

Privacy Flag – Overall Architecture Evolution

DNET

Infocom

October 25, 2017

Athens, Greece

Dr. Nenad Gligoric



**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



PRIVACY FLAG

Architecture design overview

Objectives:

- To define and analyse requirements from end user perspective
- To define the platform processes
- To design guidelines for the envisioned components
- To research and design an adequate architecture to be used by Privacy Flag



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

Problem description and methodology

- ❖ *There should be a clear link between architecture and requirements to allow delivered technology to be a “complement” to the privacy and legal aspects*
 - Use cases are identified and presented
 - Set of legal and functional requirements were drafted
 - Architecture is first drafted based on IoT-A referenced model
 - Model is further developed by using UML



Co-funded by the
European Union





Co-funded by the
Swiss Confederation



PRIVACY FLAG

Definition of 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:
 - ❖ Smartphone application,
 - ❖ Browser Add-on (BAO),
 - ❖ Distributed Agents (DA) and a
 - ❖ Crowdsourcing Evaluation Tool (CET).



Co-funded by the
European Union

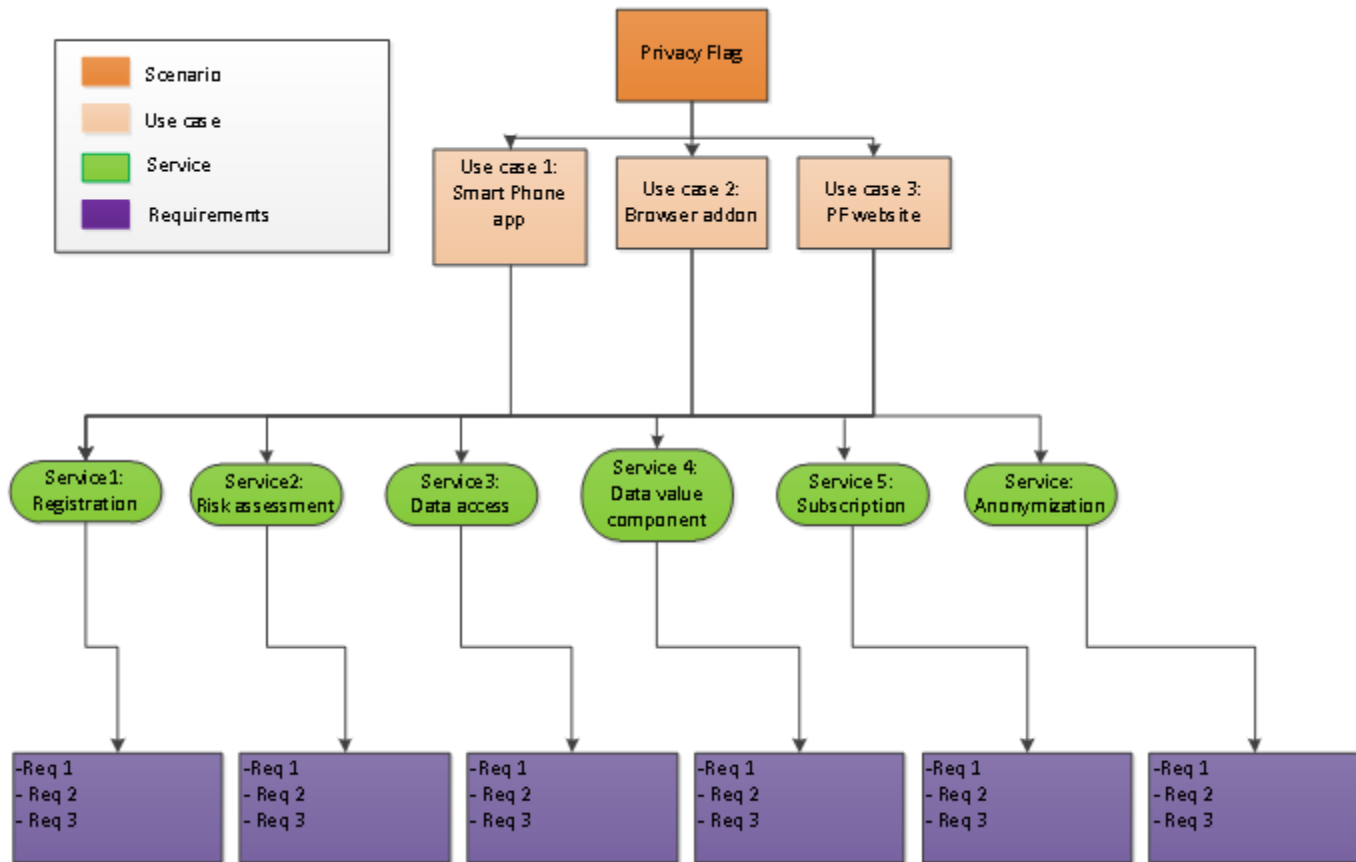


Co-funded by the
Swiss Confederation



PRIVACY FLAG

Definition of use cases





PRIVACY FLAG

Definition of use cases



