FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013   Duration: 48 months

D5.3 Realisation of "Ask The Expert" function

Due date of deliverable: 31/10/2014
Actual submission date: 06/11/2014

Revision: Version 1

Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA)

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Authors	Alberto Tofani (ENEA), Antonio Di Pietro (ENEA), Rafal Kozik (UTP), Rafal Renk (UTP)

Security Assessment	Hanneke Duijnhoven (TNO), Michal Choras (UTP)
Approval Date	4.11.2014
Remarks	No issues.

TABLE OF CONTENTS

1   Introduction

1.1   Purpose of the document

The objective of this document is to present the realisation of one of the objectives of the CIPRNet project, the "Ask The Expert" (ATE hereafter) service. The ATE service allows users to ask for support of the CIPRNet consortium regarding topics of different nature in the domain of CIP. According to the users' specific requests, it selects CIPRNet experts that have proper expertise to provide support to users. Anonymisation of the query and protection of both data and queries are implemented by the ATE service to ensure secure protocols for the authentication of the user.

The proposed ATE service will be one of the key capabilities of the CIPRNet Virtual Centre of Competence and expertise in CIP (VCCC in the following) Portal which will allow to disseminate CIP experts' knowledge and experience, organise workshops, take part in conferences, moderate discussions, and finally, organise and provide a set of lectures to relevant communities (see [4]).

1.2   Link to other CIPRNet deliverables

In this section, we identify the connections of the ATE service (and its components) with other CIPRNet products showing also the interaction of users with the different products.

The ATE service will rely on information regarding experts and their related expertise stored within the CIP Inventory Database (see [1][5]). The CIP Inventory Database will be maintained and updated during the remainder of the CIPRNet project to provide CIP reference material for the CIP community. Moreover, the ATE service implements and extends the general service requirements formalised within deliverable D5.2 (see [3]). The relations with the other deliverables are summarised in Fig. 1.
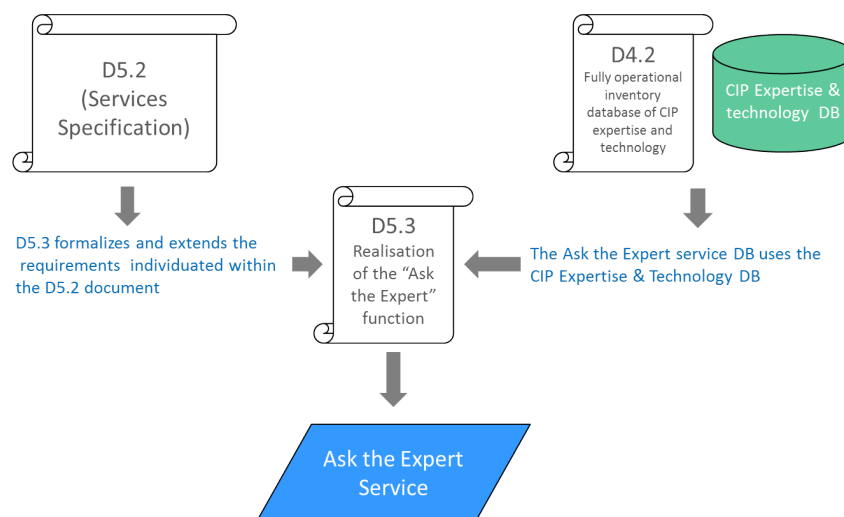

Fig. 1 Relations of D5.3 with other CIPRNet deliverables.

1.3 Document structure

The present document is organised as follows:

- **Chapter 2** describes the main features of ATE service, the different users and discusses the pros and cons of the different access control management models underlying the service;
- **Chapter 3** describes the functional and non-functional requirements of the ATE service;
- **Chapter 4** describes the architectural concepts of the ATE service and its implementation choices;
- **Chapter 5** describes the roadmap for future features of ATE service;
- **Chapter 6** draws some conclusions and the next steps to refine the current ATE service version;
- **ANNEX I** describes the open source platform Yii used to implement the ATE service.

2 The overview of the ATE service

2.1 Role of the service

The "Ask the Expert" (ATE) service is intended to provide the CIP stakeholders with following capabilities:

- to request information about any CI aspect related to CI operation, threats, management, etc.
- to get feedback on such query from the CIPRNet community of experts.

The ATE service will be part of the CIPRNet VCCC portal. Through the VCCC the end-users will be capable of submitting questions and problems related to CIP domain, which are perceived to be of different nature, e.g.:

- Technical CIP-related issues;
- CI management, crisis management for CI;
- CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data;
- Practical aspects of CI functioning.

2.2 The Actors/Users of the Service

2.2.1 Administrator/Moderator

The *Administrator* is the person who plays the role of the service moderator. He/she is responsible for the maintenance of: database of experts, types of expertise, request provided by users, etc. She/he is responsible for managing the current status of experts (e.g. their willingness to participate to the ATE service), maintaining the up-to-date data related to experts' domain of expertise, contact information, conflicts/issues resolving, historical data maintenance, etc.

The Administrator is responsible for appropriate utilisation of experts, which means that she/he will encourage less active experts to be more involved in process of end-user problems resolving. The administrator is also in charge of controlling that end-user requests are timely resolved.

