PRIVACY FLAG PROJECT

Requirements & Architecture

INFOCOM World 2016
Privacy Flag - based Special Session
Athens, 2nd November 2016

Prof. Nancy Alonistioti
National & Kapodistrian University of Athens

PRIVACY FLAG

Co-funded by the European Union

Co-funded by the Swiss Confederation

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

Conceptual Position & General Information

- Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things (IoT) deployments.

- European Research Project under the *H2020 Framework Programme*

- Digital Security Call:

Cybersecurity, Privacy & Trust, H2020-DS-2014-1

Co-funded by the European Union

Co-funded by the Swiss Confederation

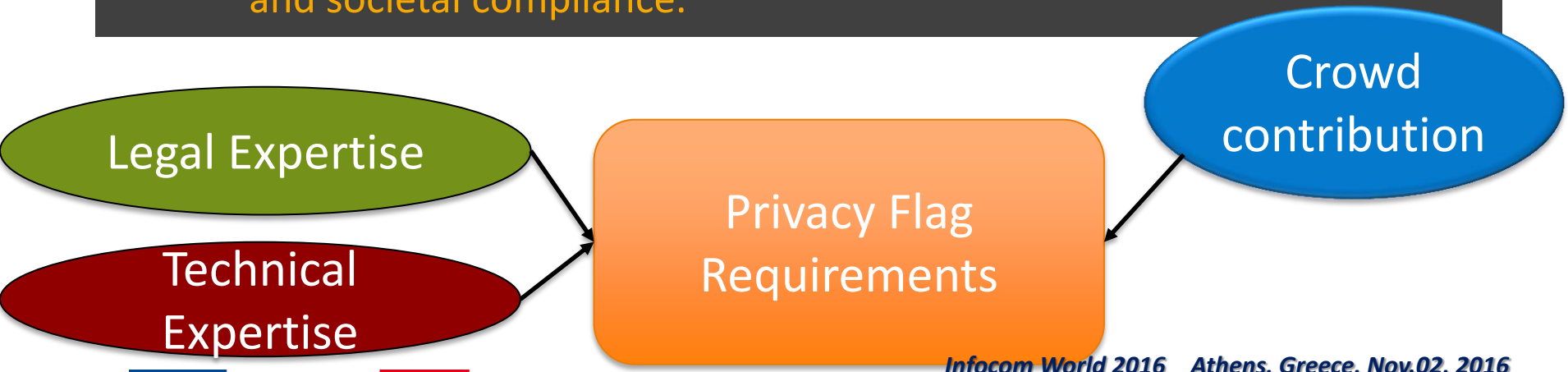
Key Challenges

- The frequent revision and modification of contents due to the approval of the **General Data Protection Regulation (GDPR).**
- The **combination of both legal and technical aspects** in generating the project requirements.
- **Represent the relevance of the legal aspects within the scope of the project**
- **Provide updated and pertinent requirements**
  - By ensuring close interaction between the partners
  - By involving the users into the creation of the system

Co-funded by the European Union
Co-funded by the Swiss Confederation

Project Achievements

- Identified, analysed and specified the Privacy Flag requirements from different perspectives, including:
  - ***Legal requirements*** related to the personal data protection and data ownership, with a focus on European and international law, following also the new GDPR.
  - ***Technical requirements*** related to platform scalability, efficiency, reliability and security.
  - ***Societal and end-users requirements***, related to end-user acceptance and societal compliance.

