This deliverable has been written in the context of the Privacy Flag Horizon 2020 European research project, which is supported by the European Commission and the Swiss State Secretariat for Education, Research and Innovation. The opinions expressed and arguments employed do not engage the supporting parties.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT No.653426
Abstract

Privacy Flag combines crowd sourcing, ICT technology and legal expertise to protect citizen privacy when visiting websites, using smart-phone applications, or living in a smart city leveraging user friendly solutions provided as a smart phone application, a web browser add-on and a public website. It will:

1. Develop a highly scalable privacy monitoring and protection solution with:
   - Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks;
   - Privacy monitoring agents to identify suspicious activities and applications;
   - Universal Privacy Risk Area Assessment Tool (UPRAAT) and methodology tailored to European norms on personal data protection;
   - Personal Data Valuation mechanism;
   - Privacy enablers against traffic monitoring and finger printing;
   - User friendly interface informing about the privacy risks when using an application or website.

2. Develop a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including:
   - In-depth privacy risk analytical tool and services;
   - Voluntary legally binding mechanism for companies located outside of Europe to align with and abide to European standards in terms of personal data protection;
   - Services for companies interested in being privacy friendly;
   - Labelling and certification process.

3. Collaborate with standardization bodies and actively disseminate towards the public and specialized communities, such as ICT lawyers, policy makers and academics. Eleven (-11-) European partners, including SMEs and a large telco operator (OTE), bring their complementary technical, legal, societal and business expertise; Privacy-Flag intends to establish strong links with standardization bodies and international fora and it also intends to assess and incorporate; outcomes from over 20 related research projects will be built and ensure a long term sustainability and growth.
Executive Summary

This document provides an overview and the main outcomes of the work done on the Privacy Flag system architecture design in WP1 during the first year (Y1) of the project. WP1 focused first on definition of use cases and respective requirements, based on the requirements identified and documented in the previously submitted deliverable D1.1 in fact, the work in WP1 has been continued by performing analysis of the requirements and design of the initial version of the Privacy Flag architecture. This architecture will serve as the “basis and framework” for all other technical activities in the full context of the project. It will be updated at the end of year 2 (Y2) and also at the end of the project (Y3), by taking into account outcomes of other technical work packages.

Section 1 describes WP1 and T1.2 goals, deliverable’s D1.2 specific concept and dedicated purpose. It also provides “key remarks” on the work progress and correlation with task T1.1 and the deliverable D1.1 [2].

In Section 2, it is explained the methodology which is used for modeling the architecture of the Privacy Flag with explanation of functionalities of the Context Views, Functional Views and Information Views.

Then, Section 3 provides the corresponding architecture description by using the methodology explained in the previous section. Moreover, it specifies three general use-cases, that is: The Smartphone app, the Browser add-on and the Website, in more details, by offering the basis for modeling the related fundamental architecture. It also presents the services which are common across different use cases as well as the “interaction” between different functional components. In addition, Section 3 provides information about services from the involved Actors’ perspective(s) as well as a description of the Security and Privacy Requirements. Section 3 also includes information about the registration procedure, the risk assessment, the data access policies, the data value component as well as the subscription and anonymization services. The architecture interface and the design of the front-end (application) and the back-end of the Privacy Flag Platform, with the integration of the Application Subsystem and the Backend system, are given at the end of this section.

Finally, Section 4 summarizes the work and points out the “key issues” discussed in the document.
## Contributors

<table>
<thead>
<tr>
<th>First name</th>
<th>Last name</th>
<th>Partner</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nenad</td>
<td>Gligoric</td>
<td>DNET</td>
<td><a href="mailto:nenad.gligoric@dunavnet.eu">nenad.gligoric@dunavnet.eu</a></td>
</tr>
<tr>
<td>George</td>
<td>Mourikas</td>
<td>HWC</td>
<td><a href="mailto:george@hwcomms.com">george@hwcomms.com</a></td>
</tr>
<tr>
<td>Evangelos</td>
<td>Sfakianakis</td>
<td>OTE</td>
<td><a href="mailto:esfok@oteresearch.gr">esfok@oteresearch.gr</a></td>
</tr>
<tr>
<td>Ioannis</td>
<td>Chochliouros</td>
<td>OTE</td>
<td><a href="mailto:ichochliouros@oteresearch.gr">ichochliouros@oteresearch.gr</a></td>
</tr>
<tr>
<td>Andreas</td>
<td>Drakos</td>
<td>VELTI</td>
<td><a href="mailto:adrakos@velti.com">adrakos@velti.com</a></td>
</tr>
<tr>
<td>Vasileios</td>
<td>Vlachos</td>
<td>CTI</td>
<td><a href="mailto:vsvlachos@gmail.com">vsvlachos@gmail.com</a></td>
</tr>
<tr>
<td>Camilla</td>
<td>Bistolfi</td>
<td>IIP</td>
<td><a href="mailto:bistolfi@stitutoitalianoprivacy.it">bistolfi@stitutoitalianoprivacy.it</a></td>
</tr>
<tr>
<td>Fabian</td>
<td>Lanze</td>
<td>LU</td>
<td><a href="mailto:fabian.lanze@uni.lu">fabian.lanze@uni.lu</a></td>
</tr>
<tr>
<td>Ali</td>
<td>Padyab</td>
<td>LTU</td>
<td><a href="mailto:ali.padyab@ltu.se">ali.padyab@ltu.se</a></td>
</tr>
<tr>
<td>Sebastien</td>
<td>Ziegler</td>
<td>MI</td>
<td><a href="mailto:sziegler@mandint.org">sziegler@mandint.org</a></td>
</tr>
<tr>
<td>Ana Maria</td>
<td>Pacheco Huamani</td>
<td>AS</td>
<td><a href="mailto:ampacheco@archimede.ch">ampacheco@archimede.ch</a></td>
</tr>
<tr>
<td>Cedric</td>
<td>Crettaz</td>
<td>MI</td>
<td><a href="mailto:ccrettaz@mandint.org">ccrettaz@mandint.org</a></td>
</tr>
<tr>
<td>Michael</td>
<td>Hazan</td>
<td>MI</td>
<td><a href="mailto:nhazan@mandint.org">nhazan@mandint.org</a></td>
</tr>
</tbody>
</table>
# Glossary

<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARM</td>
<td>Architecture Reference Model</td>
</tr>
<tr>
<td>BAO</td>
<td>Browser Add-on</td>
</tr>
<tr>
<td>CE-PRAAS, CEPRASS</td>
<td>Controller Evaluation of its Privacy Risk Area Risk Assessment Service</td>
</tr>
<tr>
<td>CET</td>
<td>Crowdsourcing Evaluation Tool</td>
</tr>
<tr>
<td>CKD</td>
<td>Common Knowledge Database</td>
</tr>
<tr>
<td>CMS</td>
<td>Content Management System</td>
</tr>
<tr>
<td>DA</td>
<td>Distributed Agent</td>
</tr>
<tr>
<td>DB</td>
<td>Data Base</td>
</tr>
<tr>
<td>DoW</td>
<td>Description of Work</td>
</tr>
<tr>
<td>Dvt</td>
<td>Data Valuation tool</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FG</td>
<td>Functional Group</td>
</tr>
<tr>
<td>FP</td>
<td>Framework Programme</td>
</tr>
<tr>
<td>FP7</td>
<td>7th Framework Programme</td>
</tr>
<tr>
<td>GA</td>
<td>Grant Agreement</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ID, id</td>
<td>Identifier</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT-A</td>
<td>IoT Architecture</td>
</tr>
<tr>
<td>IP</td>
<td>Integrated Project</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation</td>
</tr>
<tr>
<td>MA</td>
<td>Monitoring Agent</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>PF</td>
<td>Privacy Flag</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small and Medium-sized Enterprises</td>
</tr>
<tr>
<td>ToC</td>
<td>Table of Contents</td>
</tr>
<tr>
<td>UC</td>
<td>Use Case</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modelling Language</td>
</tr>
<tr>
<td>UPRAAM</td>
<td>Universal Privacy Risk Area Assess Methodology</td>
</tr>
<tr>
<td>UPRAAT</td>
<td>Universal Privacy Risk Area Assessment Tool</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>VCT</td>
<td>Voluntary Compliance Commitment Tool</td>
</tr>
</tbody>
</table>
VE Virtual Entity
WP Work Package
Table of Contents