Moreover, the Administrator is also required to have the broad view on current end-users problems. As a result she/he produces and maintains the list of frequently asked question, in order to provide the sufficient quality of the service and to avoid the same problems asked multiple times.

2.2.2 Expert

The *Expert* user will be selected among a pool of experts provided by WP4 in the inventory database. She/he will be required to provide the consent to participate and to contribute to the ATE service. The responsibility of the Expert will be to reply to end-user requests. She/he will have the capability to register and maintain the requests.

The Expert will have also the ability of resubmitting a specific request to the more appropriate CIPRNet expert in case of unavailability or incapacity of processing the request.

2.2.3   End-user

The ***End-user*** is the type of the ATE actor to whom the service is dedicated. She/he is able to send a request using pre-formatted form (e.g. a form including subject, description, domain type/name fields) to appropriate pool of experts.

Moreover the End-user has the ability to define the priority of the request in order to signalise the expert the given matter is urgent and requires fast response.

2.3   General use cases

In this section general use cases of the ATE service are presented. The UML diagram is presented in Fig. 2. More detailed description on given use case are given in Table 1.
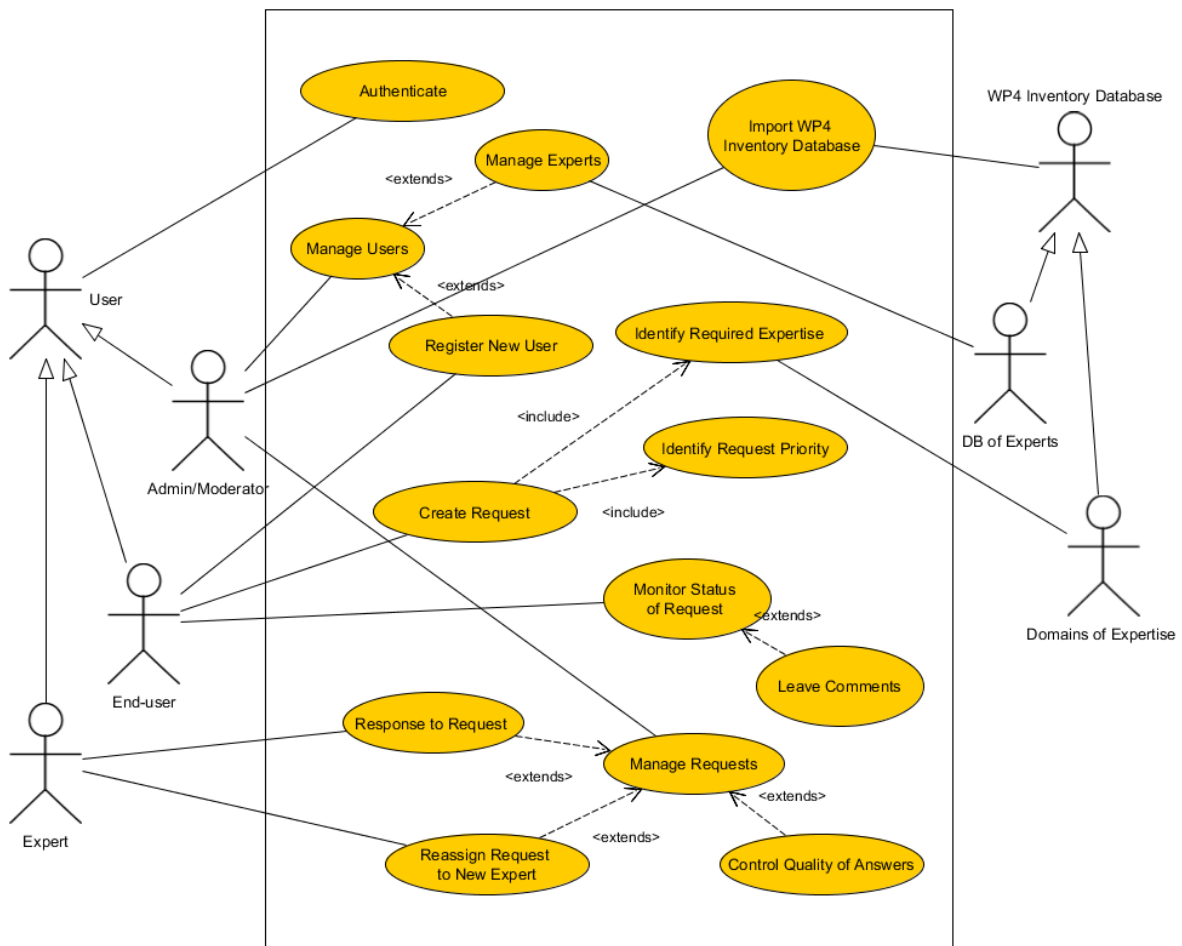

Fig. 2 General use cases of the ATE service.

