



A CIP-PSP funded pilot action
Grant agreement n°325188



Deliverable		D6.2.1 – ACDC Social Platform deployed, Online platform	
Work package	WP6		
Due date	30/06/2013		
Submission date	31/01/2014 – Updated submission – 31/08/2014		
Revision	3.01		
Status of revision	Final		
Responsible partner	Engineering Ingegneria Informatica		
Contributors	Paolo Rocetti (EII), Barbara Pirillo (EII), Véronique Pevtschin (EII)		
Project Number	CIP-ICT PSP-2012-6 / 325188		
Project Acronym	ACDC		
Project Title	Advanced Cyber Defence Centre		
Start Date of Project	01/02/2013		
Dissemination Level			
PU: Public			✓
PP: Restricted to other programme participants (including the Commission)			
RE: Restricted to a group specified by the consortium (including the Commission)			
CO: Confidential, only for members of the consortium (including the Commission)			

Version history

Rev.	Date	Author	Notes
0.1	16/01/2014	EII	Creation of first draft
0.2	20/01/2014	EII	Update
2.01	23/01/2014	EII	Contribution
2.01	27/01/2014	EII	Final revision for circulation
2.02 – 2.04	28/01/2014	EII	Internal updates
2.05	29/01/2014	EII – Alberto Montichiara	Addition of data sharing annex
2.06	30/01/2014	EII – Paolo Rocchetti	Revision of annex
2.07	31/01/2014	EII – Véronique Pevtschin	Submission
3.00	17/08/2014	EII	Expanded section 5 in section 5,6,7,8 (submission for interim review), with enhanced / new information with respect to version 2.07.
3.01	26/08/2014	EII	Updated following internal quality review

Note: the changes provided in version 3.00 to existing sections (and 3.01) are highlighted in yellow to increase legibility by the reviewers. New sections have only the title highlighted in yellow.

Table of contents

1. Executive summary	5
2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)	6
3. Introduction	7
4. Strategy for the ACDC community portal	8
5. The ACDC Community	10
5.1. Participants: Stakeholders & Representatives	10
5.2. Accessing Contents: Roles & Permissions	10
5.3. Adding new Contents: The Publication Workflow	11
6. Underlying Portal Technology: OPENNESS	12
6.1. Portal Areas: Network & Workspaces	12
6.2. Portal Framework.....	12
6.2.1. People.....	13
6.2.2. Resources	13
6.2.3. Activities	14
7. The ACDC Portal Structure.....	15
7.1. The ACDC Public Network	15
7.2. The ACDC Private Network.....	16
7.3. The Experiments Workspaces	19
7.4. The Data Sharing Workspace	20
8. The ACDC Portal Applications	21
8.1. Joining	21
8.2. Initiatives & Stakeholders	22
8.3. Tool & Services	24
8.4. Data Access Manager (DAM).....	26
9. Conclusion.....	32
10. References	33

Table of figures

Figure 1 – OPENNESS Framework	13
Figure 2 – ACDC Public Network	15
Figure 3 – News	16
Figure 4 – Activities	17
Figure 5 – Initiatives&Stakeholders	17
Figure 6 – Tool&Services	18
Figure 7 – Forum	19
Figure 8 – The ACDC Experiment Workspace.....	20
Figure 9 – Joining Form	21
Figure 10 – Stakeholder Detail	22
Figure 11 – Stakeholders List	23
Figure 12 – Stakeholder Detail	24
Figure 13 - Initiatives Graph	24
Figure 14 – Tool&Service Detail	25
Figure 15 – DAM Architecture.....	26
Figure 16 – DAM Role Model	27
Figure 17 – DAM Key Management	29
Figure 18 – DAM Group Management	30
Figure 19 – DAM Sharing Policies Management	31



Table of tables

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation	6
Table 2 – linking the ACDC portal features to fighting botnets.....	9

1. Executive summary

The creation of a participative stakeholders' community is a major objective in the ACDC project and is in line with the overall project's approach based on fostering a wider level of information sharing and, therefore, a faster and more effective communication between stakeholders active in the cyber security area with the final aim to fighting botnets across Europe.

Deliverable D6.2.1 is dedicated to the instrument adopted in the ACDC project to support the creation and animation of the stakeholders community. Starting from a pre-existing social platform, OPENNESS, developed by partner Engineering Ingegneria Informatica, a dedicated social community platform has been adapted to the ACDC needs.

With respect to the original role of the community platform as described in the Description of Work (DoW), the platform's scope has evolved considerably from its initial positioning as an online facilitator for sharing knowledge open to any interested and anonymous stakeholder to

- acting as the single entry point to the ACDC data clearing house. In this evolution, the front-end caters to the needs of providers and users of data – thereby implementing a controlled access to the data itself and requiring stakeholders to be identified
- supporting specific activities such as participating to experiments, providing information about initiatives, providing and acquiring information about tools & services to fight botnets

These features have been modelled in D6.3.1 (user involvement model in ACDC) and listed in D6.3.2 (report on user activities).

The addition of these features has modified the development of the ACDC platform in terms of security level and integration with the ACDC Data Clearing House module, and therefore also the deployment schedule of the ACDC platform, with the deployment rescheduled to March 2014 for the first version, the official launch on 24th September 2014 and the addition of the social analytics (meaningful only after a few months of usage of the platform by the internal and external stakeholders of ACDC by the 31st January 2015, ensuring a period of 4 months on which to base the analysis).

2. Overview of the link between WP5 and WP6 deliverables (M12 deadline)

As WP6 has a last number of deliverables within the first 12 months, this section provides an overview of which deliverable provides what information. In addition, due to the close link to the dissemination activities of WP5 two deliverables from WP5 are also included in the description below.

This section is repeated in all WP6 deliverables.

Deliverables	What is in the deliverable?
D6.1.1 – user profiles and categorization	The different attributes used to categorize stakeholders, easing the prioritisation of the outreach activity of WP6 and the analysis of the different groups contributing to creating the ACDC community
D6.1.2 – identified users list	The analysis of the stakeholders identified through different activities. This analysis is based on contacts established with 90% of the 426 identified stakeholders.
D6.2.1 – ACDC social platform	The description of the ACDC platform and the extension of its functionalities with respect to the original role foreseen in the DoW
D6.2.2 – Adding social analytics to ACDC social platform	The addition of tools in the ACDC platform to monitor the activities and create a statistical overview of user activities
D6.3.1 – Involvement model for users in ACDC	A detailed description of the different activities that users can choose to be involved in ACDC, presented a UML graphs.
D6.3.2 – Report on user activities	A list of the activities carried out by ACDC partners over the first 12 months of existence to lead to user involvement. First results are the letters of intent signed by 5% of the stakeholders identified in D6.1.2. Next steps identify the different activities proposed to users to become involve in ACDC; these activities are supported by the detailed approach in D6.3.1.
D5.1.1 – dissemination plan	The full list of activities defined to create awareness about ACDC and support the outreach activities of WP6
D5.1.2 – intermediate dissemination report	The report of the dissemination activities of the first 12 months; this report is complemented by D6.3.2 for the section on individual meetings with organisations to reach the first level of involvement, i.e. letters of interest.