GLOSSARY ................................................................................................................................................. 6

TABLE OF CONTENTS .............................................................................................................................. 8

INTRODUCTION .......................................................................................................................................... 12
  1.1 PURPOSE AND SCOPE OF WP1 ........................................................................................................ 12
  1.2 PURPOSE AND SCOPE OF T1.2 ....................................................................................................... 12
  1.3 PURPOSE AND SCOPE OF THE CURRENT DOCUMENT .................................................................. 12

METHODOLOGY .......................................................................................................................................... 13
  2.1 CONTEXT VIEWS ................................................................................................................................. 13
  2.2 FUNCTIONAL VIEWS .......................................................................................................................... 13
  2.3 INFORMATION VIEWS ........................................................................................................................ 16

ARCHITECTURE ......................................................................................................................................... 17
  3.1 USE-CASES ........................................................................................................................................ 18
    3.1.1 Use case 1: Smartphone app ........................................................................................................ 19
    3.1.2 Use case 2: Browser add-on ....................................................................................................... 24
    3.1.3 Use case 3: Website ..................................................................................................................... 28
  3.2 SERVICES .......................................................................................................................................... 40
    3.2.1 Registration .................................................................................................................................. 40
    3.2.2 Data Valuation Tool ..................................................................................................................... 41
    3.2.3 Data access .................................................................................................................................. 42
    3.2.4 Data Value component ................................................................................................................ 43
    3.2.5 Subscription .................................................................................................................................. 44
    3.2.6 Anonymization service ................................................................................................................. 45
  3.3 INFORMATION VIEWS .......................................................................................................................... 46
    3.3.1 Top level information view .......................................................................................................... 46
    3.3.2 Smartphone application information view ................................................................................... 48
    3.3.3 Browser add-on information view ................................................................................................ 49
    3.3.4 Website information view .......................................................................................................... 50
    3.3.5 Security information view .......................................................................................................... 51
  3.4 ARCHITECTURE INTERFACES AND INTEGRATION DESIGN ...................................................... 52
    3.4.1 System overview ........................................................................................................................ 52
    3.4.2 Privacy flag platform architecture integration ............................................................................. 52
    3.4.3 Application Subsystem integration ............................................................................................... 57
    3.4.4 Backend Subsystem integration .................................................................................................. 58

CONCLUSION ............................................................................................................................................ 59

REFERENCES ............................................................................................................................................ 60

ANNEX A. SUBSYSTEM COMPONENT SPECIFICATION TEMPLATE .................................................. 61
List of Figures

Figure 1: The domain model ................................................................. 13
Figure 2: The functional view ............................................................... 14
Figure 3: Functional view for the Privacy Flag ....................................... 15
Figure 4: Privacy Flag scenario ............................................................ 18
Figure 5: Top level Privacy Flag information view ................................. 47
Figure 6: The Smartphone application information view ....................... 48
Figure 7: The Browser add-on information view .................................... 49
Figure 8: Website information view .................................................... 50
Figure 9: The Privacy Flag security information view ............................ 51
Figure 10: <Privacy flag platform> subsystem diagram representation .... 52
Figure 11: <Application> subsystem diagram representation ................ 57
Figure 12: <Backend> subsystem diagram representation ...................... 58
List of Tables

Table 1: Privacy Flag platform generic-components in relation to the use-cases that address the main tools available by the platform.................................................................17  
Table 2: <Application (Subsystem)> component – component specification........................53  
Table 3: <Backend (Subsystem)> – component specification .........................................55  
Table 4: <name> component – component specification...............................................61
Introduction

This deliverable is one of the outcomes of the Privacy Flag (PF) research project. It describes project’s initial architecture design which has been created based on the requirements and the outputs coming from both task T1.1 and WP4. The key mechanisms and enablers are combined into the working platform based upon a methodology taken from the FP7 IOT-A research project, with suitable modifications to “suit the purposes” of the Privacy Flag project.

1.1 Purpose and scope of WP1

WP1 focuses on the architecture design of the Privacy Flag. It relies on active interaction between project partners as well as with potential end-users to collect and analyse their specific requirements, per case. The definition of the project architecture represents one of the “key milestones” of the entire Privacy Flag effort, as it provides a proper framework for the activities performed in the other WPs. Indeed, the main purpose of this work package is to ensure that the technical work carried out in the other project WPs is “aligned” with the overall vision, and forms a truly coherent system.

In order to do this, WP1 coordinates and aligns strategy and facilitate activities in the overall project framework, beginning with task T1.1 which provides a definition and analysis of the Privacy Flag requirements from an end-user/player perspective. This work was then followed by task T1.2 activities aiming to define platform processes and the design of the guidelines for the envisaged components and, finally, to design the initial Privacy Flag architecture. This initial architecture will be further elaborated and detailed during Y2, taking into account outcomes of other work packages. In addition to architecture design, task T1.2 will also monitor the fulfillment of the requirements as imposed by other WPs.

1.2 Purpose and scope of T1.2

The main goal of task T1.2 is to design the architecture of the Privacy Flag platform, by including all necessary components, functions, interfaces as well as deployment options. In order to integrate the research project developments and results, the architecture will be reviewed and updated through iterative cycles during the whole project duration, taking into account the outputs of other work packages when they become available.

1.3 Purpose and scope of the current document

This document provides specification of the initial Privacy Flag architecture. The architecture design process was based on the existing body of work in the domain and the methodologies for architecture design. In particular, the results of the IoT-A - Internet of Things Architecture (i.e., an IP EU project that has been carried out in the period from 2009 to 2012) [4] have been used as the “starting point”. These have then been extended by taking into account specific Privacy Flag requirements. Different architectural options were evaluated against the use cases scenarios and the requirements, by using an adopted methodology.
Methodology

In this section, the methodology used for modeling the Privacy Flag architecture is described. There are a number of different approaches used for defining the software architecture [1]. We have selected the methodology defined by the FP7 IoT-A project. This methodology provides an extensive framework and guidelines and was already used by some of the consortium partners in other research projects, thus making it possible to build on previous activities. In addition to this aspect, relying upon a known architecture design methodology has facilitated an easier conceptual understanding between the partners, thus overcoming potential misunderstanding(s) in relation to the naming conventions and the meaning of different concepts used.

The methodology is use-case-driven and relies on a number of views (i.e., functional, information flow, security, etc.) to provide the “complete picture” of architecture. The main input to the architecture design work were requirements identified in task T1.1 and documented in D1.1 [2].

2.1 Context Views

As indicated in Figure 1, this model consists of two parts: a Context view and a domain model. The Context View describes “the relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts)”. The Domain Model, on the other hand, provides a semantic and ontological overlay for the context view, in which it provides guidance on the core entities of a system and how the entities relate to each other. In essence, it provides a common language to be used during the architecture design process.

2.2
Functional Views

The Architecture Reference Model (ARM) [3] defines a set of functional groups and functional components derived from the requirements, as shown in Figure 2.

**Figure 2:** The functional view

ARM exposes 9 different Functional Groups (FGs) [4]:

- **The Application**: this represents the user or the application interacting with the IoT system.
- **The Device**: it can be a sensor, actuator or tag, which will provide information to the system or which modifies the system.
- **The IoT Process Management FG**: this provides the functional concepts and the interfaces necessary to augment traditional processes, with the idiosyncrasies of the IoT world.
- **The Service Organisation FG**: it is used for composing and orchestrating Services, at different levels of abstraction.
- **The Management FG**, which enables the management of the IoT: this implicates configuration of devices, tracking of faults, monitoring, reporting, and administration of the whole IoT system.
- **Virtual Entity FG**: it contains functions for interacting with the IoT system on the basis of VEs as well as functionalities for discovering and looking up services that can provide information about VEs, or which allow the interaction with VEs (but also for managing associations and finding new associations).
IoT Service FG: it contains IoT services as well as functionalities for discovery, look-up, and name resolution of IoT services.