Co-funded by the European Union

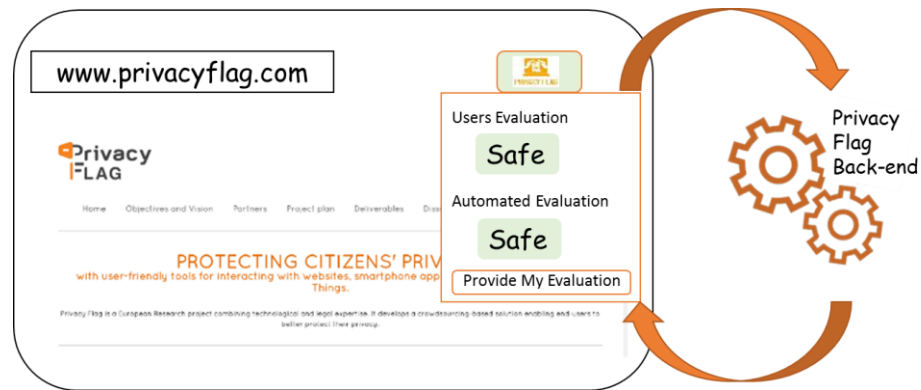


Co-funded by the Swiss Confederation



PRIVACY FLAG

Definition of use cases



Co-funded by the
European Union

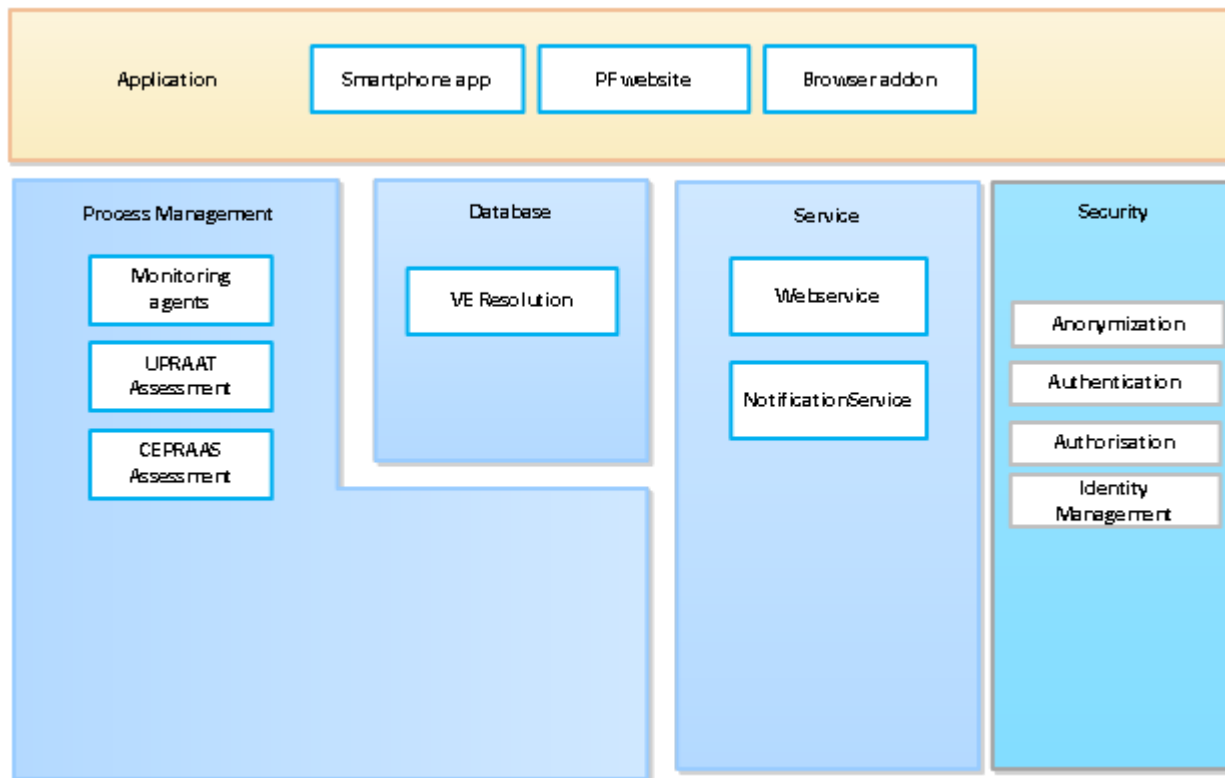


Co-funded by the
Swiss Confederation



PRIVACY FLAG

Mapping of Privacy Flag to IoT-A



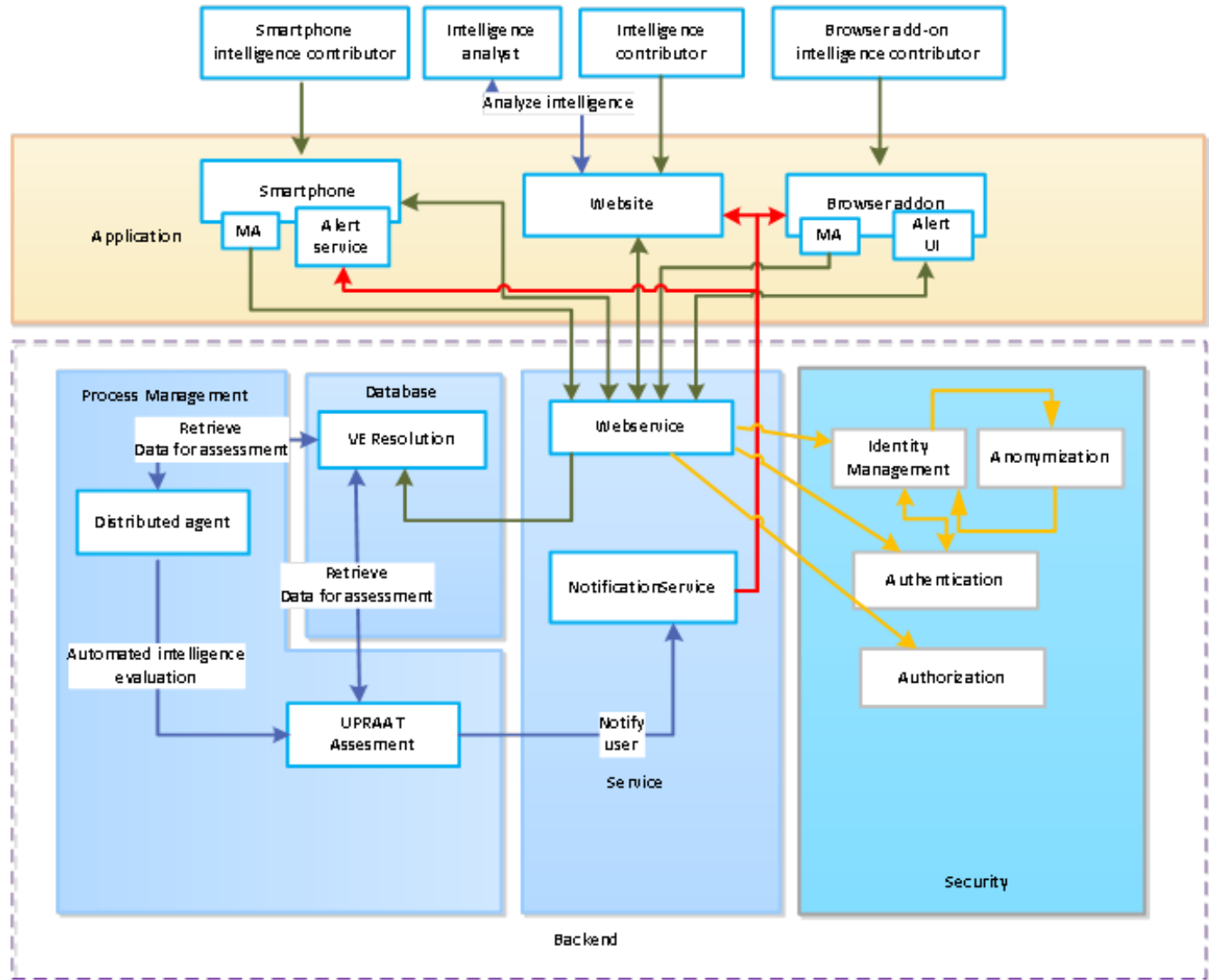
Co-funded by the European Union



Co-funded by the Swiss Confederation



PRIVACY FLAG



Co-funded by the European Union