Table 1 – overview of the WP5 – WP6 deliverables over the first 12 months of operation

3. Introduction

The ACDC project is a 30 months pilot project whose technical goal is to create a set of solutions and a centralised data clearing house provided to network operators and end-users to support the detection, mitigation and prevention of botnets.

However, this technical goal will only be successful if ACDC also acts pro-actively to ensure adoption of the ACDC approach by contributing to and / or using the different components of ACDC, including:

- the centralised data clearing house, providing Europe with the access to data focused on botnets in Europe
- the 8 national support centres relaying the ACDC information and solutions across Member States
- the use of an online platform oriented towards supporting stakeholders in interacting with ACDC

All these steps are therefore oriented towards creating, supporting and animating an active community, and ACDC devotes a specific work package, WP6, to this activity.

Deliverable D6.2.1 focuses on the definition of the features of a social community platform (also named “community portal” in the following) dedicated to support the communication and the data sharing within stakeholders active in the ACDC community.

Contrary to the Dow, the community platform is deployed as the **single front-end** to access the ACDC Data Clearing House, as well as a support to the ACDC members as a knowledge management tool and as an activity support tool.

The community portal together with the ACDC data clearing house propose an advanced policy access control enabling providers of data and solutions to tailor the type of access allowed for their contribution – and for users wishing to access the data to have a clear visibility of what are their rights and obligations with respect to the data.

The ACDC Community Portal is designed to

- Provide a single front-end to access the ACDC Central data Clearing House (CCH)
- Foster the visibility (and uptake) of activities for the ACDC community
- Support interaction with stakeholders
- Enable fast and effective information sharing among members by providing different functionalities and different interaction areas.

Structure of the Document

The core part of this document is structured as follows: section 4 presents the strategy that has been adopted to create and put in places the community platform. Section 5, in turn, introduces the main concepts that have been adopted in the portal to model the ACDC community (participant organisations and representatives, roles and content publication processes). The portal itself has been built upon the OPENNESS technology platform (created by ENGINEERING to support user communities); OPENNESS is briefly introduced in section 6. Section 7 describes how the OPENNESS concepts have been used to structure the ACDC platform, while section 8 provides some details about the applications that have been either adapted, or created, to manage contents in the ACDC platform.

4. Strategy for the ACDC community portal

The role of the ACDC community portal is to ease access to the different activities that can be shared by ACDC community members, with a view to improving the detection, mitigation and prevention of botnets across Europe;

Therefore, to define the structure of the community portal, the list of activities that can contribute to these three activities has been analysed and from this analysis, the different features of the community portal have been defined.

Improving the detection

Improving the detection of botnets can be achieved by increasing the speed at which a botnet is detected; this in turn can be achieved by increasing the amount of data sets provided by Internet Service Providers (ISPs) to the ACDC centralised data clearing house which are then analysed with state-of-the art tools and techniques. Supporting this through the ACDC community portal requires features to organise the provision of data to the centralised data clearing house, as well as retrieval of the data. These processes require the building of trust among the providers, which is linked to the advanced support for data sharing policies.

Improving the prevention

The detection of botnets introduced in the previous paragraph will only contribute to improve the prevention if information is sent as fast as possible on the one hand to the ISPs and on the other hand to users of fixed and mobile devices to avoid the creation / spreading of the botnet. Supporting this through the ACDC community portal requires on the one hand to foster stakeholders joining the community and on the other hand creating channels to share knowledge.

Improving the mitigation

Improving the mitigation is another aspect to which ACDC aims to contribute, through new tools and services developed during the piloting phase implemented by WP2 and WP3. To move from technology to uptake, the organisation of the solutions has to be done and made accessible to a wide community of stakeholders. This in turn is implemented by specific features in the ACDC community portal.

The table below aligns the different needs to the ACDC community portal features; the following section explains the portal features, based on the modelling provided in deliverable D6.3.1 [3].

Fighting botnet needs	ACDC community portal feature
Improving the prevention	<p><i>Initiatives:</i> improving awareness by collecting information about all existing botnet related initiatives</p> <p><i>Announcements:</i> used to announce new events, availability of new solutions etc.</p> <p><i>Forum:</i> the place to easily share and discuss information about botnets.</p>
Improving the detection	Data sharing: provision and retrieval of data sets

	<p>provided mainly by ISPs are done through the Central Clearing House. The Community portal allows organizations to access CCH functionalities, and control the sharing of the data provided to the CCH.</p> <p><i>Announcements:</i> providing a fast link to announcements about botnets, the place to indicate a new botnet detected, increasing the speed of information of users. Social media (such as twitter) as described in D5.1.2 is also intended to be used to duplicate the announcements feature when the content is related to new botnet detected.</p> <p><i>Experiments:</i> the place where community members can ask to join an experiment (usually ISPs, IT providers, researchers) – can find results of an experiments (all community members) – thereby discovering <i>how</i> new solutions can help based on a concrete pilot. This is a key difference with the “tools / services” section.</p>
Improve the mitigation	<p><i>Tools and services:</i> used to list available tools and services that can be implemented by users to protect against botnets. This section complements the “<i>experiments</i>” section, where the focus is on testing and validating (together) how tools and services are used in the context of the ACDC experiments.</p>

Table 2 – linking the ACDC portal features to fighting botnets

In addition to the features highlighted below, the ACDC project has taken, from the start, the regulatory aspect into account.

In the context of botnets, two non technical aspects have been introduced:

- the complexity of fighting botnets from a law enforcement point of view
- the importance of implementing the regulations linked to data protection in the context of sharing data sets in the ACDC data clearing house

The Community portal has also be conceived as the place where users are encouraged to find and share experiences and best practices in how to comply to legal aspects when sharing data. To this aim a forum has been introduced where community members with a legal background can get feedback about complexities encountered when using regulations, and which may then require an evolution based on user feedback.

5. The ACDC Community

The description of the ACDC community portal implementation (see section 7) relies on two other information: the Underlying portal technology (introduced in section 6) and the most relevant ACDC community aspects, that are detailed in following subsections.

5.1. Participants: Stakeholders & Representatives

The ACDC community is organized around the concept of participating organization and its representatives. The choice to have organizations, as part of the community, instead of spare people is due to the needs of (i) having a better view by community members of participant organizations and (ii) to easily keep the link to the organization even in case the people involved in the ACDC community from that organization will change. **Organizations dealing in any way with the botnet domain are named Stakeholders in the ACDC platform.** Information about stakeholders and their level of membership is available through the Initiatives&Stakeholders application (see below section 8.2).

People involved in the community from a participating organization are called **Stakeholders Representatives** ("representatives" in the following). Among them, the **Stakeholder Responsible** ("responsible" in the following) is the one in charge of coordinating the participation of representatives to the community activities. The responsible role is modelled through a dedicated platform role assigned to one of the representatives in the context of the participating organization. Beside representatives, a **Main Contact** is also kept in the platform for each organization. The main contact is a high level figure in the organization usually not actively contributing to activities, but only kept as a point of contact for important communications to the company. For this reason the main contact does not have a dedicated role in the platform, but it is only kept in the stakeholders' profile information. Information about stakeholder representatives and main contact is also available through the Initiatives&Stakeholders application (see below section 8.2). At joining time, the applicant organization is asked to provide information about the main contact and the Stakeholders responsible and representatives to be added to the ACDC community (see below section 8.1).