Communication FG: it is an abstraction, modelling the variety of interaction schemes derived from the many technologies belonging to IoT systems and providing a common interface to the IoT service FG.

The Security FG: it ensures the security and privacy in the IoT system.

Those functional groups are composed of many components along with their interfaces and their default functions set which "open the road" to the design of the interactions between them: i.e., the information view. For the purpose of modelling the Privacy Flag functional view, we started from the functional view provided by the methodology and adapted it to our needs. We kept the application, the process management, the service and the security modules. The Virtual Entity has been replaced by the "Database" as the association between the physical and virtual entities is transparent and more attention has been paid to the database, its design and the mechanism for accessing and managing it.

![Figure 3: Functional view for the Privacy Flag](image_url)
2.3 Information Views

The information view defines the flow of data between different functional components addressed previously. The following types of flows are possible:

- **“push (data)”**: it is a simple one-way communication from a server to a client.
- **“request/response”** is a synchronous way of communication between two parties.
- **“subscribe/notify”** is an asynchronous way of communication between two parties: The client just indicates its interest in a service and this service sends notifications when new data is available.
- **“publish/subscribe”** allows a loose coupling between communication parties. There are services offering information and advertise those offers on a broker component. When clients declare their interest in certain information on the broker, the component will make sure the information flow between the service and the client will be established.

After selection of devices and their communication methods, the system is further analysed to derive services and resources. A service is software component, which can be deployed according to the following options: on the user’s side (in the device or in the browser add-on) or in the platform cloud. Furthermore, the data storage should be selected for information collected by the system. This storage could be local, web or locally in a web cache. The following methodology gives the final picture of the architecture but it will not encompass all its aspects. For this, UML [5] is used to cover the essential information and enhance the information view and the architecture model. Finally, this model is specified by using a given methodology coming from the IOT-A [6] which also shows that this IoT-specific ARM could be accommodated for more software oriented design.
Architecture

This section describes the initial architecture of the Privacy Flag platform. First, a use case-driven methodology is used, providing more details about all use cases in the system; then, services are extracted for the overall platform and the architecture is concluded with the information views and the corresponding architecture interfaces. Architecture interface and integration design specify the application system and its integration with the backend system.

Table 3 summarizes the generic (or archetypical) use cases addressed by Privacy Flag and the project’s tasks where the platform features will be elaborated according to the DoW.

Table 1: Privacy Flag platform generic-components in relation to the use-cases that address the main tools available by the platform

<table>
<thead>
<tr>
<th>End–users</th>
<th>Risk focus</th>
<th>Evaluators</th>
<th>User interface</th>
<th>Tools</th>
<th>Data storage</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CROWD Websites</td>
<td>CROWD</td>
<td>Browser</td>
<td>Add-on + security agent</td>
<td>Common knowledge Database (CKD)</td>
<td>T4.3, T4.2</td>
<td></td>
</tr>
<tr>
<td>Smartphone app</td>
<td>Smartphone</td>
<td>Add-on + security agent</td>
<td>Website</td>
<td>Website</td>
<td>T4.4, T4.3</td>
<td></td>
</tr>
<tr>
<td>IoT deployment</td>
<td>Website</td>
<td>Website</td>
<td></td>
<td></td>
<td>T4.6</td>
<td></td>
</tr>
</tbody>
</table>

Complementary tools (in-depth evaluation)

<table>
<thead>
<tr>
<th>End–users</th>
<th>Risk focus</th>
<th>Evaluators</th>
<th>User interface</th>
<th>Tools</th>
<th>Data storage</th>
<th>Related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution driver</td>
<td>ICT Solution</td>
<td>Experts</td>
<td>Dedicated Website</td>
<td>In-depth analysis tool</td>
<td>Specific Database</td>
<td>T6.4, T3.3</td>
</tr>
<tr>
<td>Solution drivers Outside the EU</td>
<td>Legal compliance</td>
<td>Self-declaration</td>
<td>Dedicated Website</td>
<td>Automated form processing</td>
<td>Specific Database</td>
<td>T3.4</td>
</tr>
</tbody>
</table>
3.1 Use-cases

Privacy Flag is targeting risk assessment along three different domains: websites, smartphones applications, and smart city IoT deployments. These are addressed by deploying privacy risk monitoring, using a smartphone application, a Browser Add-on (BAO), Distributed Agents (DAs) and a Crowdsourcing Evaluation Tool (CET).

Figure 4: Privacy Flag scenario
### 3.1.1 Use case 1: Smartphone app

**Smartphone application:** Privacy risk monitoring using the Android [7] smartphone application enables users to be informed about (or request an assessment of or assess it himself/herself) the level of risk for his/her privacy when using other smartphone applications. The methodology of the application evaluation is as follows:

**Step 1:** The smartphone application analyzes the user’s installed applications (and checks for new or updated ones if this is not the first time the user uses the PF application). It then calculates a local Threat Level Score for each installed application.

**Step 2:** The smartphone application submits in JSON format the calculated score for all applications to the Distributed Agent and the Database.

**Step 3 (independent-optional):** The smartphone evaluations contributors (CET experts) manually evaluate applications and submit their evaluation to the database. This is called as the CET evaluation score.

**Step 4 (independent):** The database performs various calculations based on Artificial Intelligence (Ai) and Machine Learning algorithms. It also employs advanced statistical and epidemiological models to detect outliers (applications with vastly different Threat Level Scores) which indicate possible data leakage. The outputs of the database calculations are the Mean Threat Level Score and the Mean CET Evaluation Score.

**Step 5:** A distributed agent queries the database for CET evaluations related to the installed applications (if existent), the Mean Threat Level Score and the Mean CET Evaluation Score.

**Step 6:** The distributed agent then decides based on:

- The smartphone application’s Local Threat Level Score.
- The Local CET Evaluation Score.
- The Mean Threat Level Score.
- The Mean CET Evaluation Score.

The final result of the analysis of the user’s applications is presented to the user using color-coded threat levels based on how each application was categorized, i.e. green color if the application is safe or red if there is a possibility for data leakage and user information exposure.
3.1.1.1 Use case 1-1: Evaluation of installed application

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone application</td>
<td>Evaluation of installed application</td>
</tr>
</tbody>
</table>

**Description**

The PF smartphone application should enable evaluation of different applications installed on a smartphone, as well as provide the respective risk assessment. This use case will enable the following functionality:

- enable a user to assess the level of risk for each installed application
- enable a user to request the assessment of installed applications

**Context View**

**Actors Involved**

- **Information**: A piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who make an assessment of an application or request the respective assessment
- **Devices**: Smartphone devices with the PF application installed
- **Data management server components**: Management of user assessments as well as data processing and notification delivery (by subscription).
- **Subscription entity**: Abstracted description of a subscription: a notification about a
subscribed entity about a privacy risk change

**Notification:** Users should receive notifications about the level of risk some applications have
3.1.1.2 Use case 1-2: Crowd sourcing monitoring of privacy risks with Distributed Agents

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Crowd sourcing monitoring of privacy risks with Distributed Agents (smart phone app)</td>
</tr>
</tbody>
</table>

**Description**

Distributed Agents provide a technical analysis of a smart phone application based on UPRAAT questions and retrieve data from the database in order to detect outliers.

This use case will enable the following functionalities:

- enable the Privacy Flag Smart Phone Application to interact with the Distributed Agent
- enable the Distributed Agent to automatically evaluate the questions asked by UPRAAT
- enable the Privacy Flag knowledge data base to be enriched
- enable the Distributed Agent to query the DB for corresponding UPRAAT evaluations of a specific application, the Mean Threat Level Score and the Mean UPRAAT score
- enable the Distributed Agent to provide information to the Smart Phone Application regarding the automatic evaluation of the UPRAAT questionnaire which will categorize the smartphone application as safe, or warn that a possible data leakage and personal information exposure is imminent

**Context View**

![Context View Diagram](image)
## Actors Involved

<table>
<thead>
<tr>
<th><strong>Information</strong></th>
<th>Questions provided by UPRAAT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>Users who submit their evaluation score through the CET of the smartphone Application</td>
</tr>
<tr>
<td><strong>Devices</strong></td>
<td>Internet-connected smart devices (smart phone, tablet, etc.)</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Users should receive the Distributed Agents Evaluation about the threat level through the Privacy Flag Smart Phone Application</td>
</tr>
</tbody>
</table>
3.1.2 Use case 2: Browser add-on

**Browser add-on:** privacy risk monitoring for websites enables users to be informed on and to assess or request an assessment (assess himself/herself) the level of privacy risk for him/her when accessing a website through a browser.