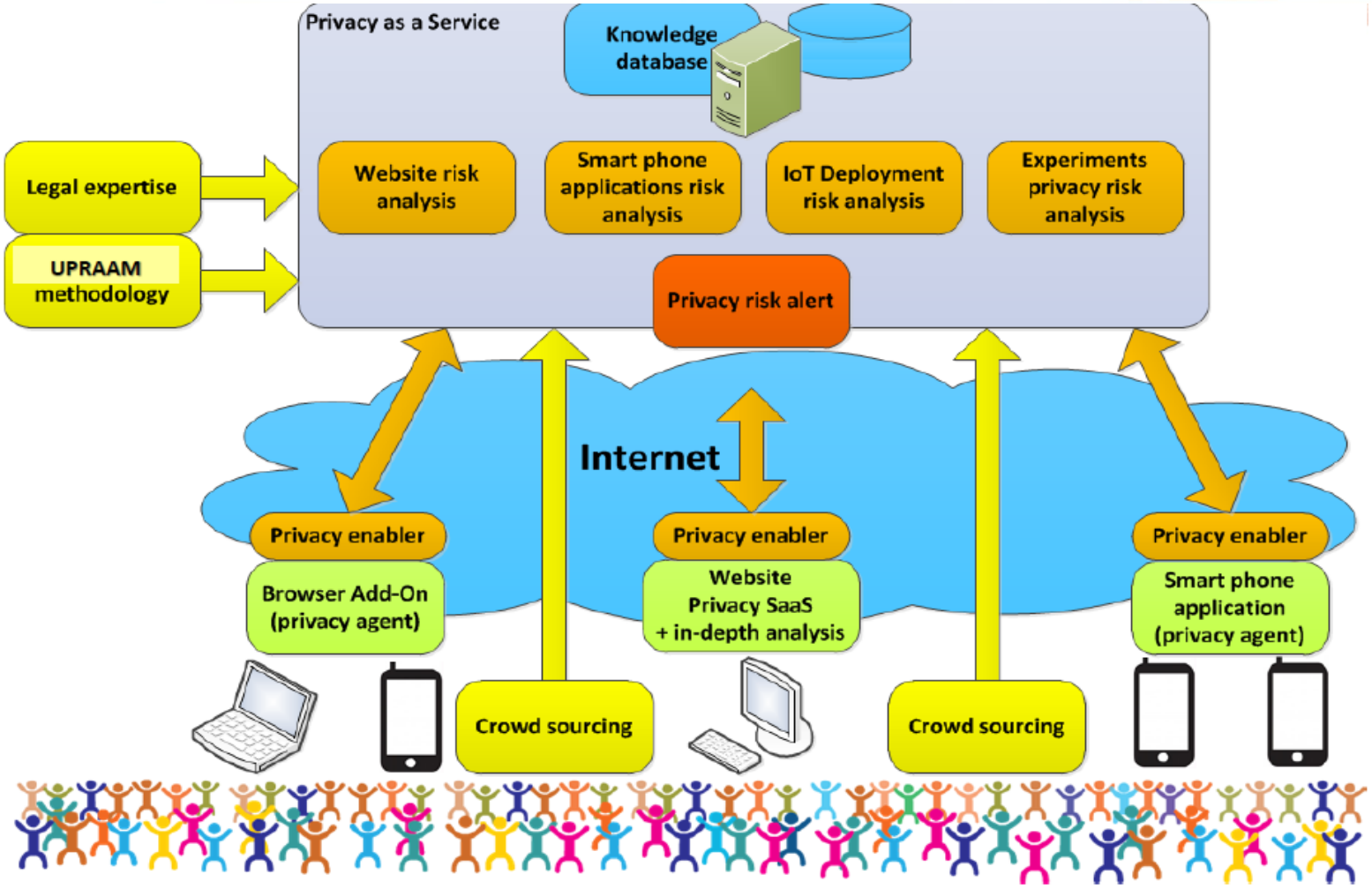


Co-funded by the European Union
Co-funded by the Swiss Confederation

High level Architecture and Process

PRIVACY FLAG

1. *Three user-friendly and freely available tools for citizens*
2. *Distributed crowd-sourcing privacy monitoring platform*
3. *Universal Privacy Risk Area Assessment Tool & Methodology (UPRAAM)*
4. *Privacy enablers*
5. *Global knowledge database on privacy risks*



Co-funded by the European Union
Co-funded by the Swiss Confederation

PRIVACY FLAG

Legal Requirements following the new GDPR (most critical)