5.2. Accessing Contents: Roles & Permissions

Most of the content available in the community platform is accessible by representatives upon completion of the registration procedure. A few specific contents are subject to specific authorization. In particular, administrative operations, as well as publication of specific contents (e.g. announcements) is restricted to some platform users. The same applies to content shared in dedicated workspaces (see sections 7.3 and 7.4), that is accessible to workspace participants only. This approach, coupled with the publication workflow described in section 5.3, aims at fostering collaboration among community members, that may suffer from excessive restrictions in the access to platform contents, while maintain some moderation over the information that is being shared.

The ACDC platform adopts the concept of role [4] to assign permissions to community members. The use of roles allows for an easier management of accesses, especially in large environments with high number of users. Both the *Stakeholder Representative* and the *Stakeholder Responsible* concepts introduced in the previous section are modelled as roles in the

community platform, being the *Stakeholder Responsible* role a super-role (i.e. with more privileges) of the *Stakeholder Responsible* one.

Beside organizational roles, other ones have been introduced in the platform, to allow for specific, and coherent, set of actions. Main roles are “Editors”, that allows for publishing and editing most of the community-level content (e.g. announcements, experiment descriptions, stakeholders information, etc.), as well as “Managers”, that are in charge of review specific kind of information before publication (see section 8.1, 8.2 and 8.3).

5.3. Adding new Contents: The Publication Workflow

As introduced in section 5.2, the sharing of contents in the ACDC Community platform is oriented to a free approach, to encourage contributions from participants. Nevertheless, some moderation is needed, especially for structured information, where fake or misleading contributions can lower the overall quality of the information hosted in the community platform. For these cases a **“Suggest/Review” publication workflow has been put in place**. Therefore, some portal applications (e.g. Initiative&Stakeholders, Tool&Services, see section 8) allows representatives to suggest new contributions to be included in the shared information base. Once a suggestion for new content is received, the relevant role, depending on the kind of suggested information (e.g. Initiative Manager, Tool Manager, see section above), is notified by email. The appointed role is then in charge to review the suggested inclusion for correctness and appropriateness and approve/deny the publication request.

The publication workflow only applies to structured information, while free text contributions (e.g. in the forum and in the wikis) are not moderated. For these contributions the community itself can correct irrelevant or inappropriate content.

6. Underlying Portal Technology: OPENNESS

The ACDC community portal is built upon the functionalities provided by OPENNESS (Open Networked Enterprise Social Software) technology [5]. The main concepts at the core of OPENNESS are connected to the *Four Principles for the Open World*: Collaboration, Transparency, Sharing and Empowerment, as well described by Don Tapscott [1] in his speech at TED, in June 2012 [2].

OPENNESS is a social platform put forward by Engineering Ingegneria Informatica to foster collaboration, social interaction and co-creation processes that supports people in reaching challenging objectives. It eases the sharing of contents and information, thus stimulating a natural creation of knowledge by community participants. It increases the transparency of interactions, highlighting the real value of contributions to the community tasks. Ultimately, it creates the conditions to empower people and enable them to reach the common goal.

The following subsections introduces the main features of OPENNESS that have been used to implement the ACDC Community platform.

***NOTE:** screenshots below refers to the version of OPENNESS applications currently published in the ACDC community portal, and may be subject to changes and improvements following OPENNESS evolution at later stages of the ACDC project.*

6.1. Portal Areas: Network & Workspaces

The structure of OPENNESS as a portal is organized around two kinds of user groups: Network and Workspaces. **Network are structured set of users that may have dedicated spaces (public and private) in the OPENNESS platform.** When a new user is registered in the platform it is added to at least one network, but it may be added to more than one, upon request of the user, or upon invite by the network administrator. Each network is composed by users from one or more organizations that (usually) have long term relationships (e.g. employees within the same company). In ACDC the concept of Network has been used to model the whole ACDC Community, as detailed in sections 7.1 and 7.2.

Within each network (or across different ones) teams can be created. Teams represents group of individuals working together to carry out specific activities. **Each team has a dedicated workspace that grant access to a number of applications useful to reach team objectives.** In ACDC, the concept of team (and associated workspace) has been used to model experiments and data sharing areas of the portal, as detailed in sections 7.3 and 7.4.

6.2. Portal Framework

Beside structuring the community participants in Networks and Teams (Workspaces), OPENNESS provides a set of features, implemented by a number of applications, that can be configured to provide easy access to Network- and Workspace-specific functionalities. The main applications currently adopted for the ACDC community platform are briefly introduced by subsections below.

The People, Activities and Resources elements available to each user are always accessible in the OPENNESS platform through a visual framework. The framework surrounds the central part of the

page, where the current content is displayed to the user. The platform also allows customizing of the interaction between the main content, shown in the central part of the page, and the elements of the OPENNESS framework, thus increasing the ease of use for the community members.



Figure 1 – OPENNESS Framework

6.2.1. People

People are the active users of the platform. They have a profile, and they will get access to a specific set of applications, depending on the assigned roles as well as on the workspaces the users are member of. The platform is able to model relationships among users, and supports different kind of grouping, either structured or flat, user-defined, static, dynamic, etc.

The People application provides users with a view on the other participants to the network and workspaces they are member of. Through this application the user is also able to define the set of people she wants to “follow” in the platform. Following a community member means to be notified about changes applied by that user to the shared content. Following activities of a network (or workspace) means the user is notified about latest changes in the network (or workspace) content. (see the Activities section below)

6.2.2. Resources

Resources represent an information chunk that can be uniquely referenced across the platform. The Resource content is not necessarily stored inside the platform. It could be an external content that only has a description in the platform itself. Resources can be connected to each other either by structural associations (e.g. an email and its attachment), or by semantic information that is associated to the resource by the system, or by contributing people (e.g. a document and a video having the same set of tags). Moreover the platform allows users to define resource groups either by enumeration or through grouping criteria. The platform allows the definition of specific actions



on a given kind of resources that eases the sharing of resources among users, the creation of new resources connected to an existing one, etc.

The *Resource* application provides the user with a view on (and an easy reference to) the content of interest for her. The Resources application shows a selection of contents (made by the user), and allows the user to define which ones she is interested in following the changes (see the Activities section below). Moreover, the Resources application allows the user to access the selected content in just one click.

6.2.3. *Activities*

Activities represent all the actions that are executed by people on and in the platform. Samples of Activities are the creation of new groups, changes to the available resources in the platform, etc. Activities can be grouped in Activity Streams, that allow users to visualize the flow of changes related to a specific resource or content. According to the level of access rights associated to them, users may follow streams of friends, groups, etc. among those defined within the platform.

The *Activities* application provides the user with a view on recent activities on the relevant content. The application allows the user to see recent activities as a list of recent changes applied to the content. The changes displayed are related to the content, people, Network and workspaces the user is “following” (see People and Resources sections above). For an image of the Activities application see section 7.2 below.

7. The ACDC Portal Structure

Based on the main aspects of the ACDC Community, introduced in section 5, and on the OPENNESS technology, whose main elements have been summarized in section 6, this section focuses on the description of the ACDC portal structure and functionalities. The current version of the ACDC portal has been organized in different areas (network and workspaces), each one hosting a given kind of information, and providing access to a different set of application. Portal areas, the contents they hosts and the applications they provides are briefly introduced below.

