers a service in their application. In this service, app users are asked if they would participate and contribute their personal user data for a statistical survey. The data should be protected by PAPAYA's Privacy by Design approach."

UI-mockup walkthrough:

We present the task to walkthrough the mockups, no interference of the moderator (the respondent goes through and the moderator observes and takes notes of parts clicked on).

"We will begin with UI walkthrough. Could you please open your browser and share your screen.

I will send you a link, and when we say start, you can take your time to observe and walkthrough the user interfaces until you reach an end. I will remain a silent observer and not interfere until this part is over. Then we will discuss the walkthrough.

"We shall now begin the recording, does everyone consent to the study?"

Click on the link in the chat:

https://xd.adobe.com/view/63d65c42-dcc1-4312-b8b1-f034c5895a83-3685/?fullscreen&hints=off

You may now begin"

Test is over when they either click on "cancel" or "consent".

(*UI discussion*) the moderator intervenes and goes through the UI mockups and asks:

"Now we would like to discuss: why did you not click on some parts and if there was anything unclear (the following)?

Page 1: consent form for participating in a study

a. More on TeleComAB's Privacy Impact Assessment and Privacy by Design approach

Page 2:(PIA & PbD): How does it work?

b. How are Privacy Risks reduced by our Privacy by design approach

Page 3 (Risk Reduction):

c. Illegitimate Data Access (more)
d. Linkable Data Processing potentially Identifying Users (more)

(a short 5 min break to collect respondents into a group in zoom, phone tablet at hand. back to main room at ~15.35)

Study part 2: focus groups discussions

We welcome the group and introduce the format of the focus groups discussion

Introduction:

“Welcome back. We now begin the second part of the study, focus group workshop. We will have a structured discussion with few other participants about your opinions and perceptions of UI, consent, incentives, functionality, and mental models.”

Setup:

“Please mute yourself when not speaking, and use the chat for making comments or raise your hand if you would like to go next in the open discussion. First, we would like you to introduce yourselves to each other: first name and pseudonym if you would like to refrain from using your name. We can do a go around to test the sound.”

Go around of introductions

Mentimeter and discussion: (share screen mentimeter)

“Will be using Mentimeter during our discussion, you can find the link in the chat:

Menti.com

Or if you want to use your phone, you can enter the code:

Pilot questions:

See mentimeter..

Incentives questions:

“Now on mentimeter post your answers to the following questions:

S1: Would you generally contribute to participating your data in this UC?

S2: Would you consent to participating your data if offered a discount on your subscription or in this case, Amazon voucher?

S3: What offers/incentives would motivate you to consent? (you can submit multiple times: 2 minutes) ”

Discussion of the incentives on mentimeter:

“Which of the following incentives do you agree to? We now go around starting with…”

(go arounds)

“Which of the following incentives you do not agree to? We now go around starting with…”

(go arounds)

S4: “Which of the following do you consider a benefit to you to share your data: you rank the options from 1st , most significant, to 4th:

- Sustainability and environmental purposes
- City planning and public transport
- Tracking of COVID19 cases
- Discounts and Vouchers”

Descriptions and mental models:

S5: “Which of the following terms do you think is most suitable for mediating (to different types of users) That TelecomAB cannot read/access the user data in “clear text”. The information is first “summarized” then concealed by altering it so that it appears to be random data, e.g. “Password” is concealed as ““&t#dFF01”:

“Aggregated and securely encoded data”

“Aggregated and securely encrypted data”

“Aggregated and securely protected data”

Next slide:

S6: What alternative descriptions do you think are suitable?

Now we go around and discuss why:

“Aggregated and securely encoded data” is suitable/not suitable?”

(go arounds)

“Aggregated and securely encrypted data” is suitable/not suitable?”

(go arounds)

“Aggregated and securely protected data” is suitable/not suitable?”

(go arounds)

“can you think of alternative descriptions?- keep in mind the general public: different type of users”

(go arounds)

Functionality: we share the link to the mockups again

“You can use the following link of the mockups UI as a reference in the discussion that follows:

https://xd.adobe.com/view/63d65c42-dcc1-4312-b8b1-f034c5895a83-3685/?fullscreen&hints=off”

but first we take 5 minutes break”

------5 minutes break-----

See the following description of privacy functionality:

S7: “Our Privacy by Design approach ensures that your data will only be sent to us and statistically analysed by us in aggregated and securely encoded form.

We will not be able to decode your data and can only to derive statistics from your and other users’ data.”

- What are your thoughts on the description?
- Is the explanation well understood?
- Is there anything missing?”

(go arounds)

S8: “See the following description of functional encryption:

- What are your thoughts on the description?
- Is the explanation well understood?
- Is there anything missing?”