Requirement	GDPR Directive	Project relevance
Purpose Limitation	Purpose limitation principle set forth by Recital 28 of the *Data Protection Directive*, in conjunction with Article 6(1) b). Art. 29 WP has provided an in-depth analysis of this principle in its *Opinion 03/2013 on purpose limitation*.	• **Privacy Flag services will process user's and SMEs' data for legitimate, specific and explicit purposes, determined at the time of collection.** • **Purposes of the data processing will be well defined** • **No need for expert legal or technical knowledge**
Data Minimization	Article 6(1) c) - normative base of data minimization - of the Data Protection Directive. Art.29 WP Opinion 02/2013 underline the necessity to collect: • data that are strictly necessary to perform the desired functionality.	**Collected data will be adequate, relevant and not excessive in relation to the purposes for which they are processed, in order to prevent unnecessary and potentially unlawful data processing**
Data accuracy and updating	Article 6(1) d): The normative base of data accuracy and updating of the Data Protection Directive	**Natural or legal person data, which are inaccurate or incomplete, having regard to the purposes for which they were collected or processed, will be erased or rectified.** • **E.g. SME and user will have access to a personal area on the website, so as to register themselves and they will always have the possibility of modifying the information provided.**

Co-funded by the European Union
Co-funded by the Swiss Confederation

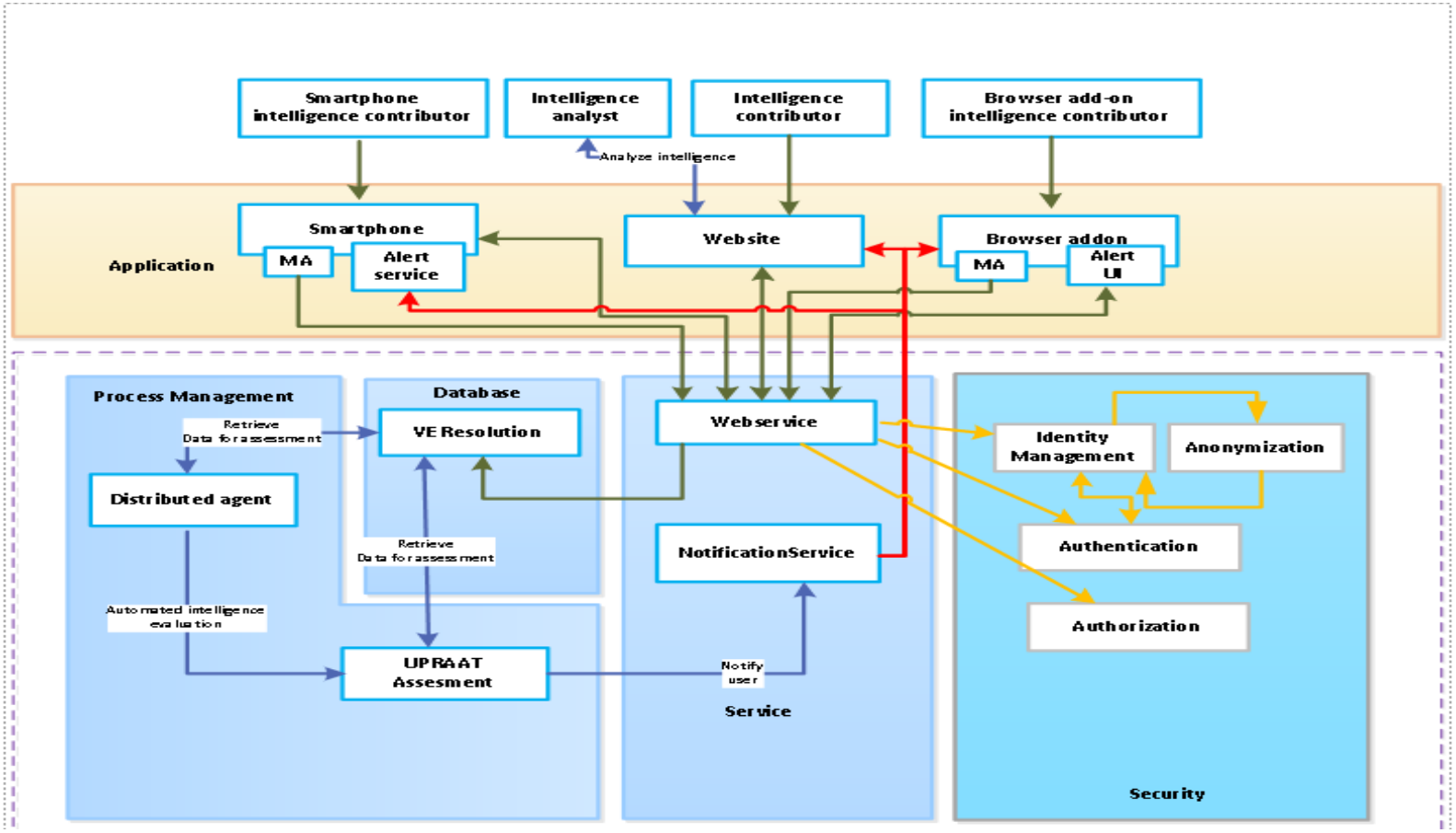
PRIVACY FLAG

Legal Requirements following the new GDPR (most critical)

Requirement	GDPR Directive	Project relevance
Data anonymization and pseudonymization	Article 6(1), Article 15(1), Opinion 05/2014 on Anonymization Techniques written by the Art. 29 WP, Regulation 679/2016 on personal data protection, Regulation in Article 32(1)(a)	**Privacy Flag must ensure that data are irreversibly anonymised and aggregated, permitting identification of data subjects for no longer than is necessary. Pseudonymization should be set as the default option, when anonymization is not possible.** • **A code is attributed to each user when using the Services for the project's purposes.** • **Re-identification of users takes place only if strictly necessary to prevent frauds, misuse of the Services etc.**