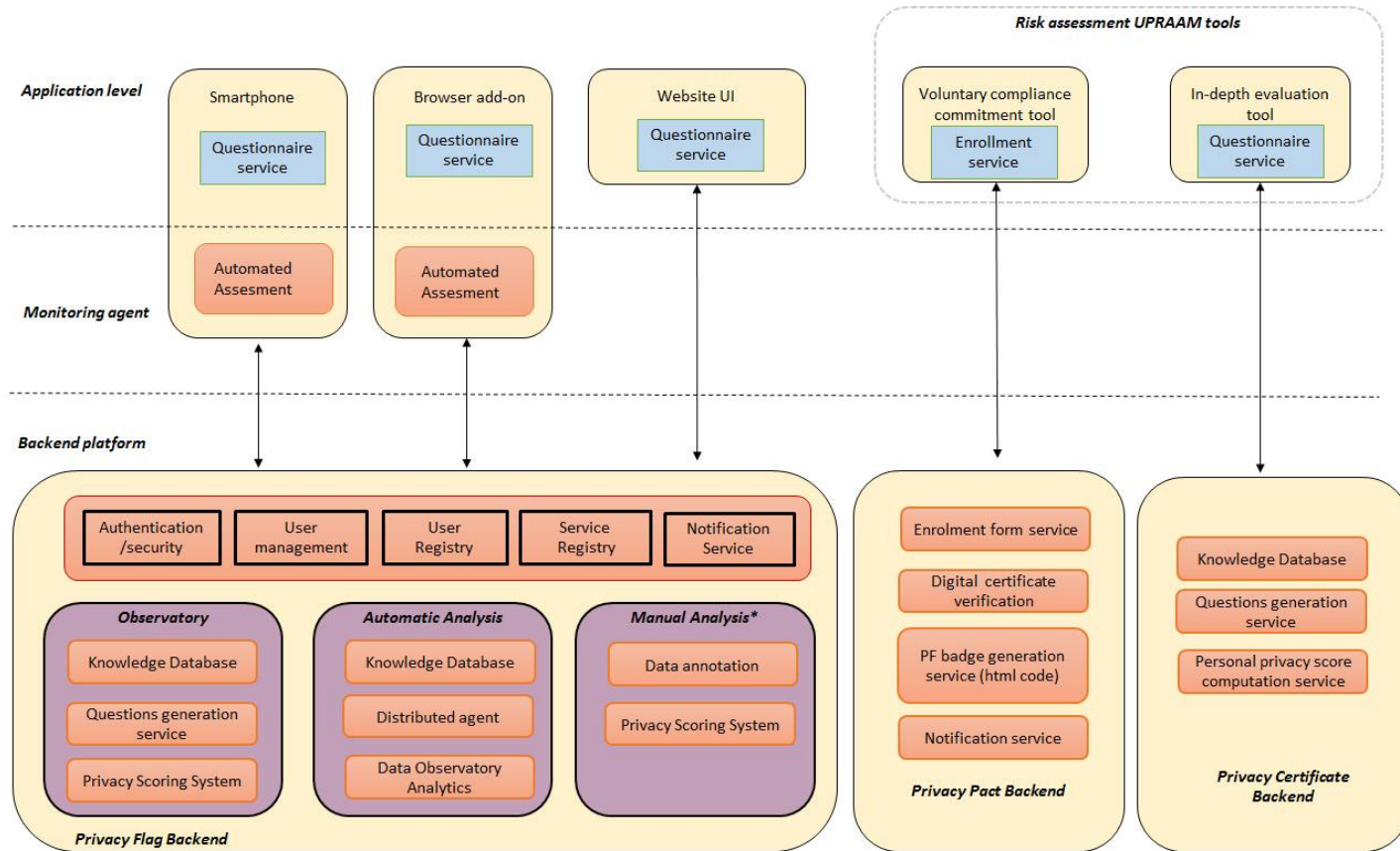
Co-funded by the Swiss Confederation



PRIVACY FLAG

Year 2: Updated architecture design

- Project's overall architecture design is updated, based on ongoing WPs (WP2-4)
- Approach was oriented mainly toward inclusion/update of processes and work developed in the 2nd year of the project
- Suitable modifications are done to the architecture, information views from IoT-A are used in the previous document for use case modelling