Table 1: List of general use cases of the ATE service

Use-case	Description
Authenticate	Allows different user to be authenticated and authorised to the ATE service.
Manage Experts	Allows the Administrator/Moderator to manage the pool of experts. It will require data from WP4 Inventory Database.
Import W4 Inventory Database	Provides mechanism to import (from WP4 inventory database) the information related to the experts and their domains of expertise.
Manage Users	Allows the Administrator to manage the user of the ATE service. It allows for users roles management and their modifications.
Register New User	It is an extended use case of "Manage Users". I allow the End-users to register to the ATE. I also allow the Administrator to create new accounts.
Identify Required Expertise	It uses the WP4 Inventory Database to provide the list of possible types of expertise.
Identify Request Priority	It allows the End-user to specify how urgent the request is.
Create Request	It allows the End-user to create new request.
Monitor Status of Request	It allows the End-user to monitor the status of her/his request. It also allows the moderator to monitor the effectiveness of different experts and assess their engagement.
Leave Comment	It allows the End-user to leave the comment related to expert answer.
Manage Request	Provides the Administrator/Moderator means for managing the request.
Response to Request	Allows the expert to provide answer related to particular request.
Control Quality of Answers	Allows the Administrator/Moderator to control the quality of answers provided by experts.
Reassign Request to New User	It allows the Expert to resubmit the request to other expert (e.g. more appropriate to that query).
Reassign Request to a new Expert	It allows one Expert or the Administrator to reassign the request to a more appropriate Expert

2.4 Overview of access control management models

In order to provide the mentioned above functionalities of the service, it is required to adapt appropriate access control model, which will be able to meet the requirements with respect to the end-user needs, flexibility (in the sense of user management), and scalability.

In this section we have analysed different Access Control (AC) models in order to identify the most appropriate ones for the ATE service. Commonly, Access Models use different techniques that allow assigning different security attributes for users and resources (see [6]). These techniques allow implementing an appropriate balancing between finesse and coarseness of security rules.

An example of coarse access control rule may be: "*Experts can close a request*", while "*An expert can close the rule if she/he has confidentiality level 2 and the request is related to domain the expert is assigned*" is an example of very fine-grained access control rule.

A very fine-grained model allows specifying complex access control rules; however, it may become less scalable and hard to maintain for complex multi-resource/multi-users systems. However, a coarse-grained model will be less complicated to maintain although in some cases it may be difficult to define specific access control rules for specific users.

2.4.1   MAC – Mandatory Access Model

MAC [6] model assigns security attributes both for user and resource.

It allows the Administrator to define different levels of confidentiality. Indeed, this model is used in systems of high relevance (e.g. military/governmental systems). Under these policies, users can only access resources that have the same or lover security attributes (e.g. confidentiality level). Moreover, in a MAC model only the Administrator can define the security models and policies; users cannot have any influence on access control mechanisms.

Table 2: MAC advantages and disadvantages

Advantages	Disadvantages
This type of AC allows the Administrator to define very fine-grained (detailed) access control mechanisms.	Maintaining different levels of confidentiality implies a management burden.
	It may turn out that, in case of the ATE service, this method will not scale well for large pool of Experts and End-users.

2.4.2   DAC – Discriminatory Access Model

DAC [6] is a traditional access control method provided by Linux-like operating systems. In such a model, only the owner of the resource controls access permissions. The owner decides who can access the resource and what operations are allowed. Examples of solutions adapting DAC model are access control mechanisms used by LINUX and Windows systems. In this case, if user is not on the list of users assigned to that resource (e.g. Linux group), or the action requested by user is not permitted (e.g. write action) then the user is denied the access.

In contrast to MAC model, DAC allows the user to influence the access control mechanism: users may create objects (e.g. files) and allow defined group of users to execute certain type of actions.

Table 3: DAC advantages and disadvantages

Advantages	Disadvantages
It can be decentralised (object can maintain information about who and how should be granted access) and as a result more scalable.	Decentralisation may cause difficulties for Administrator to control users, which are granted privileges to specific resources and under specific circumstances.
	Allowing the user to control the privileges to some resources may cause some security implications.

2.4.3 RBAC – Role-based Access Model

RBAC [6] uses so-called *roles* assigned to user in order to provide access control mechanism. *Roles* are closely related to function that given person may serve in a given organisation. Each role in RBAC model has assigned privileges, so that user will be assigned certain types of privileges. This is one of the main differences of RBAC when compared to DAC or MAC, where the privileges are directly assigned to users.

The same roles are also assigned to resources. If the role assigned to resource is not on user roles list, then the user will not be able to access it.

Table 4: RBAC advantages and disadvantages

Advantages	Disadvantages
As being commonly used with web-based frameworks, many libraries/modules implementing that model are freely available.	Very specific and detailed access control rules (so called fine grained access control rules) will produce big number of roles that will become difficult to manage.
It allows Administrator to reflect the roles and responsibilities of given person within an organisation	
It allows to achieve good balance between coarseness and finest of access control rules.	

2.4.4 PBAC – Policy-based Access Model

PBAC [6] combines the security attributes (e.g. roles) from the resource, the environment, and the user that sends the request.

The user is granted the access to a given resource if the request is compliant with a certain policy. Policy defines under what circumstances the access to a given asset (resource) can be granted or should be denied. For instance, a policy may specify that for a given resource only simple login and password are required, while for other certificates issued by a trusted authority are needed.