The methodology of the website evaluation is explained in the following six steps:

**Step 1:** The browser add-on analyses the website that the user is currently connected to. The browser add-on (BAO) uses the **Threat List Matrix** and calculates a **Local Threat Level Score** for each **Threat Factor** of the Threat List Matrix.

**Step 2:** The browser add-on submits in JSON format the Threat Level Score of all Threat Factors to DA and the DB.

**Step 3 (independent - optional):** CET experts evaluate manually the website and submit their evaluation to the DB of the **Local CET Evaluation Score**

**Step 4 (independent - out of order):** The DB performs various calculations based on Artificial Intelligence and Machine Learning algorithms. The DB also employs advanced statistical and epidemiological models to detect outliers (websites with vastly different Threat Level Scores) which indicate possible data leakage. The outputs of the DB are the **Mean Threat Level Score** and the **Mean CET Evaluation Score**

**Step 5:** DA queries the DB for CET evaluations of the specific site (if existent) the Mean Threat Level Score and the Mean CET Evaluation Score.

**Step 6:** DA decides based on

- the BAO Local Threat Level Score
- the Local CET Evaluation Score
- Mean Threat Level Score
- Mean CET Evaluation Score.

The final result of the analysis of the website is presented to the user by using color-coded threat levels, based on how the website was categorized, i.e.: green color if the website is safe or red if there is a possibility of data leakage and personal data exposure.
3.1.2.1 Use case 2-1: Website evaluation and crowd source monitoring

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser Add-on</td>
<td>Website evaluation</td>
</tr>
</tbody>
</table>

**Description**

The PF browser add-ons should enable the evaluation of websites based on both user evaluation and automated distributed agents.

This use case will enable a following functionality:

- enable a user to assess the level of risk for when visiting a website
- enable a user to request an assessment of the level of risk for a specific website

**Context View**

**Actors Involved**

- **Information**: A piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who make an assessment of the website or receive a notification
- **Browsers**: the set of browsers where the add-on is available
- **Data management server components**: Management of user assessments as well as data processing and notification delivery
- **Notification**: users should receive notifications about the level of risk some websites have when they visit them
3.1.2.2 Use case 2-2: Crowd source monitoring of privacy risks with distributed agents

For the requirements: refer to those identified for the distributed agents in section 3.1.1.2.

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Crowd source monitoring of privacy risks with Distributed Agents (browser add-on)</td>
</tr>
</tbody>
</table>

**Description**

Distributed Agents provide a technical analysis of a specific website based on UPRAAT questions and retrieve data from the database in order to detect outliers.

This use case will enable the following functionalities:

- enable the Privacy Flag Web Browser add-on to interact with the Distributed Agent
- enable the Distributed Agent to automatically evaluate the questions asked by UPRAAT
- enable the Privacy Flag knowledge data base to be enriched
- enable the Distributed Agent to query the DB for corresponding UPRAAT evaluations of a specific website, the Mean Threat Level Score and the Mean UPRAAT score
- enable the Distributed Agent to provide information to the Privacy Flag Web Browser add-on regarding the automatic evaluation of the UPRAAT questionnaire which will categorize the website as safe, or possible data leakage and user information exposure is imminent

**Context View**

- Users
  - Laptop with installed browser add-on
- UPRAAT Evaluation
- Distributed Agent
- Database
- General statistical patterns
- Automatic analysis output
### Actors Involved

<table>
<thead>
<tr>
<th><strong>Category</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information</strong></td>
<td>Questions provided by UPRAAT</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Users who submit their evaluation score through the CET of the Web Browser add-on</td>
</tr>
<tr>
<td><strong>Devices</strong></td>
<td>Internet-connected devices (PCs, laptops, etc.)</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Users should receive the Distributed Agent’s Evaluation about the threat level through the Privacy Flag Web Browser add-on</td>
</tr>
</tbody>
</table>
3.1.3 Use case 3: Website

The Privacy Flag website will enable end users to register to the platform. The registration process will obtain some of the user’s personal data such as: email, name, organisation, chosen password and chosen account type from within the predefined list (i.e., expert user, or standard member). If a user submits a registration for the expert account, then additional credentials proving expertise in relevant fields are required and they are cross-checked by the Privacy Flag Admin. The website will enable the user to assess and be informed on (or request an assessment or assess by himself/herself) the level of risk for his/her privacy. The website is developed in .Net [8] leveraging dotNetNuke [9] CMS for the backend operations.

**Step 1:** User enrolls the Privacy Flag account by submitting his credentials for approval. He can apply for the expert account or for the user “contributor” account. Admin reviews and manage received applications and inquires additional information if required.

**Step 2:** User submits risk assessment application using website form, which generate a notification for administrator in form of an email. The administrator identify if application is consistent. If the application meets criteria and there is no missing data, administrator identifies one or two experts to perform the in-depth analysis.

**Step 3:** Expert evaluation: The administrator invite identified expert(s) to preform in-depth analysis of the applicant. Then the expert(s) validates his/their acceptance and start(s) reviewing the documents and information provided by the applicant. The expert(s) follow(s) an extended version of the UPRAAT by completing several forms with predefined questions. He/they can save his/their inputs and perform the evaluation in several times by logging into his/their personal account(s). The expert(s) if needed can request additional information from the user. He/they can contact(s) the applicant through an online messaging interface (to track all the correspondence) in order to get the complementary information.

**Step 4:** Review validation: When the expert(s) completes in-depth analysis of the applicant, the report is submitted to the system and stored in the server side. The administrator reviews the report and validates it. Then the administrator identifies the senior expert. The senior expert task is to validate the report about in-depth analysis. The senior expert can review the report in several times. Once the senior expert considers he can make a decision, he provides and submits his decision on line (to validate or not the report). The administrator and the experts receive a message with the decision is done. The administrator can then inform the user about the decision. If the decision is positive, the applicant appears on a list of validated evaluations.
3.1.3.1 Use case 3-1: IoT Deployment privacy risk assessment

For the requirements: refer to those identified for the website in section 3.1.3.

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>IoT deployment privacy risks assessment</td>
</tr>
</tbody>
</table>

The “IoT deployment assessment” is crowdsourced and the users are people, completely anonymized.

**Description**

IoT deployment privacy risk should enable evaluation of IoT deployments in users’ vicinity by enabling a user to make an assessment, request an assessment for a deployment or assess his/her deployment.

This use case will enable a following functionality:

- Enable a user to assess the level of risk when identifying an IoT deployment in an environment using Privacy Flag website.
- Enable a user to request an assessment of the level of risk for an IoT deployment in an environment using Privacy Flag website.
- Enable a user to assess his/her IoT deployment for the level of risk using Privacy Flag website.
- Enable a user to be informed of the level of risk for an IoT deployment in an environment.

**Context View**

![Diagram showing the interaction between users, mobile devices, sensors, and the IoT deployment assessment process.]
### Actors Involved

- **Information**: a piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who make an assessment of the IoT deployment or receive notification
- **Devices**: Smartphone devices with embedded sensors
- **Data management server components**: Management of user assessments as well as data processing and notification delivery (by subscription).
- **Subscription entity**: Abstracted description of a subscription: a notification about a subscribed entity about a privacy risk change
- **Notification**: a user should receive notifications about the level of risk some IoT deployment have
3.1.3.2 Use case 3-2: In depth evaluation tools

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3.3</td>
<td>In-depth analysis - Controller Evaluation of Privacy Risk Area Assessment Service (CE-PRAAS)</td>
</tr>
</tbody>
</table>

The use case of “In-depth evaluation” is on a completely separate website, where the users are people representing a legal entity who must register to apply for the process defined by task T6.4 and follow an interactive process.