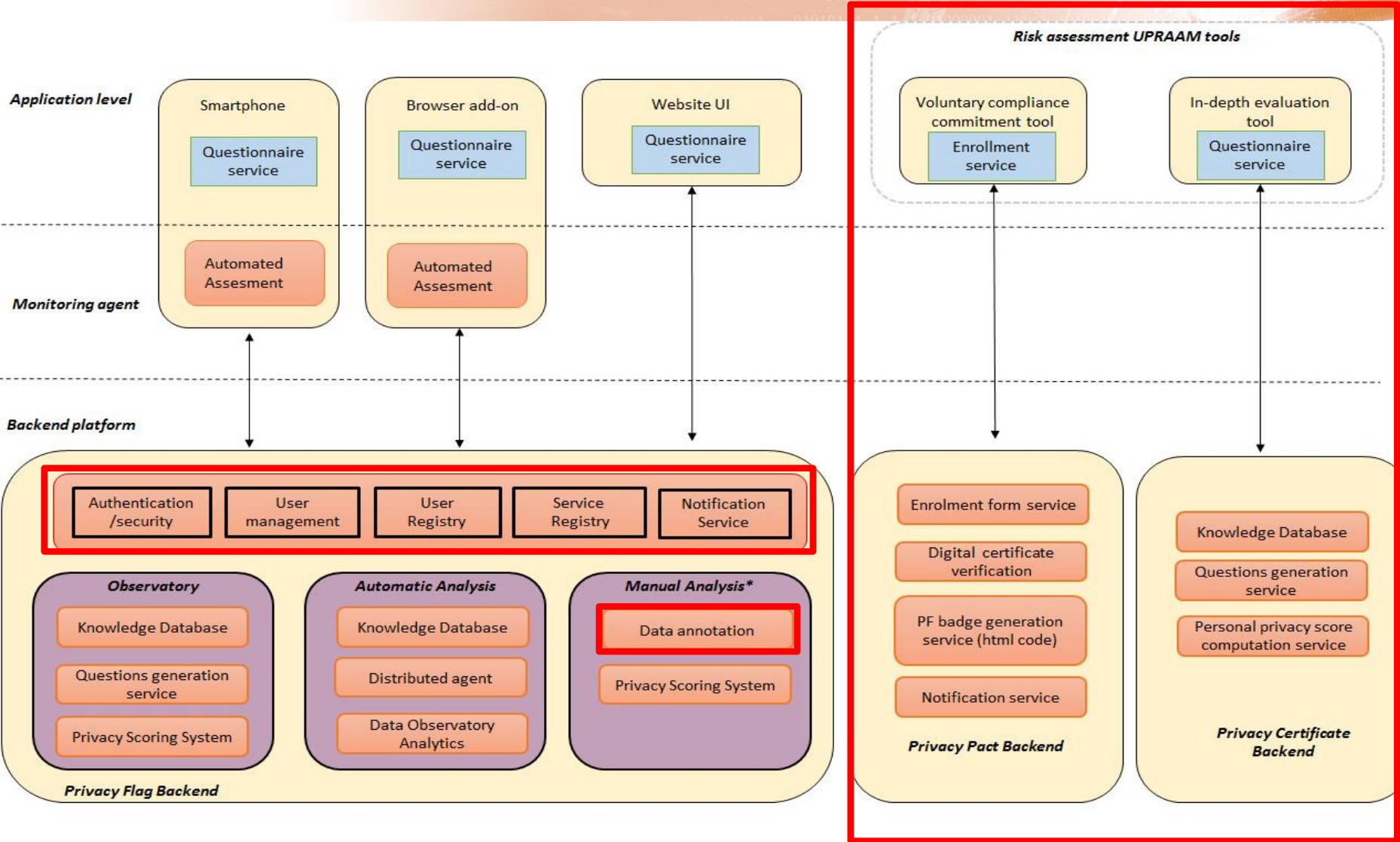
*Manual analysis is done for any evaluation annotated manually by the Privacy Flag users (experts, contributors, etc.)



Co-funded by the European Union



Co-funded by the Swiss Confederation



*Manual analysis is done for any evaluation annotated manually by the Privacy Flag users (experts, contributors, etc.)