An example of security policy is shown in Fig. 3.

Fig. 3 Example of security policy provided by mean of XACML language.

Table 5: PBAC advantages and disadvantages

Advantages	Disadvantages
It allows to achieve very fine-grained rules.	It requires much knowledge (e.g. knowledge how to use XACML policy language) and skill to appropriately define security rules.
	Usually implemented as third-party servers or web-services for multi-platform authentication and authorisation purposes (e.g. for Enterprise Service Bus environment).

2.5 Recommendation for access control model

In order to achieve the best balance between the simplicity and the flexibility, *the RBAC model has been adopted*.

This type of access control method allows the ATE service administrator to have appropriate tools to define access controls rules for any user and resource, as well as to have simple, intuitive, and not overwhelming console for maintaining these rules.

Moreover, the RBAC model is commonly used in information management systems like blogs or wiki-like services, which are functionally similar to the ATE.

3 Service Requirements

The template of CIPRNet requirements is presented in Table 6 and consists of the following fields:

- **ID** is a unique identification number of the requirement, combined of the type and number of requirements (FR: Functional Requirement, NFR: Non-Functional Requirement).
- **Priority** (MoSCoW) – is determined by the importance of the requirement for end-users. Importance is determined by M(ust), S(hould), C(ould) and W(ould) markers.
- **Source** - indicates the origin of a given requirement (e.g. DoW, Consortium experience denoted with *internal*, end-user/stakeholder).
- **Version** - shows the evolution of the requirement.
- **Description** – provides explanation of the requirement.
- **Comment** – additional, relevant information can be placed here, e.g. reference requirements, comments, examples, etc.

Table 6: CIPRNet requirements template

ID		Priority (MoSCoW)	
Source		Version	
Description			
Comment			

In the following we present a classification in terms of functional and non-functional requirements.

3.1 Functional Requirements

ID	FR#1	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The Ask the Expert MUST be accessible via the VCCC portal		
Comment	The VCCC portal will contain a link to the Ask the Expert service web application		

ID	FR#2	Priority (MoSCoW)	M
Source	D5.2	Version	V1

Description	The Ask the Expert MUST allow to submit requests of information for the following minimal set of categories: (1) Technical CIP-related issues, (2) CI management, crisis management for CI, (3) CI-related documentation, e.g. national and EU regulations, policies, public reports and statistical data and (4) Practical aspects of CI functioning
Comment	The set of categories represents the minimal set

ID	FR#3		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	If the question is pertinent with the CIPRNet aims and scope, end-users will receive a short answer by the CIPRNet expert and/or links to publicly available sources (if this is justifiable in the context of a given question), For more complex questions, the requesting user will be put in contact with the most appropriate CIPRNet expert(s), selected from the pool of experts, based on the subject raised by the user			
Comment				

ID	FR#4		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	User requests will be gathered through pre formatted forms. The requesting form will have the following minimal set of fields: subject, description, domain type/name.			
Comment				

ID	FR#5		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE service MUST register all request and to allow for their maintenance.			
Comment				

ID	FR#6		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE service MUST register all request and to allow their maintenance			
Comment				

ID	FR#7	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The ATE service MUST filter the user requests		
Comment	e.g. to reject nonsense, out of the service scope, or too trivial requests, spam messages, etc		

ID	FR#8	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The ATE service MUST use the DB that will contain experts information		
Comment	Such database should contain at least the following information: experts status (available/non-available), contact info, domain of expertise, scope of the possible issues to be solved.		

ID	FR#9	Priority (MoSCoW)	S
Source	D5.2	Version	V1
Description	The ATE service MUST allow to queue user requests		
Comment			

ID	FR#10	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	Each user request can be in one of the following possible states: SOLVED, IN PROGRESS, UNSOLVABLE		
Comment			

ID	FR#11	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	User request can be sorted by category/topic		
Comment			

ID	FR#12		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE service will deliver the user request to the most appropriate CIPRNET expert(s)			
Comment				

ID	FR#13		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE service will allow CIPRNET expert to reply to user requests			
Comment				

ID	FR#14		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE service will have three different typology of users: ADMINISTRATOR, EXPERT, AUTHENTICATED			
Comment	ADMINISTRATOR will admin all DB tables EXPERT will participate in discussions with users and can change the status of a request (e.g. from OPEN to SOLVED) AUTHENTICATED users, after the registration procedure, can request information to the pool of experts. AUTHENTICATED users will participate in discussions with EXPERTs			

ID	FR#15		Priority (MoSCoW)	M
Source	D5.2		Version	V1
Description	The ATE DB will allow the storage of past requests			
Comment	ADMINISTRATOR users can control the utilisation of experts, control the distribution of topics, themes and question categories and the quality of service (e.g. issues unsolved vs. overall number of investigated issues).			