7.1. The ACDC Public Network

Not all the information hosted by the ACDC community portal is restricted to ACDC representatives. Some of the information is, in fact, public. This is mainly due to **the need of attract new ACDC community participants, and inform them about why and how participation to the ACDC community can help them in fighting botnets**. This let them better evaluate their participation to the ACDC community. Furthermore, the public part also hosts the application form new organisations uses to express their interest in joining the ACDC community (see section 8.1 for more details about the joining application and the joining process).

The public part of the ACDC community portal has been modelled as a public section in the community network. This means that the structure is similar to the other portal areas, described below, except it doesn't shows OPENNESS functionalities (people, resources, activities) introduced in sections 6.2 above.

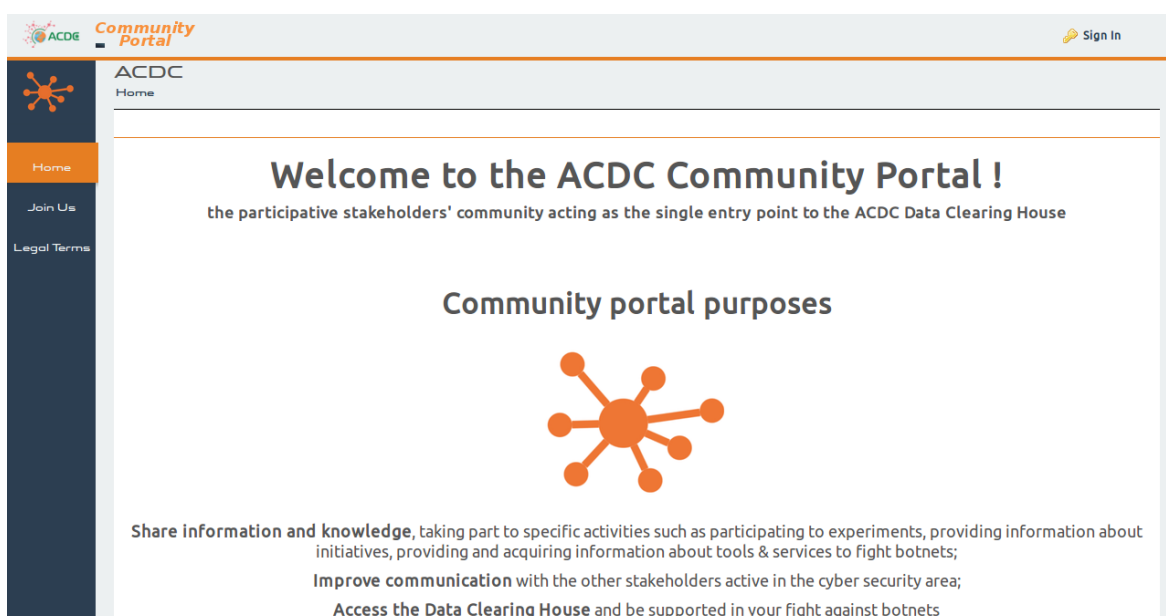


Figure 2 – ACDC Public Network

Moreover, the public part of the ACDC portal hosts the legal terms for community portal usage, that new representatives have to accept in order to complete the registration process.

7.2. The ACDC Private Network

The ACDC private network is the common area where all users are directed upon successful login into the community portal. **The aim of the ACDC Private Network is to host information targeting the whole ACDC community**, and provide applications to access the community-level information.

Differently from the public area introduced above, the private area also shows the OPENNESS applications related to people, resources and activities. Moreover, the left side menu changes to display applications of the ACDC private network. Applications currently part of the ACDC Private Network are: **News, Activities, Initiatives&Stakeholders, Tool&Services**, and the **Forum** (NOTE: this list may evolve in time together with ACDC community needs).

The News application provides users with latest announcements about community activities in particular, or the botnet topic in general. Samples of announcements are: the launching of a new experiment, as well as about experiment results; new stakeholders joining the ACDC community; the publication of papers; announcements about botnets takedown; recent findings about botnets; relevant conferences; etc.

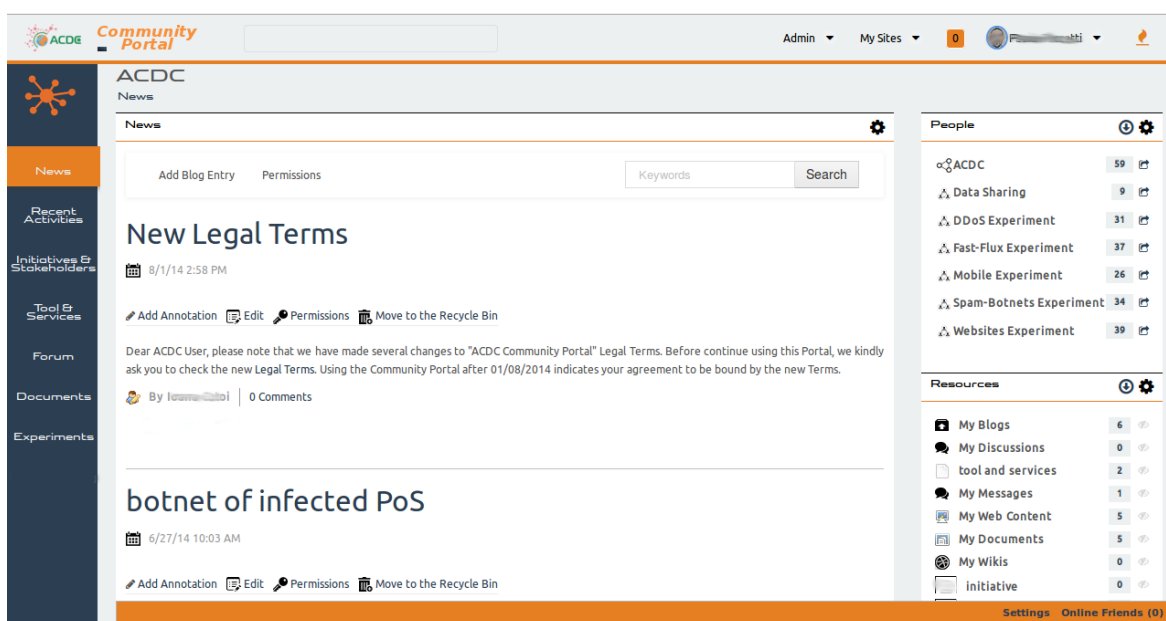


Figure 3 – News

The publication of new announcements (and the editing of existing ones) is restricted to Editors in the platform (see Roles & Permissions, section 5.2). References can be also added to each announcement to link it to relevant content in the community platform. For instance, a news about results from an ACDC Experiment can refer to the page (or document) detailing the experiment findings.

Activities have been already introduced in section 6.2.3 as part of the OPENNESS framework. **In the context of ACDC the Activities page is used for a number of purposes, ranging from stay informed about content changes** (e.g. Tools & Services, organization of experiments, uploaded documents), **to follow users and group activities**. It differs from the News section in the level of detail and in the target of the information provided. While News are high level information targeting the whole community, recent activities refers to low-level changes in the portal content and target specific users.