**Description**

The in-depth analysis of privacy risk is an extension of the UPRAAM methodology to be defined by task T6.4 and supported by task T3.3 which will develop and provide the requested online tool for T6.4 implementation. The detailed use case will evolve and be updated according to task T6.4 instructions. In order to understand this CEPRAAS functionality this use case presents an outline of the Privacy Flag platform that includes the UPRAAM subsystem and CEPRAAS subsystem.

- **UPRAAM** subsystem provides the compliance assessment methodology and process to determine if an object (application, website or IoT deployment) is compliant with the European personal data protection norms. Compared to the UPRAAM methodology used by the crowdsourcing tool, the UPRAAM methodology applied to the in-depth analysis is refined and further extended by AS.

- **CEPRAAS** subsystem includes the set of enablers in order to interact with an Enterprise willing to undergo a UPRAAM with a potential outcome the assessed level of compliance with personal data protection norm.

Privacy Flag will explore the potential of UPRAAM for in-depth analysis of personal data protection compliance as set by the experts. The in-depth analysis is managed by a distinct database and benefits from a distinct user interface. The use case presents the main sequence of interactions, as well as a complementary set of interactions.

- The starting point of CEPRAAS is when the **Enterprise Staff** actor applies online on an ad hoc webpage (not on the Privacy Flag website) to get an in-depth evaluation (this action triggers the “Access request activity to CEPRAAS” activity). The application is performed through an online form this creates a workspace with the possibility to upload documents (.pdf) files.

- The application details and documentation provided is stored in a dedicated and secured CEPRAAS database (background backend activity), and an internal (to the CEPRAAS subsystem) alert is sent to the **Customer Relations Agent** (member of the CEPRAAS staff).

- The **Customer Relations Agent** reviews the application and identifies any missing input in order to provide the “Grant access” activity. If information is missing, the **Customer Relations Agent** contacts the CEPRAAS staff to get the complementary profile information within the already created workspace.

- The CEPRAAS administrator and **Customer Relations Agent** review the application and
validate it (in order to complete the “Grand access” activity).

The Enterprise staff is invited to pay a fee online or through bank transfer (“Payment transaction” activity).

Once the payment is received, the CEPRAAS administrator identifies the Privacy Risk Assessment Expert actor or actors (who receive an invitation email) to perform the Privacy Intelligence Risk Assessment activities with the collaboration of the Security Managers (from the Enterprise).

The Privacy Risk Assessment Expert actor -or actors- accept the task from the administrator.

Privacy Risk Assessment Expert actor starts the interactions (“Provide details of Enterprise system” activity) with the appointed contact point from the Enterprise (Security Manager actor). The interactions are summarised in the Context view use case diagram below, with activities “Provide details of Enterprise systems”, “Asses Privacy Risk of Enterprise”, “Prepare Enterprise Specific Risk Assessment” and “Provide Guidance on provisions of Enterprise System details” but a more detailed explanation is given below:

- The Privacy Risk Assessment Expert(s) follow(s) an extended version of the UPRAAM by completing several forms with predefined questions. He/they can save his/their inputs and perform the evaluation in several times by logging into his/their personal account(s).
- The expert(s) can request complementary inputs from the applicant. He/they then contact(s) the applicant through an online messaging interface (to track all the correspondence) in order to get the complementary information.
- The Enterprise Security Manager logs in and completes his/her application with the requested information and documents.
- Once the Privacy Risk Assessment Expert(s) has/have completed the analysis, he/they submit(s) his/their report(s) into the system (“Prepare Enterprise Specific Risk Assessment”).
- The report is then reviewed by another set of experts who can validate, refuse or request complementary information from the experts.

Once the CEPRAAS Administrator validates with an iteration procedure the “Prepare Enterprise Specific Risk Assessment” then the Assessment is ready to be released to the Enterprise.

The validated reports are listed on a public page, giving access to a public summary of the evaluation result.

Complementary interactions:

- The CEPRAAS Administrator and experts can access all the documents and history of actions and correspondence at any time.
- The CEPRAAS Administrator can edit and modify the forms.
- The CEPRAAS Administrator can manage the list of Privacy Risk Assessment Experts and
access their list of ongoing and past evaluations.

In order to address task T6.4 objectives, the in-depth analytical tool should be aligned with the requirements related to certification processes, including ISO 17021 [10], 17065 [11] and 17067 [12].
Context View (part 1/2)
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT No. 653426

Deliverable D1.2 “Privacy Flag initial architectural design”
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT No.653426

Actors Involved

Privacy Flag Subscriber: is the superclass of actors who are members of the CROWD subsystem and this superclass is generalised into actors which contribute and consume intelligence/‘the flag’/alerts to and from the UPRAAM subsystem (which is part of the PRIVACY FLAG platform)

IoT Deployment Intelligence Contributor: is the actor “contributing intelligence” to the UPRAAM system relating to the IoT Deployment

Browser Add-on Intelligence Contributor: is the actor “contributing intelligence” to the UPRAAM system by utilising the browser add-on

Smartphone Application Intelligence Contributor: is the actor “contributing intelligence” to the UPRAAM system by utilising the smartphone application

Consumer of ‘the Flag’ and Alerts: it is the actor which “consumes the intelligence of types ‘the flag’” and “Alerts provided for consumption” from the UPRAAM subsystem

Privacy Flag staff: is the superclass of the internal actors within the UPRAAM subsystem

Qualified Technical Expert: this actor is a technical expert actor in the field of Personal data protection performing the UPRAAM-based in-depth analysis on the technical aspects of personal data protection.

Qualified Legal Expert: this actor is a legal expert actor in the field of Personal data protection performing the UPRAAM-based in-depth analysis on the legal aspects of personal data protection.

Senior Experts: will review and validate the report prepared by the technical and legal experts.

Enterprise staff: is an actor responsible for requesting access to the CEPRAAS subsystem (see activity “Access Request to CEPRAAS”) and in order to complete this activity the Customer Relations Agent requires to grant access.

Security Manager: is the actor who has deep knowledge of the Enterprise systems and is able to “Provides details of Enterprise systems” according to the in-depth analysis requirements.

CEPRAAS Staff: includes all the actors that participate in activities within the CEPRAAS subsystem.

Customer Relations Agent: a generalisation of the CEPRAAS Staff responsible for activity “Granting Access” to the requested Enterprise Staff actors and grants/triggers the activity “Alert Privacy Flag Subscribers of Enterprise Privacy Risk Assessment update”.

Privacy Risk Assessment Expert: a generalisation of the CEPRAAS Staff responsible for activities within the Privacy Intelligence Risk Assessment subsystem. The main activities include the “Provide Guidance on provision of Enterprise System details” activity, responsible for “Prepare Enterprise Specific Risk Assessment” activity and the activity “Assess Privacy Risk of Enterprise”
### 3.1.3.3 Use case 3-3: Voluntary Compliance Commitment tool

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Voluntary Compliance Commitment Tool</td>
</tr>
</tbody>
</table>

**Description**

Company XY sells “manga comics” to EU customers from Japan. In doing so it collects customers’ personal data, such as name, contact details, location (also by means of geolocation tools), consumers’ preferences regarding the type of stories he/she is interested in, etc. This information is processed to satisfy the contract (delivering the purchased goods, obtain the payment, etc.), as well as to advertise other similar or completely different products, also by third parties not involved in the initial transaction (e.g., a retailer of electronic devices).

Company XY knows that the EU has strict legal standards concerning data protection and wants to be sure to comply with them in order to gain a competitive advantage over competitors that do not offer adequate safeguards for personal data.