Information to data subject	Article 10 of the *Data Protection Directive* -> minimum level of information to be given to any data subject, except where he/she already has it, before collecting his/her personal data and/or seeking his/her consent.	**On Privacy Flag website, the Consortium provides a privacy policy referred to all of its tools specifying information about data collection and use, their sharing etc.**
Unambiguous Consent	In accordance with Recital 30 of the Data Protection Directive (*"In order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject"*). In addition with Article 7 paragraphs a) to f) and Art.29 WP.	**Personal data will be processed, in principle, if the data subject has given a prior informed, specific and freely given consent, that must be specific to the processing of special and location data. Exceptions to the latter rule will be applied in specific cases**

Co-funded by the European Union
Co-funded by the Swiss Confederation

First Privacy Flag Architecture based on the requirements



Design of the first version of the Privacy Flag architecture

Co-funded by the European Union
Co-funded by the Swiss Confederation

Technical Requirements – The most critical

Requirement	Project relevance
Project data management **(Process Management Component)**	**The system:** • **must automatically record all enablers/tools generated data, storing these data into the Privacy Flag platform, minimizing the collection of personal data from the crowd.** • **will provide interfaces that allow all tools and enablers to send data to the Privacy Flag platform.**
Prior Information Notice **(Notification Service Component)**	**Before the download of Privacy Flag enablers, users will receive prior information about his/her personal data processing with a brief project purposes description.**
Users' source access **(Security Component)**	**Persons in charge of the processing will access only on the sources to which the user has given his/her consent or to which another legal basis is applicable.**
Anonymization **(Security Component)**	**The Security and Privacy Enabler (SPE) will ensure that all connections of an end-user are appropriately anonymized. Users of the system will leave digital marks such as their IP addresses in each communication attempt. The system must enable the hiding of such identifying characteristics from a third party.**