ID	FR#16		Priority (MoSCoW)	S
Source	D5.2		Version	V1
Description	The ATE DB will store FAQs			
Comment				

ID	FR#17	Priority (MoSCoW)	S
Source	D5.2	Version	V1
Description	The ATE service will allow the building of the FAQs section		
Comment			

ID	FR#18	Priority (MoSCoW)	M
Source	Internal	Version	V1
Description	The ATE should present Disclaimer notice which stresses what we could commit to do and what we could not.		
Comment			

ID	FR#19	Priority (MoSCoW)	S
Source	Internal	Version	V1
Description	The ATE should have FAQs to provide the solution to some questions, if any, that we could expect being more frequently raised.		
Comment			

ID	FR#20	Priority (MoSCoW)	S
Source	Internal	Version	V1
Description	The user should have ability to define the degree of urgency of her/his query		
Comment			

ID	FR#21	Priority (MoSCoW)	W
Source	Internal	Version	V1
Description	The user might have ability to make a conversation in a real-time.		
Comment			

3.2 Non Functional Requirements

ID	NFR#1	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The ATE Service will operate on a 24/7 basis		
Comment			

ID	NFR#2	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The ATE Service MUST allow to configure privacy and security setting for user requests		
Comment	Privacy and security functions and settings, e.g. to define the anonymity level of a request, whether the query/request will be publicised and available for a wider audience, etc.		

ID	NFR#3	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	Private discussions will be shown only to the participant in the discussion		
Comment			

ID	NFR#4	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	Public discussions will be shown only to all AUTHENTICATED users		
Comment			

ID	NFR#5	Priority (MoSCoW)	M
Source	D5.2	Version	V1
Description	The ATE server will create weekly backups of the service DB		
Comment			

ID	NFR#6	Priority (MoSCoW)	M
Source	Internal	Version	V1
Description	The content published on the ATE server must meet certain legal requirements.		
Comment	The minimum legal requirements include: (a) legal and copyright notices, (b) informed consent if cookies are used, (c) disclaimer for content to state the liability of the consortium and of the EC, and (d) data protection notice making explicit how any personal information collected from users will be used.		

4 Service Implementation

The ATE service is a PHP-MYSQL-APACHE web application that has been implemented using the YII PHP framework [ANNEX I] on a LAMP server running in the ENEA Casaccia Research Centre. The choice of technologies ensured the best compromise regarding the service management flexibility, service implementation costs and service compliance with other CIPRNet assets (i.e. the Inventory Database).

4.1 ATE Database

The ATE service relies on a MYSQL database that store all the information related to the service. In particular, the ATE database tables store information regarding:

- Users
- Requests
- Experts

Fig. 4 shows a simplified Entity-Relationship diagram of the ATE Database. The diagram also shows the link between the ATE database entities (the blue entities in the diagram) and the Inventory Database entities (the orange entities in the diagram)
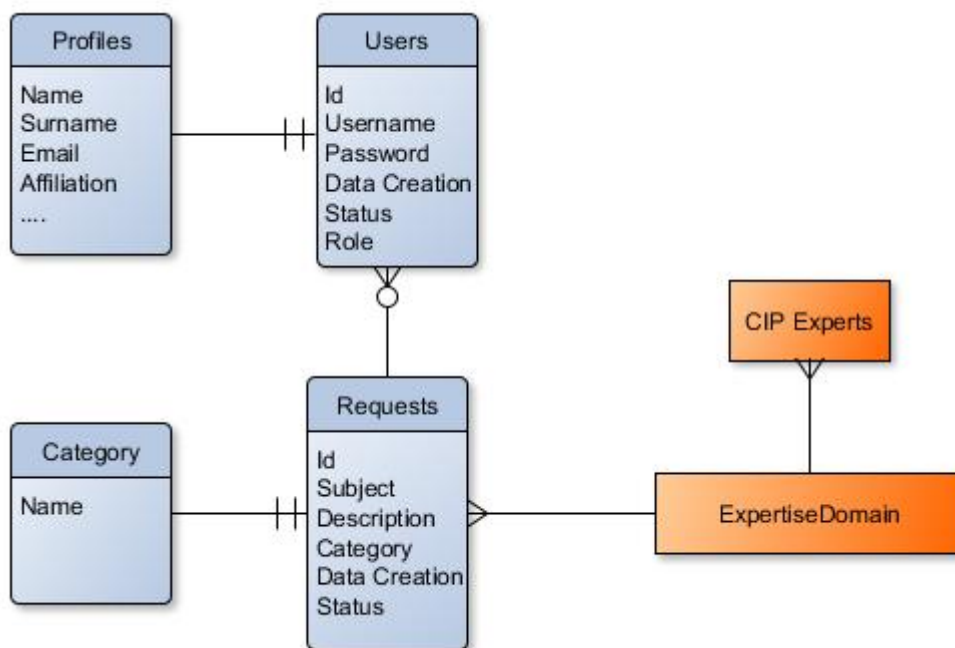
Fig. 4 The ATE database E-R schema

The ATE service will have many users. Each user has a Profile that contains the user info details. Each user has a Role. As described in section 2.2, the service has the following different user roles: Expert, Administrator/Moderator and End-User.

End-User after the registration to the service can submit requests to the service. Each request will belong to a category and the user will indicate the different expertise that the request would need on order to be answered. It is worthwhile to note that (1) the pool of experts of the ATE service will be the CIP Experts in the Inventory Database that will decide to be involved

in the ATE service and (2) the ATE service relies on information stored within the Inventory Database. Currently, the ATE service exploits CIP Inventory Database information regarding experts and the related expertise domains.