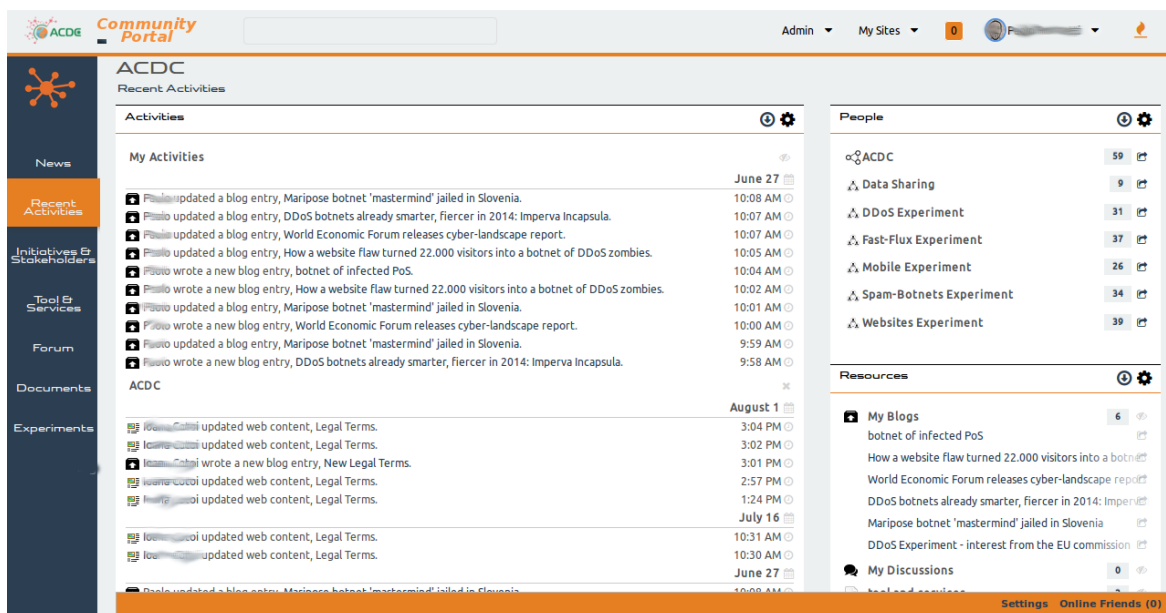


Figure 4 – Activities

The **Initiatives&Stakeholders** application provides community participants with a view about past, current and future initiatives to fight botnets, and the involved stakeholders. Stakeholders may, or may not, be part of the ACDC community, in the former case the name of participants from the stakeholder are also shown. Information about initiatives and stakeholders can also be displayed as a visual graph. The inclusion of new initiatives and stakeholders adopts the Publication Workflow described in section 5.3: all community members are allowed to suggest new initiatives to be added, while participants with the “Initiative Manager” role are in charge of review suggestions and approve/deny the publication. For more details about the Initiatives&Stakeholders application see section 8.2.

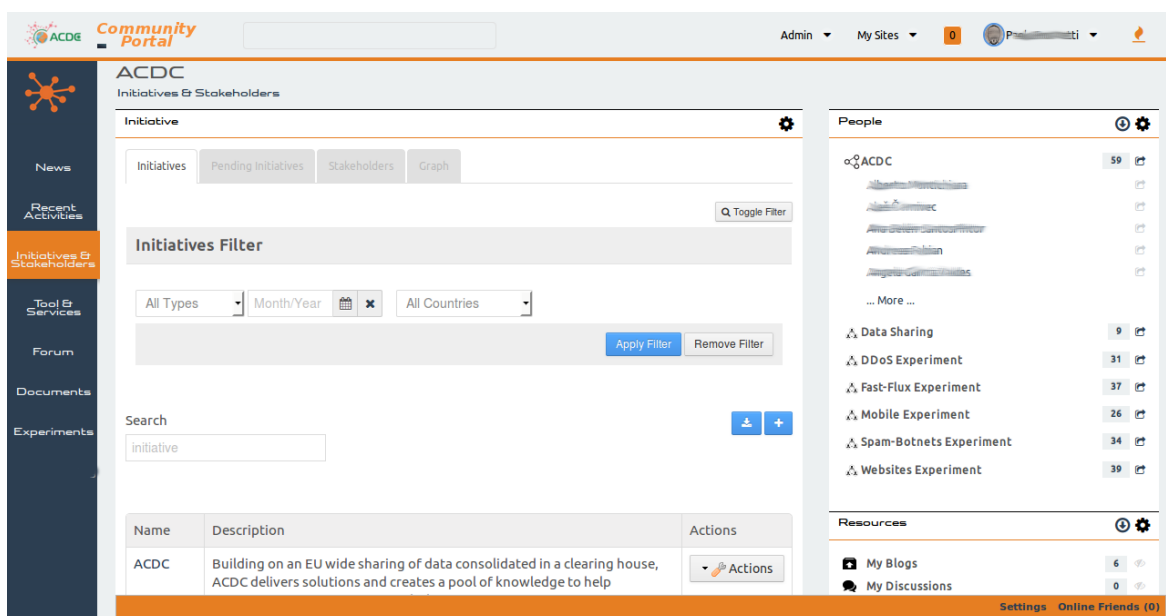


Figure 5 – Initiatives&Stakeholders

The aim of the **Tool&Services** application is to collect information about the tools and services already available to fight botnets, information provided by the application concerns tool and

services within the ACDC scope or beyond. This will serve as a starting point for community participants to discover what can be of help in fighting botnets. Some general information is maintained for each of the tool or services included in the application: the tool or service name; the reference to the website distributing the tool, or providing the service website; a brief textual description about the tool or service functionalities and a categorization based on that introduced in deliverable *D2.3 - Technology Development Framework* [6]. Furthermore, the Tool&Service application is connected to the forum one. For each tool, or service, a dedicated section in the forum allows community participants to comment and exchange detailed information about the tool, or service. The inclusion of new tool and services adopts the Publication Workflow described in section 5.3: all community members are allowed to suggest new tool or services to be added, while participants with the “Tool Manager” role are in charge of review suggestions and approve/deny the publication. For more details about the Tool&Services application see section 8.2.