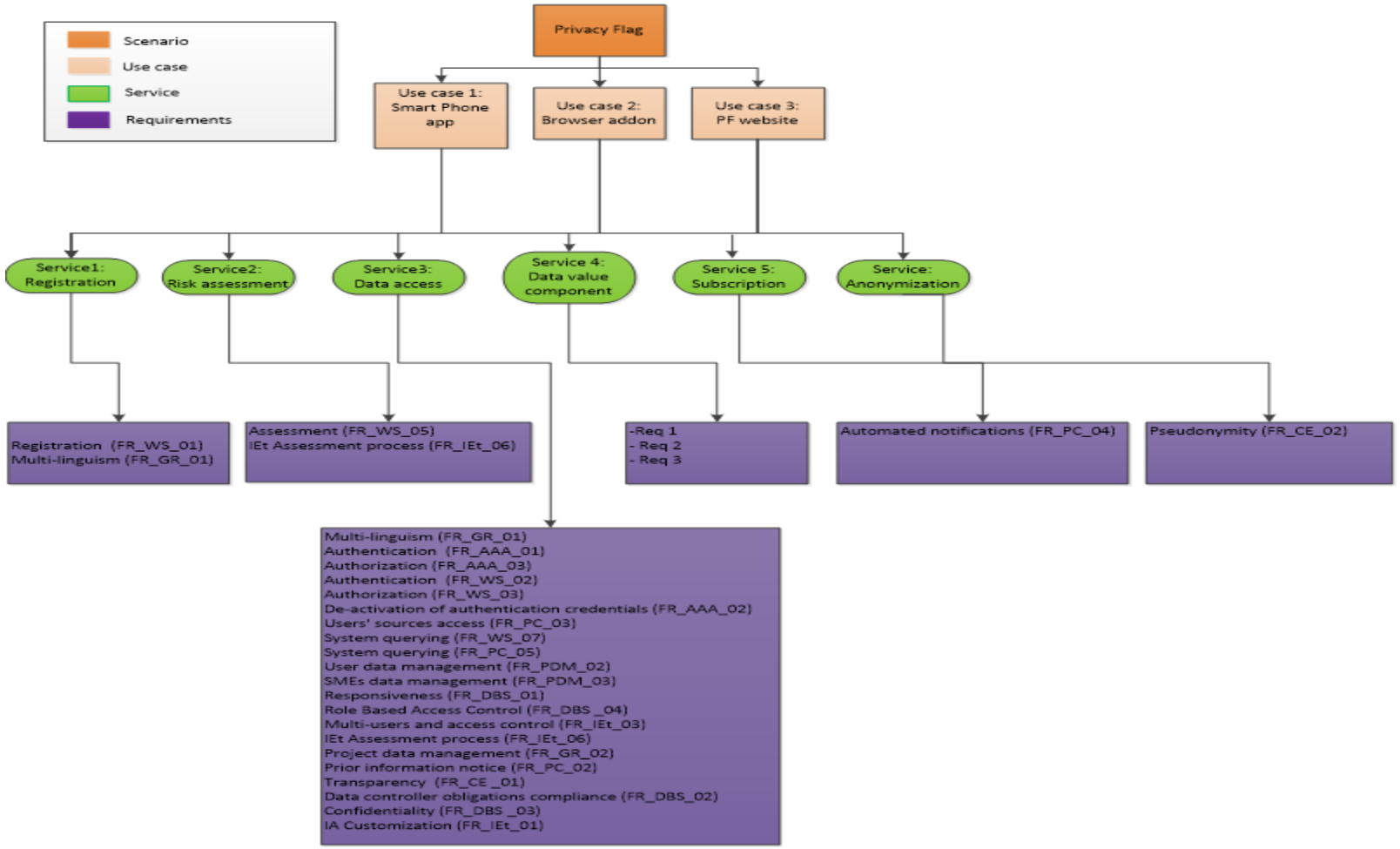
PRIVACY FLAG

Technical Requirements – The most critical

Requirement	Project relevance
Data integrity and confidentiality **(Database Component – VE Resolution)**	**The system:** • **must ensure that the data stored and exchanged between the subject and the system itself will not be accidentally modified during the storage/exchange or corrupted by a third non-authorised party** • **must guarantee that said data are confidential and they are not disclosed to unauthorised persons.**
SMEs Data Management **(Security and Database Components)**	**The system will enable SMEs to easily provide required information, data and document required for the in-depth analysis in view of the certification or labelling process.**
User Data Management **(Security and Database Components)**	**In case of personal data collection, the system enables users to control their personal data, to access, rectify, delete or block them. Users can always change the sets of data that they have shared.**
End-to-end security **(Security Component)**	**"full lifecycle protection". It is a paradigm of an interrupted protection of data transferring between two communicating parties without being intercepted or read by other parties.** **At the end of the participation to the project (app/add-on uninstallation or in-depth analysis withdrawn), all collected data will be destroyed.**