Company XY therefore decides to adopt PF’s Voluntary Compliance Commitment Tool (“VCT”);

- The Company XY goes to PF’s main website and finds a banner or a link to the VCT, which operates from a dedicated website.
- The dedicated website contains the terms of use, explaining "what this tool does for you" and "What we do for you" (clarifying to what extent we provide the user with free counselling services)
- The Company XY has to subscribe to the VCT website. The subscription is performed through an online form in which the Company has to insert a valid e-mail and a password of at least eight characters, including a number and a capital letter.
- The Company XY receives a confirmation e-mail to validate its account and, then it can log in and complete the VCT in its personal page.
- The VCT personal page (it is a standard web page for each subscriber) contains a form whereby the following information is collected from the User (the SME):
  - Company name, website, and address;
  - Authorized representatives;
  - Type of business carried out;
  - Type of data processed;
  - A description of the Security Measures Applied (this will be a standard form prepared by PF and filled in by the applicant, containing standard questions to which the company has to reply with yes/no);
- Once the information is provided, the system has to automatically verify whether all the replies to the Security Measures Questionnaire are “Yes”.
  - If one or more replies are “No”, the user will be deemed as non-compliant with the EU security measure standards and needs to be contacted via email or the website’s
messaging system by a PF’s expert. A notification, in this context, will be sent to the expert. The user will see a message informing him/her that he/she will be contacted by PF’s expert to assess the security measure issues. If the issue persists, the expert will advise the user to perform an in-depth analysis. If the issue is solved, upon notification by the expert to the website administrators, the user must be able to see the Security Measures form unlocked, and fill it in again with the right answers as certified by the expert, and to conclude the procedure by signing the VCT.

- If all the replies to the Security Measures Questionnaire are “Yes”, the user will see an active button which states “Read the VCT”

- Upon clicking on the button, the user sees the PDF of the legal text (the unilateral declaration) where the information provided (name, address, types of data etc.) is automatically filled in the relevant sections. The form does not allow “next” or “finish”, unless the user selects “I have read the VCT”.

- The Security Measures Form (in PDF format) is also attached to the VCT. This form contains standard multiple choice questions about security measures already adopted by the applicant (the reply to the questions will be only Yes at this point).

- The user reads through the text and eventually signs it by clicking the submission button.

- The user can then print the VCT contract that must be signed by the legally authorized representatives of the company.

- The user logs in and uploads the signed contract as a pdf in the system.

- The system stores in its server all the submission info (documents, signature, timestamp, contact info etc.) and the persons in charge of processing for PF get access to all the information submitted.

- An alert is sent to the platform administrator for him to check that the submission is complete and conform in order to validate it.

- At the end of this procedure a badge may be released in order to let the subscriber use it on its website to certify that company voluntarily committed to abide to the EU data protection rules.

- The list of companies that have signed the VCT and have been validated will be available on the website and it will be made public.
Context View

Actors Involved

- **VCT**: a dedicated section on PF website, including the online user interface to submit applications and relevant data.
- **Applicant**: an organization that submits an application and its information through the VCT section of the website and signs the unilateral declaration.
- **Administrator**: who overviews and manages the overall process and access rights, and will validate the completed processes.
- **Experts**: who perform the analysis of the Security Measures Form and potentially convince the user to purchase the In-depth analysis.
- **A database**: with all submitted data, as well as logs of all communications.
- **Personal Area**: where the user finds information associated to his/her profile and the services used.
- **A messaging system**: enabling the various stakeholders to communicate.
- **Token-Logo**: the user should receive a badge that is placed on its website in order to certify its compliance with EU-PF data protection rules.
3.2 Services

The high-level use cases presented above are derived to a set of functional services used as an enabler in the platform offering a set of different functionalities to the other building components in the system as well as to the end-user.

3.2.1 Registration

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Registration</td>
</tr>
</tbody>
</table>

**Description**

Access to the resources is enabled to the users only if they are registered to avoid having users providing false and misleading assessments. The registration process is done automatically by Android applications, i.e. by using the device’s UUID and sending it to the backend. Also, from the website and browser add-on by asking the user’s email that should be verified by clicking the link sent to the provided email.

**Actors Involved**

- **User**: person that uses mobile app/ browser add-on/ website to register to the Privacy Flag platform
- **Backend**: system that saves generated data into the PF database
3.2.2 Data Valuation Tool

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>Data Value Component</td>
</tr>
</tbody>
</table>

Description

The PF Crowd Sourcing Data Value Component aims to analyse the perception of end users of the importance (value) of their data and, also, increase their awareness when sharing their data. This service will enable the following functionality:

- enable users to assess the value and importance of data they are willing to share over the network
- enable users to analyse their valuation perceptions with different type of visualizations
- enable users to compare their input with the average input provided to the PF
- enable users to submit (only if they choose to do it) their analysis to the PF

Actors Involved

- **Information**: A data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who make an assessment of the PF data value tool
- **Web Interface**: the web interface to use the tool (embedded in the PF site)
- **Data management server components**: Management of user assessments as well as data processing
3.2.3 Data access

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data access and management</td>
</tr>
</tbody>
</table>

**Description**

Data access will be available using interfaces that will be implemented to enable adding/changing/manipulating a resource that will be saved/retrieved into/from the Privacy Flag database. In case of personal data collection, the system enables users to control their personal data, to access, rectify, delete or block them. It is always possible, for the users, to change the sets of data that they have shared. This use case will enable the following functionalities:

- enable available Privacy Flag tools to store the generated data
- enable available Privacy Flag tools to retrieve data stored in the database
- enable the ability to backup stored data
- enable the Database to scale according to the workload

**Context View**

![Diagram of Privacy Flag tool, Database, Data storage, Data retrieval, Copy, and Backups]

**Actors Involved**

Information: Data generated by available Privacy Flag tools, Distributed Agents or data retrieved from the database
3.2.4 Data Value component

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>Data Value Component</td>
</tr>
</tbody>
</table>

**Description**

The PF Crowd Sourcing Data Value Component aims to analyse the perception of end users of the importance (value) of their data and as well as increase their awareness when sharing data.

This service will enable a following functionality:

- enable users to assess the importance of data they are willing to share over the network
- enable users to analyse their perception with different types of visualizations
- enable users to compare their input with the average input to the PF
- enable users to submit (only if they chose to do it) their analysis to the PF

**Actors Involved**

- **Information**: A piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who make an assessment on the PF data value tool
- **Web Interface**: the web interface to use the tool (embedded in the PF site)
- **Data management server components**: Management of user assessments as well as data processing
3.2.5 Subscription

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td></td>
</tr>
</tbody>
</table>

**Description**

As new legislation and rules or changes are prescribed, compliant websites, organizations etc. need to be informed of their existence. For this notification to be delivered, a subscription to PF may be required. Hence, subscribed entities have the following services: 1) Up-to-date information on relevant news; 2) have the PF system relate stored data to registered-compliant entities (at least just for contact reasons; 3) have the PF system to be able to perform a comparison of their current data, policies and security mechanisms and notify them for any additional requirements on data etc.

**Actors Involved**

- **Information**: A piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who want to be notified of new rules, etc.
- **Assessed entities**: That have stored data in the PF database
- **PF expert**: who checks if stored data is sufficiently compliant with new regulations
- **Administrator**: who manages subscriptions
- **Web Interface**: the web interface to use the tool (embedded in the PF site)
- **Data management server components**: management of user data assessments as well as data processing
3.2.6 Anonymization service

<table>
<thead>
<tr>
<th>UC</th>
<th>Use Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security and Privacy Enabler</td>
</tr>
</tbody>
</table>

**Description**

When Privacy Flag users communicate with the backend services such as the Privacy Flag database, even if the content of communication is adequately encrypted, the connection itself may reveal significant information, e.g., who in particular is using the tools and the applications provided by the platform. In addition, the transmitted content may be susceptible to traffic analysis attacks.

Therefore, the Security and Privacy Enabler will allow the following functionality:

- enable users to remain completely anonymous by not revealing identifying characteristics such as the IP address when they communicate with the platform
- the anonymous communication session will not induce significant loss in terms of quality of service, i.e., the users will not experience noticeable disruptions in terms of bandwidth or latency
- enable users to transmit their information (e.g., answers of a UPRAAT questionnaire) without the risk of being subjected to traffic analysis, i.e., the transmitted data remain strictly confidential

**Actors Involved**

- **Information**: A piece of data as a passive digital artefact, which is an information item provided by the user.
- **User**: Users who provide any kind of information to the system
- **Devices**: Smartphones, web browsers
3.3 Information views

Information views define the interaction between different functional components. Data flow is obviously dependent on the modelled use case and can be split into multiple stages. For example, those steps could be the discovery of a service, the subscription to the service, the crowdsourcing of data to the service, etc.