As a result the ATE service persistence layer comprises two databases (Fig. 5): the ATE database containing all information related to the ATE users and requests and the CIP Inventory Database containing information related to the experts involved in the service, their contact info, their affiliation and other kind of information as reported in D4.2 (see [5]).
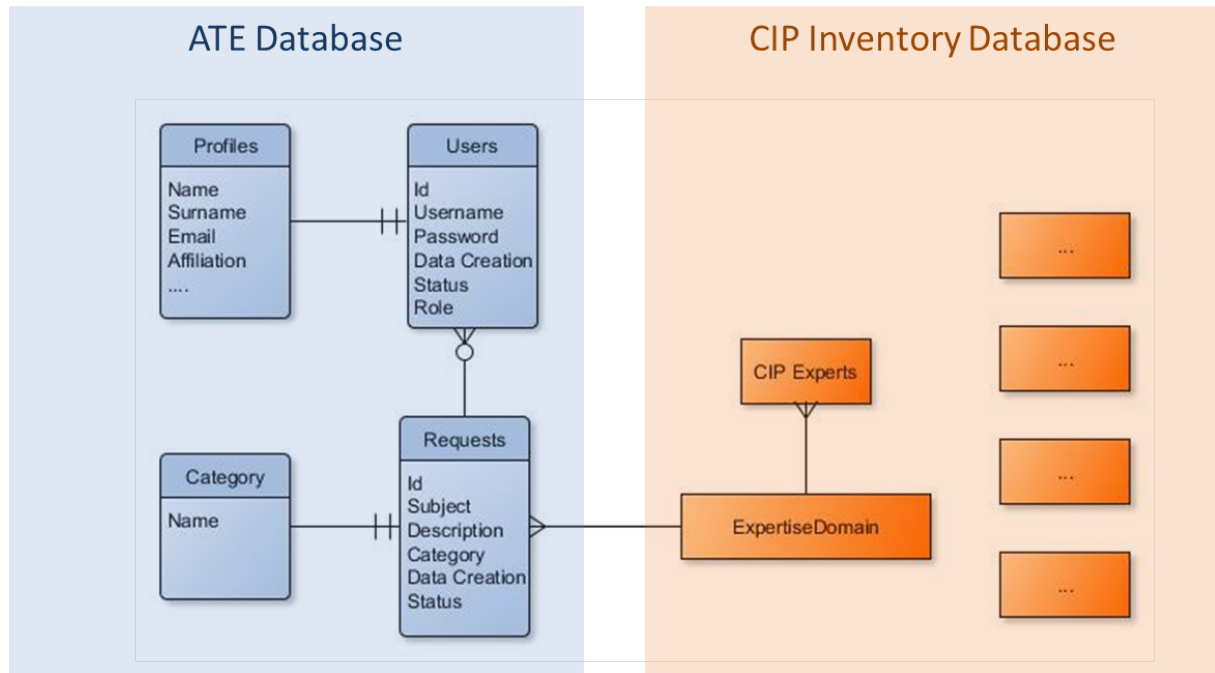
Fig. 5 The ATE service persistence layer.

4.2 User Login/Registration forms

In order to use the ATE service End-User, a generic user needs to complete the registration procedure. The registration procedure has the following steps:

1. Filling of the registration form (Fig. 6) and providing the requested information. The registration form will clearly display the necessary information (as, for instance, a valid email address) and it is fundamental for completing the registration procedure.
2. After the submission of the registration form, the user will receive an email containing a link to confirm the registration to the service.
3. The user has to click on the confirmation link. The web application will show a welcome message.
4. The user is thus activated and becomes an End-user. From this moment, the End-user using the chosen credentials can login to the service. Section 4.4 describes the steps needed to submit requests to the service and to monitor their state.

Fig. 6 The ATE service registration form

4.3 Service Administrator

The Administrator of the ATE service can manage all tables in the ATE Database. In particular, the Administrator, using the User Management module (Fig. 7) of the application will be able to:

- Manage Users – the Administrator can change all the information related to users. In particular, the Administrator can suspend and/or ban a user;
- Manage users profiles – using this action the Administrator can request more information to the End-User during the registration procedure and/or update some profile fields name/attributes;
- Create a user – for example, after receiving an explicit request from a CIP Expert in the CIP Inventory Database, the Administrator can use this action to add the expert to the ATE expert pool;
- List Users.

Another relevant module for the Administrator is the Role-Based Access Control module (Fig. 8). Using this module, the Administrator can:

- Assign a role to a user
- Assign permissions to the different roles
- Create new roles, tasks, operations
- Define Business rules

Fig. 7 Administrator User Management module

Using the Admin dashboard the Administrator will have the possibility to perform all the statistical queries as individuated in the service requirements as, for instance, which is the most active expert, which are unsolved user requests, which is the most popular user request category etc.