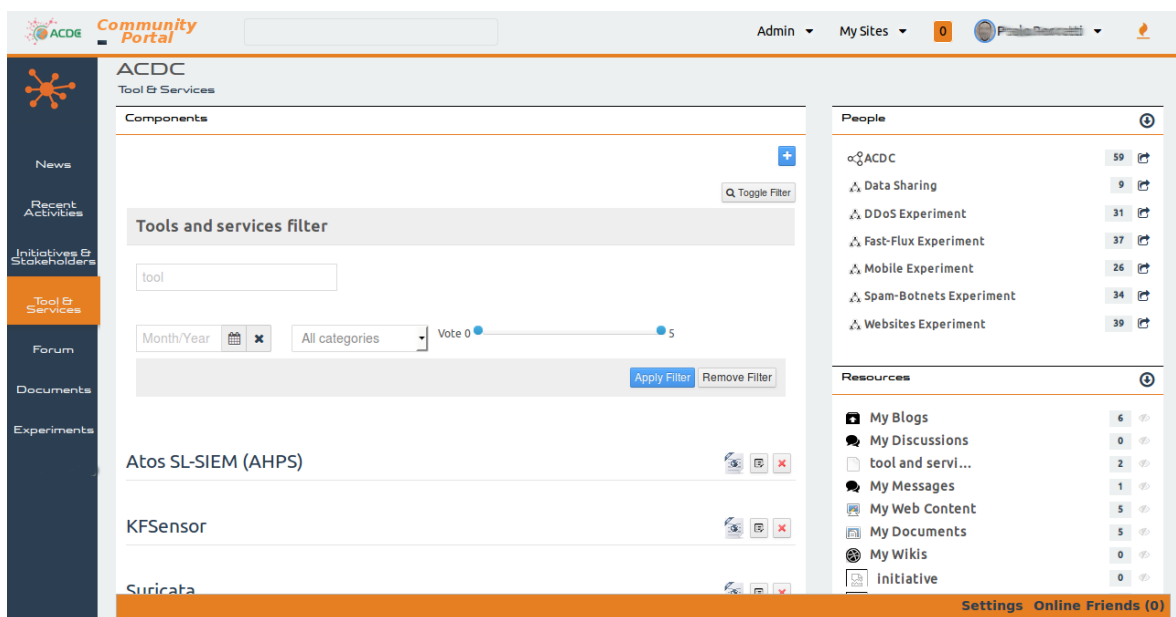


Figure 6 – Tool&Services

The ACDC Forum is the place collecting all the discussions among community members. The stakeholder uses this application to see all the comments, messages, threads and related posts published in the portal. All the content can be filtered by keyword. Thanks to this application the stakeholders will be able to read all the content related to a specific topic and to actively contribute to the Forum by posting comments. Specific sections of the forum are dedicated to discussions about tool and services, regulations, how to use the community portal, etc.

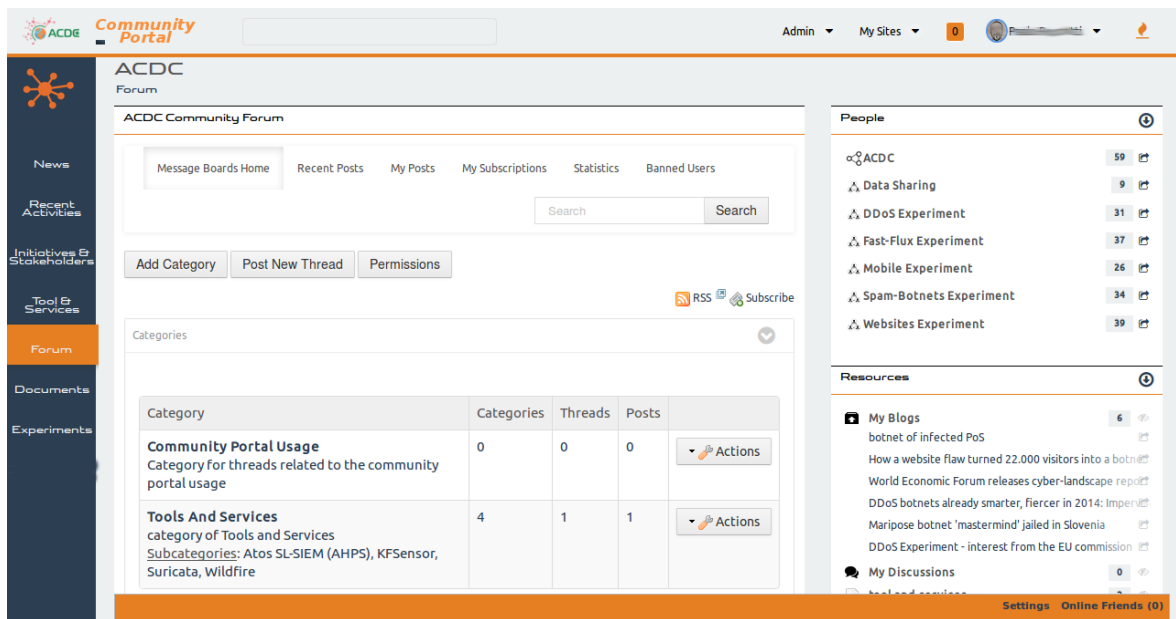


Figure 7 – Forum

7.3. The Experiments Workspaces

Besides Public and private network areas of the community portal, some workspaces have been also introduced to host information about topics of particular importance in the ACDC project. This is the case for ACDC Experiments, that benefits from a set of dedicated workspaces, one for each experiment.

Workspaces for experiments can be accessed by the People application, part of the OPENNESS framework. Members of the ACDC Community will have the possibility to request participation to a botnet experiment, while the access to the experiment descriptions – explaining the benefits a participant would get by joining the experiment – is publicly accessible.

By participating to an experiment a stakeholder will be able to get access to the dedicated *Experiment Workspace*, where a set of specific information (experiment news, experiment documentation, participants list, etc.) will be available.

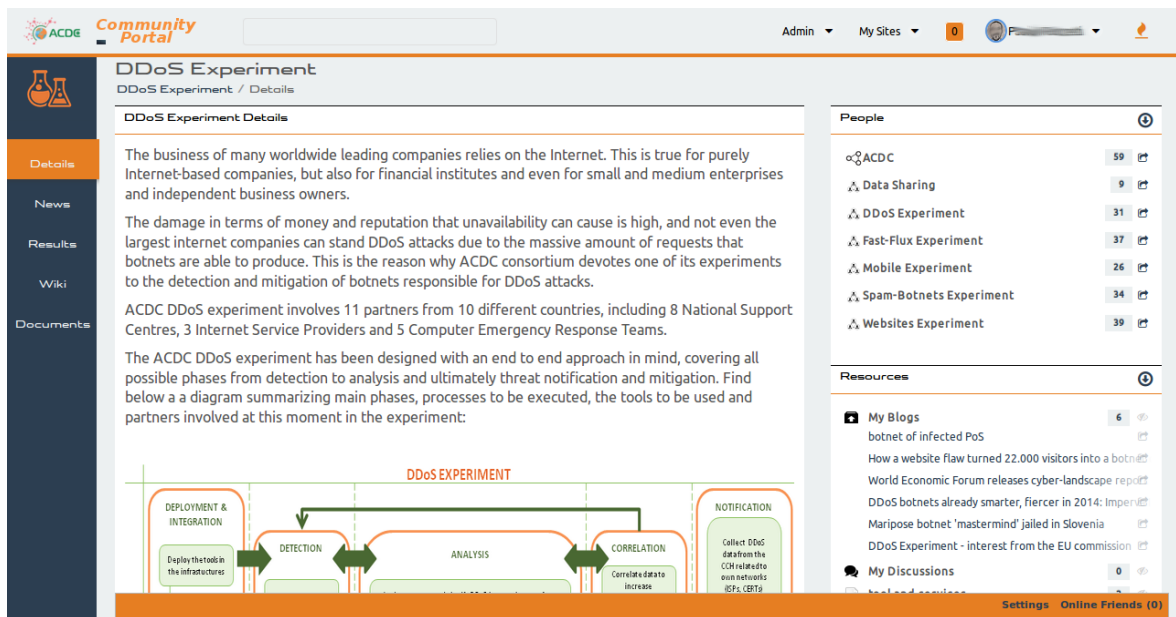


Figure 8 – The ACDC Experiment Workspace

7.4. The Data Sharing Workspace

In the ACDC community, the stakeholder will be able to share data with other stakeholders and receive data from other stakeholders. The sharing of data happens through the Central Clearing House (CCH). The role of the community portal in the data sharing is to identify stakeholders entitled to ask for (or provide) data among the community and to allow them to set the rules that constrain the data sharing within the community. This is done in the Data Sharing Workspace within the community portal.