(go arounds)

S9: “Which description do you prefer?”

Why and comments

(go arounds)

S10: “What are your thought on the presentation of the risks? What do you understand from the visualization?”

- Is there anything missing?

(go arounds)

Questions on comprehension:

S11: “From the data that the user contributes to the study, do you think that TeleComAB can directly see the user’s social network usage information? Yes, no, not sure

(give few minutes to answer)

We can go around and say why do you think so?”

(go arounds)

(answer: No)

S12: Which data do you think is [securely encoded]:

a. the data sent by the user to TelecomAB,
b. the statistical analysis result that TelecomAB produces
c. both
d. none (answer: (a))

(give few minutes to answer)

We can go around and say why do you think so?

(go arounds)

S13a: “Who do you think can de-code/decrypt/access the data that user sends in clear text

(a) TelecomAB,
(b) MediaSurvey Cooperation that requests the result
(c) both
(d) none of them (answer: (d)).”

We can go around and say why do you think so?

(go arounds)

S13b: “now that you can see the description, does it change your answer? Who do you think can de-code/decrypt/access the data that user sends in clear text

(a) TelecomAB,
(b) MediaSurvey Cooperation that requests the result
(c) both
(d) none of them (answer: (d)).”

We can go around and say why do you think so?

Study part 3: questionnaire

The respondent is asked to fill out the demographics questionnaire.

The respondent is thanked and provided with information about the study’s dissemination.

“Thank you for your participation. Please input your name and email address so that we send you the confirmed as a thank you, we would like to offer you a voucher as a token of our gratitude.”

References

[1] M. Mosconi, E. Ciceri, S. Galliani, M. Azraoui, S. Canard, D. Le Hello, A. Palomares Perez and M. Önen, *D2.1 Use Case Specification,* 2019.

[2] S. Fischer-Hübner, B. Kane, J. S. Pettersson, T. Pulls, L. Iwaya, L. Fritsch, B. Rozenberg, R. Shmelkin, A. Palomares Perez, N. Ituarte Aranda and J. Carlos, *D2.2 - Requirements Specification,* 2019.

[3] J.-G. Lee, J. Han and K.-Y. Whang, "Trajectory clustering: A partition-and-group framework," in *SIGMOD*, 2007.

[4] T. Bohman, C. Cooper and A. M. Frieze, "Min-wise independent linear permutations," *. Electr. J. Comb.,* 2000.

[5] S. Canard, B. Vialla, B. Bozdemir, O. Ermis, M. Önen, M. Barham, B. Rozenberg, R. Shmelkin, I. Adir and R. Masalha, *D3.3 - Complete Specification and Implementation of Privacy preserving Data Analytics,* 2020.

[6] B. Rozenberg, R. Shmelkin, B. Bozdemir, O. Ermis, M. Önen, M. Barham, M. Azraoui, S. Canard, B. Vialla and T. Pulls, *D4.2 - Progress report on platform implementation and PETs integration,* 2020.

[7] S. Canard, N. Desmoulins, S. Hallay, A. Hamdi and D. Le Hello, "WeStat: a Privacy-Preserving Mobile Data Usage Statistics System.," in *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics (IWSPA)*, 2021.

[8] S. Fischer-Hübner, M. T. Beckerle, J. S. Pettersson and P. Murmann, *D3.4 - Transparent Privacy preserving Data Analytics,* 2020.

[9] W. Bai, M. Pearson, P. G. Kelley and M. L. Mazurek, "Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2020.

[10] A. Demjaha, J. M. Spring, I. Becker, S. Parkin and M. A. Sasse, "Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption.," in *USEC*, 2018.

[11] A. Alaqra, S. Fischer-Hübner and F. E. , "Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of

perspectives by medical professionals and patients," in *Journal of medical Internet Reserach (JMIR)*, 2018.

[12] A. Alaqra, E. Ciceri, S. Fischer-Hübner, B. Kane, M. Mosconi and S. Vicini, "Using PAPAYA for eHealth-Use Case Analysis and Requirements.," in *IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)*, 2020.

[13] B. Rozenberg, R. Shmelkin, B. Bozdemir, O. Ermis, M. Önen, S. Canard, B. Vialla and T. Pulls, *D4.3 Final report on platform implementation and PETs integration,* 2021.

[14] B. Schneiderman, C. Plaisant, M. Cohen and S. Jacobs, Designing the User Interface: Strategies for Effective Human-Computer Interaction (6th ed.), New York: Pearson., 2016.

[15] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Seattle, Washington, USA, 1990.

[16] P. Stanley, "Designing for accessibility is not that hard," 2019. [Online]. Available: https://uxdesign.cc/designing-for-accessibility-is-not-that-hard-c04cc4779d94.