Once the ATE database will have a consistent numbers of requests, discussions (Experts and Authenticated users can leave comments on a request view page), authenticated users the ATE service will implement specific actions to be included in the Administrator Dashboard to display statistical info regarding the service utilisation. The Administrator can use this statistical information to build the so-called FAQs section. The Administrator Dashboard shows the allowed actions to the Administrator user. Currently, the Administrator can manage requests and experts.

Fig. 8 Permission management with the RBAC module.

Fig. 9 The Administrator Dashboard.

4.4 User request management workflow

Using a request submission form, the End-User can submit a request to be delivered to the experts of the ATE service. This section describes the request management workflow (Fig. 10) from the submission phase to the end of lifetime of a request (a request is no more active either if an Expert closes the request or declares the request to be unsolvable).
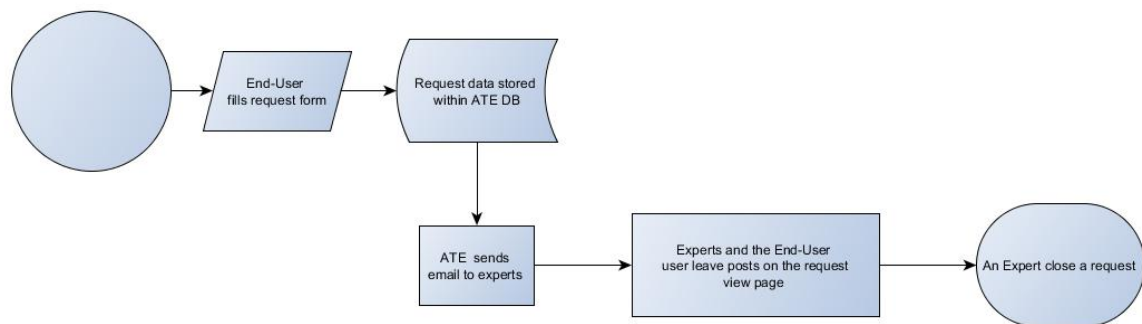
Fig. 10 The User request management workflow

Using the End-User Dashboard, a user can click on the Create Request action (Fig. 11 shows the End-User dashboard for the *demo* user). After clicking on the link, the user will be directed on the request submission page (Fig. 12).
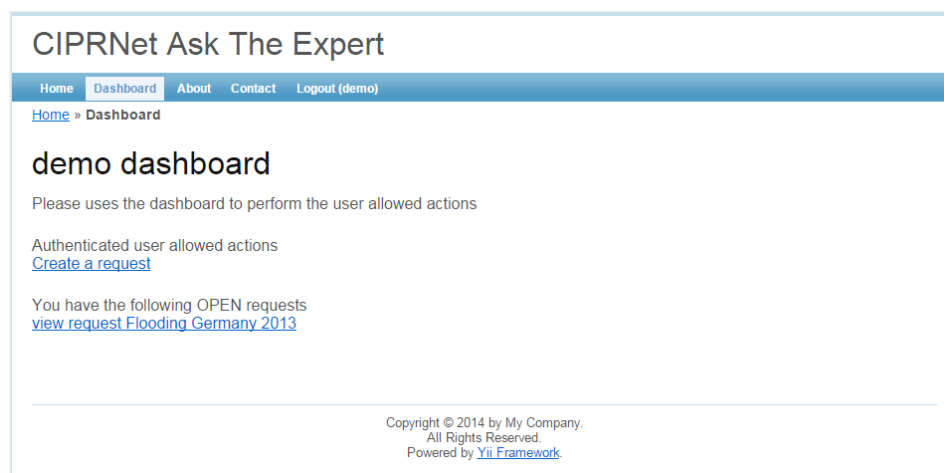
Fig. 11 The End-User Dashboard

Using the form, the End-User can insert the attributes related to a request:

- Subject – a very short description of the request
- Description – an exhaustive description of the request containing all the needed details
- Type – according to the service requirement document a request must belong to a category. Currently the End-User can choose among these different options: (1) Technical CIP, (2) CI Management, (3) Crisis Management (4) Document request and (5) CI functioning
- Request Expertise – the End-User can choose multiple expertises from the list. Only ATE experts that have the chosen expertise will be contacted in order to handle the request.

Fig. 12 Request Submission Form

The request submission form contains the Create button that allows the End-User to submit the request. As shown in Fig. 13 after the End-User submits a request, the ATE application stores all the request information on the ATE DB and queries the CIP Inventory Database to individuate all the ATE experts that have at least one of the requested expertise to handle the request. Then, the ATE application sends an email to the selected experts to inform them that there is a new request waiting an answer.

Both the End-User and involved ATE Experts can start to view the request and to leave comments on the view request page (the so called request discussion page). The ATE Expert Dashboard will show all the requests that can be handled by the Expert (Fig. 14 shows an example of a ATE Expert dashboard). The comments on the discussion page together with other form of communication (email messages, private conversations) will allow Experts to handle the request. Only the ATE Expert has the privilege to close a request. The ATE Experts can exploit the CIP Inventory Database to find information to handle the End-User requests.