It is worth noting that the actual data flows among the CCH and the participants' systems, without going through the ACDC community portal. This avoids both performance issues, both the risk of compromise the information in case of eavesdropping of community portal traffic.

The Data Sharing Workspace contains information about how to connect participants systems to the CCH services, as well as to discuss the data format that are provided to, and can be retrieved from, the CCH. **This workspace also provides access to a dedicated application to manage access controls to the CCH: the Data Access Manager (DAM).** Essentially, DAM allows community participants to (i) manage the access control keys (API-Keys) that are used to send or retrieve data from the CCH and (ii) set sharing policies for data sharing with other community members. Moreover, DAM allows CCH administrators to set general controls on the kind, and amount, of information each community participant can retrieve or provide to the CCH. These controls are then enforced by the CCH itself. Detailed information about the DAM can be found in section 8.4.

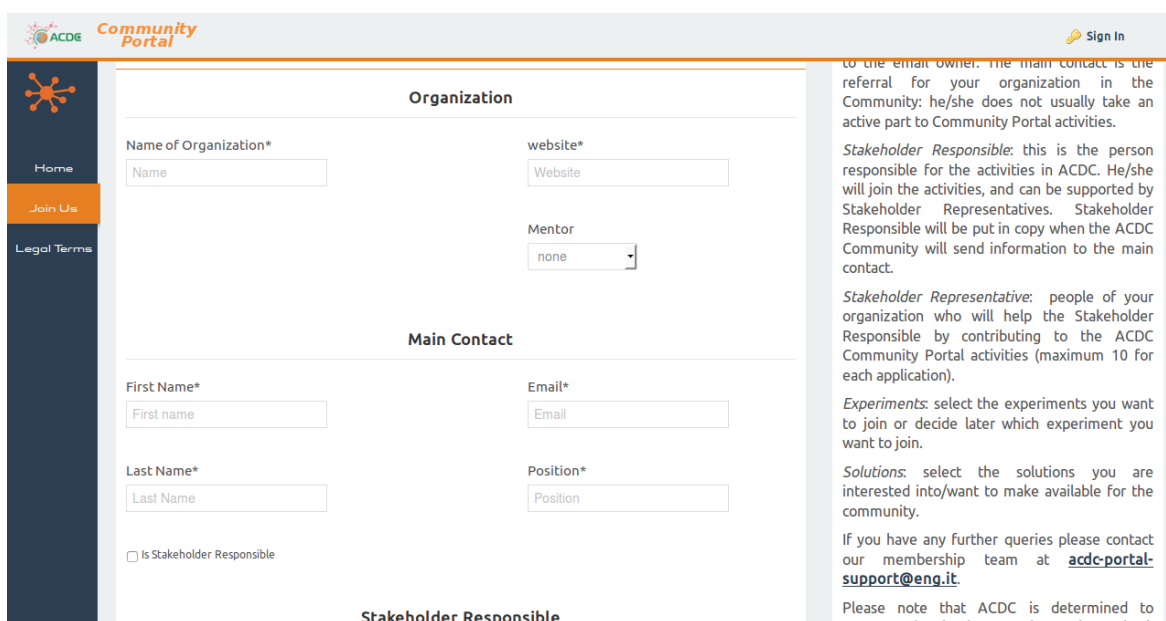
8. The ACDC Portal Applications

This section describes in more detail the applications that have been developed (or adapted) to fulfil ACDC Community needs. The section focuses on four main applications already developed, or still under development, for the ACDC Community: Joining, Initiatives&Stakeholders, Tool&Services and the Data Access Manager (DAM).

NOTE: screenshots and diagrams below refers to the version of OPENNESS applications currently published in the ACDC community portal, and may be subject to changes and improvements at a later stage of the ACDC project.

8.1. Joining

As introduced in section 7.1, the joining application is used by new participants to request registration to the ACDC Community. For this reason it is the only application, among those in the ACDC portal, exposing functionalities to unauthenticated users. The registration process works as follows: applicants to the ACDC Community opens the form exposed by the public part of the application, and provides minimal set of information about them and the organization they belongs to. Information about the Organization includes the Organization Name, the Organization Website, the mentor organization, if any, and the profiling of the organization based on the categorization criteria defined in D6.1.1 - User Profiles and Categorization of the ACDC project [7].



The screenshot shows the 'Joining Form' on the ACDC Community Portal. The form is divided into two main sections: 'Organization' and 'Main Contact'. The 'Organization' section includes fields for 'Name of Organization*' (with a sub-field 'Name'), 'website*' (with a sub-field 'Website'), and a 'Mentor' dropdown menu currently set to 'none'. The 'Main Contact' section includes fields for 'First Name*' (with a sub-field 'First name'), 'Last Name*' (with a sub-field 'Last Name'), 'Email*' (with a sub-field 'Email'), and 'Position*' (with a sub-field 'Position'). There is also a checkbox labeled 'Is Stakeholder Responsible'. To the right of the form, there is a sidebar with text explaining the roles of 'Stakeholder Responsible' and 'Stakeholder Representative', and instructions for selecting experiments and solutions. At the bottom of the sidebar, it provides contact information for the membership team at acdc-portal-support@eng.it and a note about ACDC's commitment to protect and maintain user privacy.

Stakeholder Responsible
Figure 9 – Joining Form

In this context, the Mentor Organization is another organization, already member of the ACDC community, that could act as a trusted anchor to evaluate the membership request by the new organization. Moreover, once the registration process has been completed, the mentor organization will provide a temporary guidance to the new member in contributing to community activities and interactions.

Once the application request is received by the portal, participants holding the Application Manager role are alerted by email of the new registration request. The Stakeholder Responsible

of the organization indicated as mentor, if any, is also notified of the new request. Application Managers can then connect to the administrative interface of the portal to handle the application request (by approve or deny it). Managers can also contact the mentor organization, if one has been specified in the form, to get more information about the applicant organization and better evaluate the joining request.