3.3.1 Top level information view

This information view shows all interaction in the system between functional components, the application and the backend. Application layer of the Privacy Flag platform is used for collecting information from users manually from the smartphone app, mobile add-on and the website; and automatically using Monitoring Agents (MA) deployed as a service in the Android smartphone application and in the browser add-on. All information from the Application layer is collected over the Webservice API which collects the data and exposes the main backend functionality. In the backend, the Process Management block is executing events for the assessment of the privacy risks; it also saves the outcome of the assessment using the VE Resolution in the Database, sends the outcome to the Application layer to update required fingerprints in the end-user devices/browsers and to notify the end-users.

The information exchange between components is given in green; red are notification flows and the yellow color is used for presenting the security flows, i.e.: Authentication, Authorization, Identity management and Anonymization.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT No.653426

Deliverable D1.2 Privacy Flag initial architectural design
### 3.3.2 Smartphone application information view

The smartphone application has build-in Score computation component, a Monitoring Agent and Alert service. Score computation is event processing mechanism dislocated from the backend, using the synchronized matrix for computation of the risks for installed applications.

The Monitoring Agent in the smartphone application collects information about the user’s device for the risk assessent and POSTs it to the webservice endpoint. User could also contribute to the assessment by providing the assessment directly from the smartphone app. The UPRAAT assessment process running in the backend assess the risk of the application and notify the user about the outcome of the assessment sending the list of application and its risk level. Alert service is used to present the result of the assessment to the end-user sent as a push message or collected from the webservice in predefined time.

![Diagram of Smartphone application information view](image-url)

*Figure 6: The Smartphone application information view*
3.3.3 Browser add-on information view

The Browser add-on has two main functionalities deployed: a Monitoring Agent and Alert User Interface (UI) service. A Monitoring Agent (MA) in the browser add-on collects data about the website that user visits and sends it to the server. This data is assessed by the UPRAAT process in the backend and returned to the browser add-on syncing the local add-on privacy level matrix. The Alert UI of the add-on provides an information to the user about the level of risks of the website that user visits.

Figure 7: The Browser add-on information view
3.3.4 Website information view

The Privacy Flag website collects data for assessment from the users and sends it to the web-service endpoint. This data is manually analysed by the intelligence analyst that assesses the privacy risk of the entity by using the website form. The end-user (Privacy Flag Intelligence contributor) can directly submit assessment of the risks by sending data later used to enhance fingerprint database. A Distributed Agent running in the backend of the website platform automatically extracts required data for the analysis from the Database based on the pre-defined logic and sends this input to the UPRAAT for final risk quantification. Notification service will notify the end-user about the results of the analysis.

![Figure 8: Website information view](image)
3.3.5 Security information view

This information flow shows how the security components interact when a user or application is requesting a Service.

The security of the platform has leveraged using Identity Management, Authentication, Authorization and Anonymization. Complete communication between the Application Layer and the backend should be authenticated and authorized permitting access only to resources that user is authorized to use. All private data for the users are anonymized to disable privacy issues in case of security breach from outside and direct access to these from the inside. The information flow which is given below shows how the security components interact when a user or application is requesting a Service.

![Figure 9: The Privacy Flag security information view](image-url)
3.4 Architecture interfaces and integration design

3.4.1 System overview
This section provides a description of the Privacy flag platform in the scope of technical characteristics of the architecture components. The analysis of the architecture is explained in terms of components, interfaces and ports depicted from the component diagrams included in the subsequent sections.

3.4.2 Privacy flag platform architecture integration
This is the top-level architecture of the Privacy Flag platform with the main interfaces. The description of components, ports and interfaces depicted from Figure 10 are included in subsequent sections 3.1.2.1, 3.1.2.2

Figure 10: <Privacy flag platform> subsystem diagram representation
### 3.4.2.1 Application (Subsystem)

**Table 2: <Application (Subsystem)> component – component specification**

<table>
<thead>
<tr>
<th>Name Component</th>
<th>Name = Application (Subsystem)</th>
<th>Subsystem = Privacy Flag platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose (what, not how)</strong></td>
<td>This subsystem includes all the graphical user interface aspects of the platform with the components that are deployed in the user-interface devices</td>
<td></td>
</tr>
<tr>
<td><strong>Inputs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UPRAAM_Subscriber is the interface which communicates credentials of actors to the backend under the umbrella of external and internal users utilising the UPRAAM tools (UPRAAM_Subscriber)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CEPRAAS_Subscriber is the interface which communicates credentials of actors to the backend under the umbrella of external and internal users utilising the CEPRAAS service (CEPRAAS_Subscriber)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCT_Subscriber is the interface which communicates credentials of actors to the backend under the umbrella of external and internal users utilising the Voluntary Commitment Tool (VCT_Subscriber)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UPRAAM_API is the interface which perform application specific calls to the backend on behalf of the UPRAAM associated components (UPRAAM_API)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CEPRAAS_API is the interface which perform application specific calls to the backend on behalf of the CEPRAAS associated components (CEPRAAS_API)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCT_API is the interface which perform application specific calls to the backend on behalf of the voluntary compliance tool associated components (VCT_API)</td>
<td></td>
</tr>
<tr>
<td><strong>Outputs</strong></td>
<td>(Monitoring agents collecting relevant data and communicating them to the Backend subsystem (UPRAAM_API))</td>
<td></td>
</tr>
<tr>
<td><strong>Dependencies</strong></td>
<td>Backend (Subsystem)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All actors of the platform</td>
<td></td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>UPRAAM_Subscriber</td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>CEPRAAS_Subscriber</td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>VCT_Subscriber</td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>UPRAAM_API</td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>CEPRAAS_API</td>
<td>required</td>
</tr>
<tr>
<td></td>
<td>VCT_API</td>
<td>required</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>AA_ClientSide</td>
<td>direction: bi-directional</td>
</tr>
<tr>
<td></td>
<td>UPRAAM_API_CS</td>
<td>direction: bi-directional</td>
</tr>
<tr>
<td></td>
<td>CEPRAAS_API_CS</td>
<td>direction: bi-directional</td>
</tr>
<tr>
<td></td>
<td>VCT_API_CS</td>
<td>direction: bi-directional</td>
</tr>
<tr>
<td>Contracts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UPRAAM_Subscriber</strong></td>
<td>contract: invariant</td>
<td>Access control to the internal / administrative UPRAAM staff in order to access the UPRAAM tools</td>
</tr>
<tr>
<td><strong>UPRAAM_Subscriber</strong></td>
<td>contract: invariant</td>
<td>External actors of UPRAAM i.e. the intelligence providers need to have an automatic way of id assignment when utilising the browser Add-on or the Smartphone application or the web-based data-valuation tool in order to escort the associate data to the backend (via the UPRAAM_API interface). External actors of UPRAAM create an id after installation or when creating a session with the web-based data-valuation tool.</td>
</tr>
<tr>
<td><strong>UPRAAM_API</strong></td>
<td>contract: invariant</td>
<td>This Interface represents data communication between UPRAAM components (Applications to/from Backend) depending on intelligence providers preferred intelligence providing tool (Browser Add-on, Smartphone application or web-based data valuation tool)</td>
</tr>
<tr>
<td><strong>UPRAAM_API</strong></td>
<td>contract: invariant</td>
<td>Implements the communication interface of data collected by the monitoring agents and Backend (Subsystem)</td>
</tr>
<tr>
<td><strong>CEPRAAS_Subscriber</strong></td>
<td>contract: invariant</td>
<td>Access control interface for CEPRAAS staff and External actors (Enterprise staff) in order to access the CEPRAAS subsystem.</td>
</tr>
<tr>
<td><strong>CEPRAAS_Subscriber</strong></td>
<td>contract: pre-condition</td>
<td>External actors (Enterprise staff) need to make an account and be approved by CEPRAAS staff in order to have access to the CEPRAAS service.</td>
</tr>
<tr>
<td><strong>CEPRAAS_Subscriber</strong></td>
<td>contract: post-condition</td>
<td>External actors (Enterprise staff) can interact with the appointed “Customer Relations Agent” of CEPRAAS staff (after the pre-condition contract is complete)</td>
</tr>
<tr>
<td><strong>CEPRAAS_API</strong></td>
<td>contract: invariant</td>
<td>Interface for communication of information between the CEPRAAS staff and Enterprise staff actors. The record of communication between the two parties is going to be logged and stored in the backend via this interface</td>
</tr>
<tr>
<td><strong>CEPRAAS_API</strong></td>
<td>contract: invariant</td>
<td>Communication of information between the CEPRAAS staff actors is going to be performed via this interface.</td>
</tr>
<tr>
<td><strong>CEPRAAS_API</strong></td>
<td>contract: invariant</td>
<td>Communication of information between the CEPRAAS staff and the CEPRAAS backend is going to be performed via this interface.</td>
</tr>
<tr>
<td><strong>VCT_Subscriber</strong></td>
<td>contract: pre-condition</td>
<td>External actors (Company XY) need to provide basic identifying information in order to proceed with the VCT access. A unique id session token is produced by the backend communicated via this interface.</td>
</tr>
<tr>
<td><strong>VCT_Subscriber</strong></td>
<td>contract: invariant</td>
<td>Access control and verification of VCT staff credentials will be performed via this interface.</td>
</tr>
<tr>
<td><strong>VCT_API</strong></td>
<td>contract: invariant</td>
<td>This interface facilitates the communication of confidential information (provided by the Company XY) to the backend where storage and processing of the information is performed. Additional information communicated via this interface include the VCT staff interactions with the backend stored data and VCT process adjustments.</td>
</tr>
</tbody>
</table>