Fig. 13 A request discussion page

Fig. 14 An example of the ATE Expert Dashboard

5 ATE Service deployment diagram

The ATE Service will be accessed through the VCCC Web Portal, one the main CIPRNet product that will allow the deployment of different services for CIP researchers, end-users and other CIPRNet stakeholders, as for example the CIP Inventory DB Service, the CIPedia Service (see [2]) and the ATE Service. The deployment diagram of Fig. 15 shows the deployment of the ATE service, the main technologies that has been used for its implementation and how the ATE DB is connected with the CIP Inventory DB.
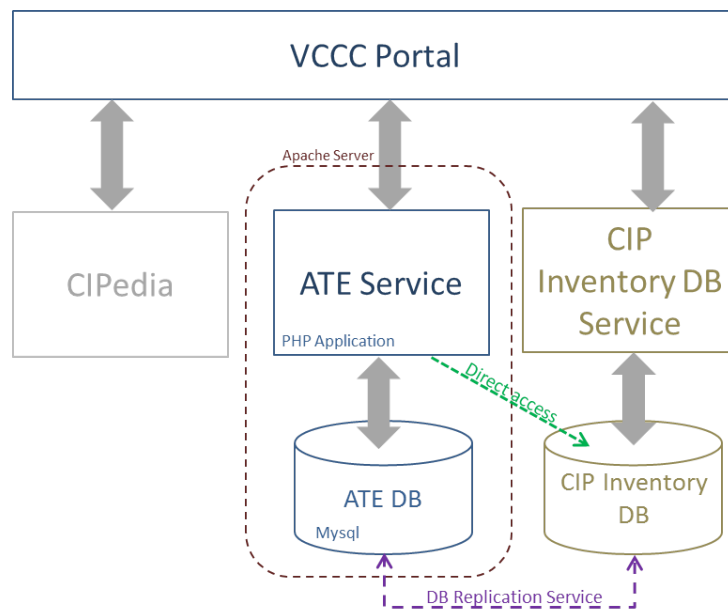

Fig. 15 ATE Service deployment diagram

The ATE PHP web application will run on an Apache ENEA server and it relies on the MySQL Database ATE DB. As described in the previous sections the ATE Service will exploit information stored within the CIP Inventory DB. Currently, the ATE Service uses a local copy of the CIP Inventory DB. For the final deployment of the service two options are possible: (1) to work with a local copy of the CIP Inventory DB and to implement a DB Replication service (purple arrow in Fig. 15), (2) to access directly the CIP Inventory DB server (green arrow in Fig. 15).

6 Roadmap for future features

Table 7: List of features planned for upcoming version of ATE service

ID	Priority	Description
f-01	Medium	Administrator should have technical possibility to exclude certain type of experts to answer request coming from competing institutions.
f-02	Medium	Real-time chat between expert and end-user.
f-03	Low	Analytical tool that will help the administrator/experts to maintain the FAQ

7 Conclusion

This document describes the realisation of the Ask The Expert Service that is available through the CIPRNet VCCC Web Portal. The service requirements have been formalised starting from the general service requirements individuated in [3]. The service exploits also the CIP Inventory Database to manage information regarding CIP Experts and CIP expertise. The service has been implemented using free technologies and will rely on resource already available to the consortium. Currently the service is running on an ENEA private server. The next steps toward the service deployment in the VCCC Web portal are: (1) deploy the service on a ENEA public server, (2) select experts among the CIPRNet partners willing to test the service to find bugs and check service usability (the testing period should last no more than 1 month), (3) to fix bugs and implement service improvements.

Finally, the PHP framework used for the ATE service implementation allows to easily add functionalities to the service. In particular, there are two ways to extend service functionalities: (1) to implement a module to be added to the service and (2) to import an already available extensions form the PHP framework extension repository. For example, the ATE Service can be improved by adding the possibilities to End-Users and Experts to use an Instant Messaging module to realise the real-time chat as proposed in Section 6.

8 References

[1]   FP7 CIPRNet Project, Deliverable 4.1 "Inventory of expertise".

[2]   FP7 CIPRNet Project, Deliverable 8.4 "Publicly announced CIPedia".

[3]   FP7 CIPRNet Project, Deliverable 5.2 "Service specification".

[4]   FP7 CIPRNet Project, "Description of Work"

[5]   FP7 CIPRNet Project, Deliverable 4.2 "Fully operational inventory database of CIP expertise and technology".

[6]   NIST, A Survey of Access Control Model, Privilege Management Workshop, 2009.

9 ANNEX I - Yii framework

Yii is an open source and object oriented PHP framework that allows the developers to build Web 2.0 applications. Yii shipped with such built-in features including:

- MVC (Model-View-Controller),
- DAO (Data Access Object),
- I18N/L10N (internationalization and localisation),
- Authentication and role-based access control.

Security provides a wide range of input validation mechanism and output filtering to provide protection against such cyber attacks as XSS (Cross-site scripting) and SQLI (SQL Injection).

Yii allows the developer to build any type of web application and can be used to create such solutions like CMS (Content Management Systems), online forums, e-commerce systems, etc.

It provides caching mechanism that allows the developer to handle large volume of traffic generated by users.

Yii is released under the BSD License. That kind of license does not impact the ATE service, because it allows the ATE to be either open-source or proprietary Web application.