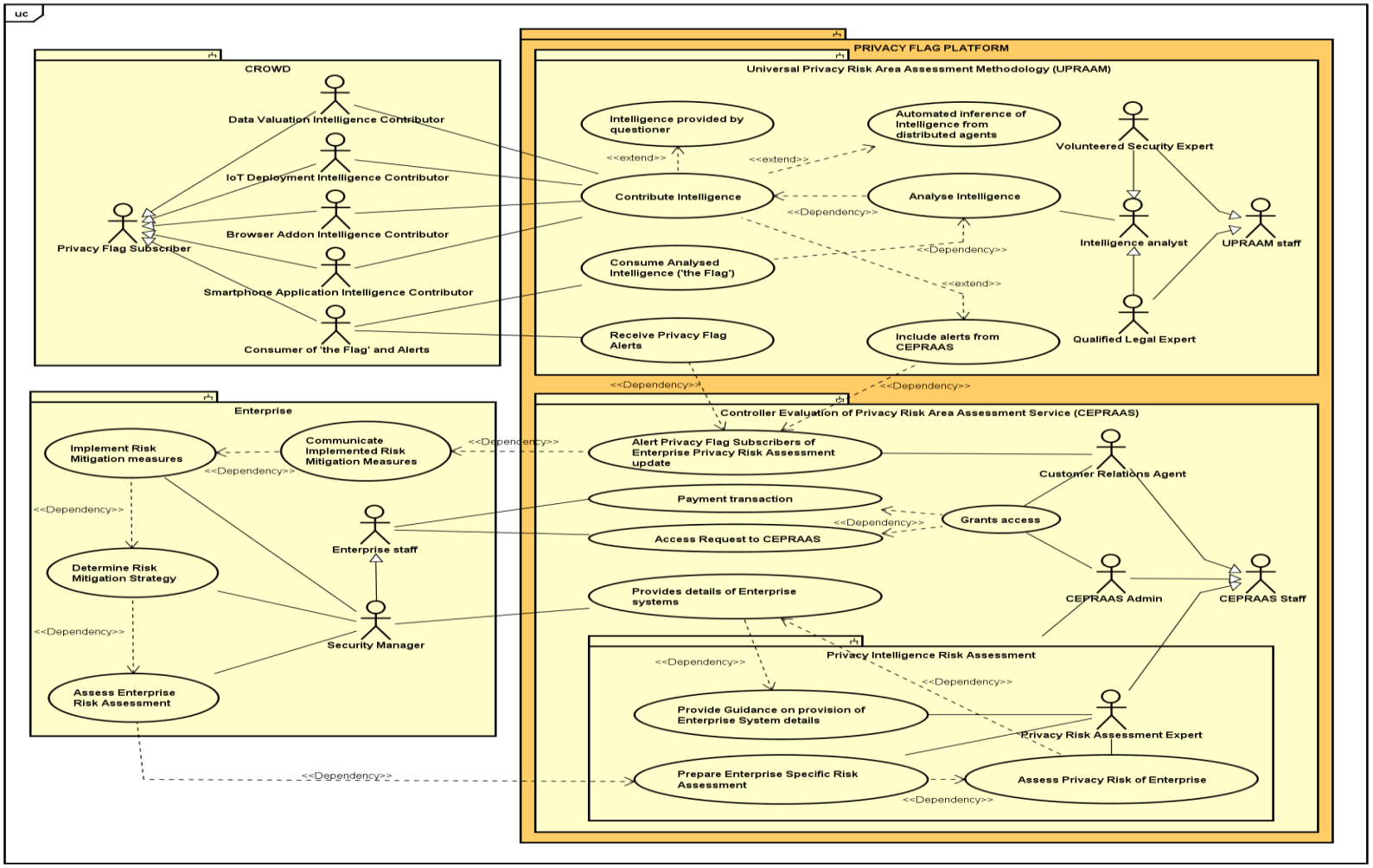
Co-funded by the European Union
Co-funded by the Swiss Confederation

Use Case Requirement Classification



Co-funded by the European Union
Co-funded by the Swiss Confederation

Context View of the Privacy Flag Platform



PRIVACY FLAG

Thank You for your Attention

Questions ?

Contact Details

http://www.privacyflag.eu/

https://twitter.com/privacyflag

https://www.facebook.com/privacyflag/?fref=ts

SCAN Lab - http://scan.di.uoa.gr/

nancy@di.uoa.gr

Co-funded by the European Union

Co-funded by the Swiss Confederation