Diagram

The component described in this table is included in Figure 10: <Privacy flag platform> subsystem diagram representation.
3.4.2.2 Backend (Subsystem)

There will be three separate back-ends, i.e.: (i) Privacy Flag crowdsourcing platform; (ii) In-depth analysis tool, and; (iii) Voluntary compliance tool.

| Name Component | Name = Backend (Subsystem)  
Subsystem = Privacy Flag platform |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose (what, not how)</td>
<td>This component incorporates the activities performed in the server side by the privacy flag platform</td>
</tr>
</tbody>
</table>
| Inputs | Handles request for creation, deletion, modifications and authentication of actors’ credentials (UPRAAM_Subscriber, CEPRAAS_Subscriber, VCT_Subscriber)  
Request to access the hosted processing engines and database storage of information transacted with the application side (UPRAAM_API, CEPRAAS_API, VCT_API) |
| Outputs | Authorisation and Authentication of actors credentials (UPRAAM_Subscriber, CEPRAAS_Subscriber, VCT_Subscriber)  
Provide access to the post-processing information transacted with the application side (UPRAAM_API, CEPRAAS_API, VCT_API) |
| Dependencies | Application (Subsystem) |
| Interfaces | UPRAAM_Subscriber | provided  
CEPRAAS_Subscriber | provided  
VCT_Subscriber | provided  
UPRAAM_API | provided  
CEPRAAS_API | provided  
VCT_API | provided |
| Ports | AA_ServerSide | direction: bi-directional  
UPRAAM_API_SS | direction: bi-directional  
CEPRAAS_API_SS | direction: bi-directional  
VCT_API_SS | direction: bi-directional |
| Contracts | UPRAAM_Subscriber | contract: pre-condition | When a new installation of a browser add-on or a smartphone application instance, a unique identifier-id is communicated to the backend and stored. This unique identifier-id is utilised to authorise and authenticates every request for UPRAAM transaction by a device (smartphone or browser add-on) before any UPRAAM_API information is transacted with the UPRAAM backend. |
| | UPRAAM_Subscriber | contract: post-condition | After the unique identifier-id is issued subsequent UPRAAM interactions are cross-checked in the backend in order to avoid |
duplication of submitted information.

**UPRAAM Subscriber** | contract: invariant | Each transaction via the web-interface (data valuation or the IoT deployment assessment) unique identifier/session id is issued by the backend before the information with the UPRAAM backend is accessible.

**UPRAAM Subscriber** | contract: invariant | Verification by the backend subsystem is required in order for the UPRAAM staff to have access to the UPRAAM tools

**UPRAAM API** | contract: invariant | UPRAAM staff interact with the UPRAAM tools via this interface.

**UPRAAM API** | contract: invariant | Backend Subsystem provides access (via this interface) to the intelligence providers of the data produced by the UPRAAM assessment tools

**CEPRAAS Subscriber** | contract: invariant | All actors interacting with the CEPRAAS Subsystem authorisation and authentication of credentials utilise this interface.

**CEPRAAS API** | contract: invariant | Interfacing with the CEPRAAS tools and the backend throughput of information contract this interface.

**VCT Subscriber** | contract: pre-condition | When a new VCT session starts and the initial Company XY information are collected, a unique identifier-id is issued by the Application subsystem and the backend VCT processes and stores the credentials.

**VCT Subscriber** | contract: post-condition | After the unique identifier-id is issued subsequent VCT interactions are crosschecked in the backend in order to avoid duplication of submitted information.

**VCT Subscriber** | contract: invariant | Verification by the backend subsystem is required in order for the VCT staff to have access to the VCT tools and stored information.

**VCT API** | contract: invariant | VCT staff interact with the VCT tools via this interface

**VCT API** | contract: invariant | Backend Subsystem provides access (via this interface) to the intelligence providers of the data produced by the VCT assessment tools

**Diagram** The component described in this table is included in Figure 10: <Privacy flag platform> subsystem diagram representation
3.4.3 Application Subsystem integration
This is the description of the Application subsystem component diagram with the main interfaces and components. The description of components, ports and interfaces depicted from Figure 12 are included in subsequent sections.

![Diagram of Application Subsystem](image-url)

Figure 11: <Application> subsystem diagram representation
3.4.4 Backend Subsystem integration

This is the description of the Backend subsystem component diagram with the main interfaces and components. There are three distinct back-ends as already mentioned in the previous section. The description of components, ports and interfaces depicted from Figure 13 are included in subsequent sections.

Figure 12: <Backend> subsystem diagram representation
Conclusion

This deliverable provides architectural design of the Privacy Flag that relies on the requirements presented in D1.1 [2], extended with the use cases specified and the methodology identified for creating the platform architecture model enabling integration of the components, tools, mechanisms and protocols when they become available from the pending WPs. The methodology for specification of the architecture is based on IOT-A ARM model used as a ground for defining communication flows, building blocks and high-level architecture and revised to support more software-oriented system design.

In addition, technical specification in this deliverable presents different architectural views for the application and backend subsystem taking into account Privacy Flag use-cases scenarios describing in detail application, browser add-on and crowd source monitoring with distributed agents to identify interfaces of the architecture and its integration design.

The reference architecture will be updated through iterative cycles during the project lifetime as input from pending WPs becomes available, revising interface definition, communication flows and adding building blocks to specify latest version of the Privacy Flag platform.

The resulting architecture model will enable autonomous crowd-sourcing, evaluation of the crowd-sourced data, risk assessment using different agents, algorithms and external tools.
References


Annex A. Subsystem component specification template

| name Component | Name = name  
|                | Subsystem = name |
| Purpose (what, not how) | freeform description |
| Inputs | * freeform description (interface name) |
| Outputs | * freeform description (interface name) |
| Dependencies | * name (actor or component or subsystem or external) |
| Interfaces | * name | provided or required |
|            | (tip) provided interface: one supplied by this component |
|            | (tip) required interface: one supplied by another component (i.e. dependency) |
| Ports | (tip) interaction points |
|        | * name | direction: input or output or bi-directional |
|        | (tip) bi-directional = a port has both required & provided interfaces; |
|        | (tip) output = a port has only required interfaces; |
|        | (tip) input = a port has only provided interfaces; |
| Contracts | (tip) explanation of key constraints & behaviours, per interface or applied to whole component |
|        | * interface or whole | contract: pre-condition or post-condition or invariant | explanation |
|        | (tip) pre-condition: that which must be true when interface or component is invoked |
|        | (tip) post-condition: outcome when pre-conditions are true |
|        | (tip) invariant: that which must always be true |
| Diagram | (tip) cross-reference uml2 component diagram of link to diagram |

Table 4: <name> component – component specification