Co-funded by the European Union

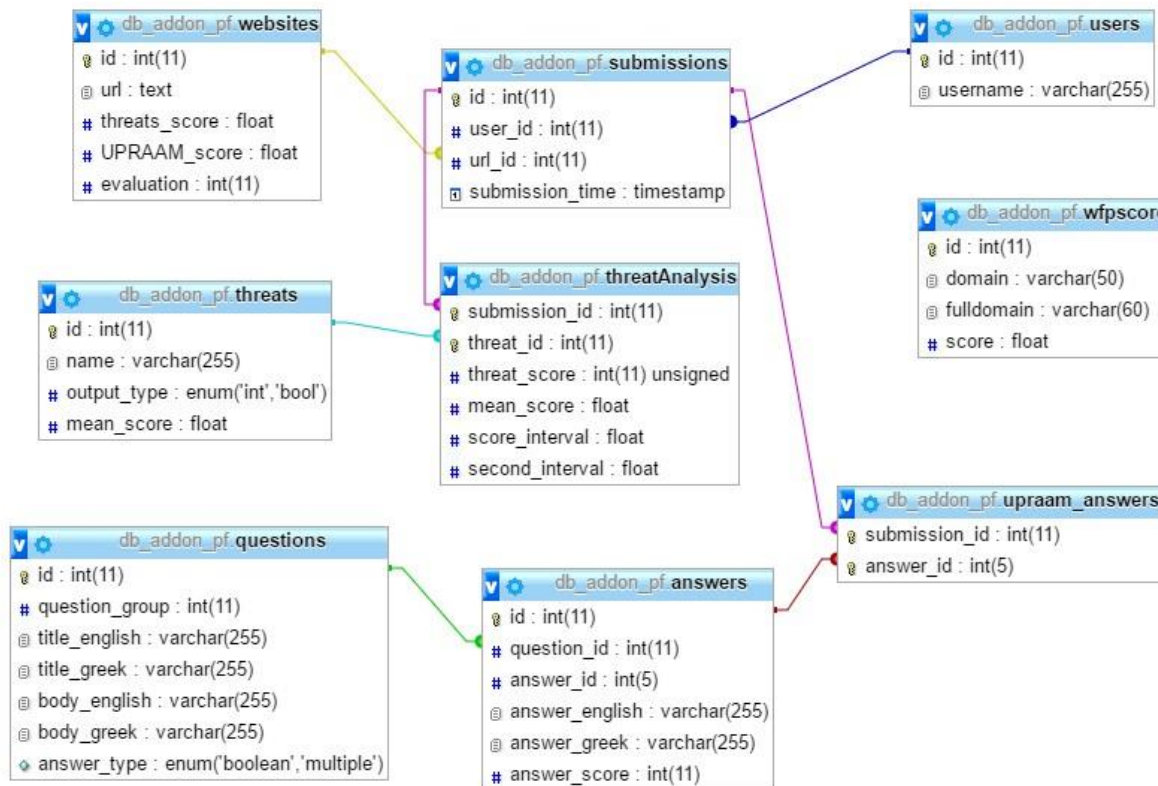


Co-funded by the Swiss Confederation



PRIVACY FLAG

Database datamodel v1



- To extract the data model, the use cases are at first, individually analyzed and then merged to create a preliminary data model.
- This model is taken as the ground for defining in depth the models for end user tools





PRIVACY FLAG

APIs

Name	getAndroidEvaluation	
Description	This API extracts the evaluation for the android applications kept in the Privacy Flag data storage as an array containing package names as ids. To obtain the evaluations, the array with IDs of the applications is sent in the request body	
SERVER URL	Disclosed for security reasons	
Method: POST	/smartphone/application/sync/	
HEADERS		
	Content-type	application/json
	Accept	application/json

Request Payload:





```
{
  "applist": [{
    "package": "com.test1.google",
    "name": "Google+"
  }, {
    "package": "com.test1.viber",
    "name": "Viber"
  }, {
    "package": "com.test1.whatsup",
    "name": "Whatsup"
  }, {
    "package": "com.katana.facebook",
    "name": "facebook"
  }, {
    "package": "com.pay.pal",
    "name": "Paypal"
  }
]
```

- APIs are specified and already used to foster the integration
- The format is uniform and it uses standard description for fields used for making an API calls (server url, header, request payload, response messages, etc.)
- Server URLs are being removed to avoid potential security issues



PRIVACY FLAG

Key challenges

-  **Legal aspect:** The revision of the architecture and modification of contents in relation with the General Data Protection Regulation (GDPR).
-  Privacy by design for the components
-  Achieve scalability with the architecture to allow collection of large crowdsourcing datasets
-  Effort that took place as a part of end user evaluation in WP5 were providing feedback to enhance and improve WP2-4 tools, that also had impact to the architecture



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG

3rd Year priorities

- **Compliance check for all tools, enablers and mechanisms coming from the project with the GDPR (T8.1) will be the focus of the Y3**
- **Provide final architecture design specified and handed on as final architecture document**



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



PRIVACY FLAG



PRIVACY FLAG

Thank you!

www.privacyflag.eu



Co-funded by the
European Union



Co-funded by the
Swiss Confederation



National and Kapodistrian University of Athens



PRIVACY FLAG



Co-funded by the European Union



Co-funded by the Swiss Confederation