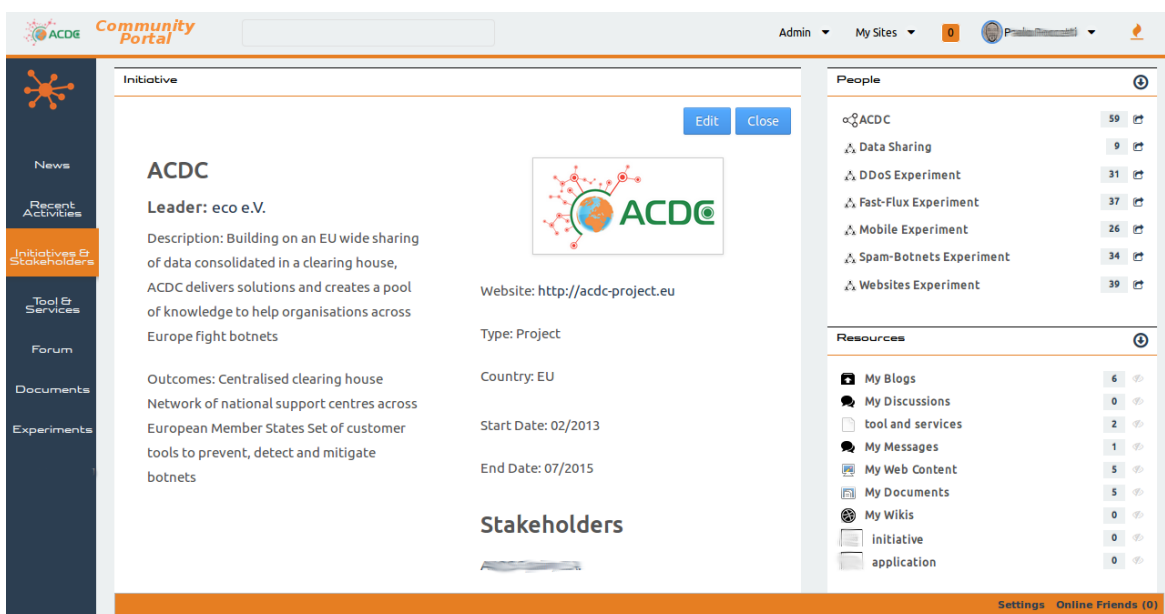
Once the request has been approved, the people indicated in the application form are notified of the result, and, in case of approval, the new organization becomes visible in the Stakeholders tab of the Initiatives&Stakeholders application (see below). Additionally, the people indicated as Stakeholder Responsible and Stakeholder Representatives will receive, at the email address indicated in the form, the account details to login to the community portal.

8.2. Initiatives & Stakeholders

The Initiatives&Stakeholders application, introduced in section 7.2, is organized in four tabs (**Initiatives**, **Pending Initiatives**, **Stakeholders** and **Graph**), this provides the ACDC participants with a more organized view on the application content.

The *Initiatives* tab contains the list of initiatives dealing with the botnet domain. The action links at the right side on each entry also allows Initiative Managers to edit the corresponding initiative. Furthermore, through the controls at the top of the list, ACDC participants can suggest new initiatives to be included. Once a new suggestion is submitted, by filling the related form, Initiative Managers are notified (by following the Publication Workflow described in section 5.3) and will find the new suggestion in the Pending Initiatives tab, where they can access the suggestion details and approve/deny it. (see section 7.2 for a screenshot of the Initiatives tab)

By clicking on each entry in the list a detail about the related initiative is displayed. Main information for each initiative are the Initiative name, the leading Stakeholder, if any, and the participant Stakeholders. Additionally, a short text about the initiative and the expected outcomes is also stored, as well as start and end dates, and the initiative website.



The screenshot displays the 'ACDC' initiative details within the 'Community Portal'. The interface includes a top navigation bar with 'Admin', 'My Sites', and a user profile 'Piero (Guest)'. A left sidebar lists navigation options: 'News', 'Recent Activities', 'Initiatives & Stakeholders' (highlighted), 'Tool & Services', 'Forum', 'Documents', and 'Experiments'. The main content area shows the 'Initiative' details for 'ACDC', including its logo, leader 'eco e.V.', description, website 'http://acdc-project.eu', type 'Project', country 'EU', start date '02/2013', and end date '07/2015'. A 'Stakeholders' section is also visible. On the right, a 'People' sidebar lists various experiments and resources with their respective counts.

Entity	Count
ACDC	59
Data Sharing	9
DDoS Experiment	31
Fast-Flux Experiment	37
Mobile Experiment	26
Spam-Botnets Experiment	34
Websites Experiment	39

Entity	Count
My Blogs	6
My Discussions	0
tool and services	2
My Messages	1
My Web Content	5
My Documents	5
My Wikis	0
Initiative	0
application	0

Figure 10 – Stakeholder Detail

Beside initiatives, the application also allows, in the **Stakeholders tab**, to browse the list of **Stakeholders participating to initiatives**. The Stakeholders included in the list are therefore not only those members of the ACDC Community, but also external ones, dealing in some ways with the botnet domain. The list also allows Initiative Managers to add new Stakeholders to the list, to reference them in related initiatives. The involvement of each stakeholder in the ACDC community is also reported in the “Membership” column of the list.

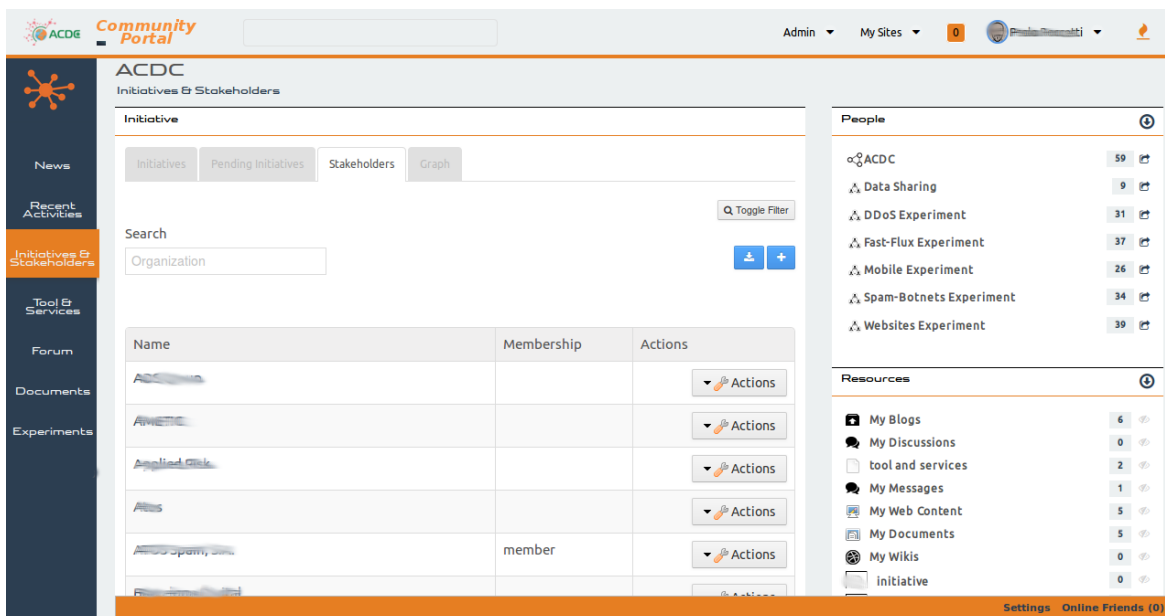


Figure 11 – Stakeholders List

Each entry in the Stakeholders list can be clicked for details on the related stakeholder. Besides overall information (logo, website, legal address, etc.), the information collected for each Stakeholder corresponds to the categorization criteria presented in deliverable D6.1.1 – User Profiles and Categorization [7]: Country of operation, Sectors, Cybersecurity Positioning Areas, ACDC Experiments, ACDC Solutions. Additionally, the Stakeholder detail displays the list of initiatives the Stakeholder is participating to.

For Stakeholders members of the ACDC Community this page also reports *Main Contact* information, as well as *Stakeholder Responsible* and *Representatives* from that organization that are contributing to the community.

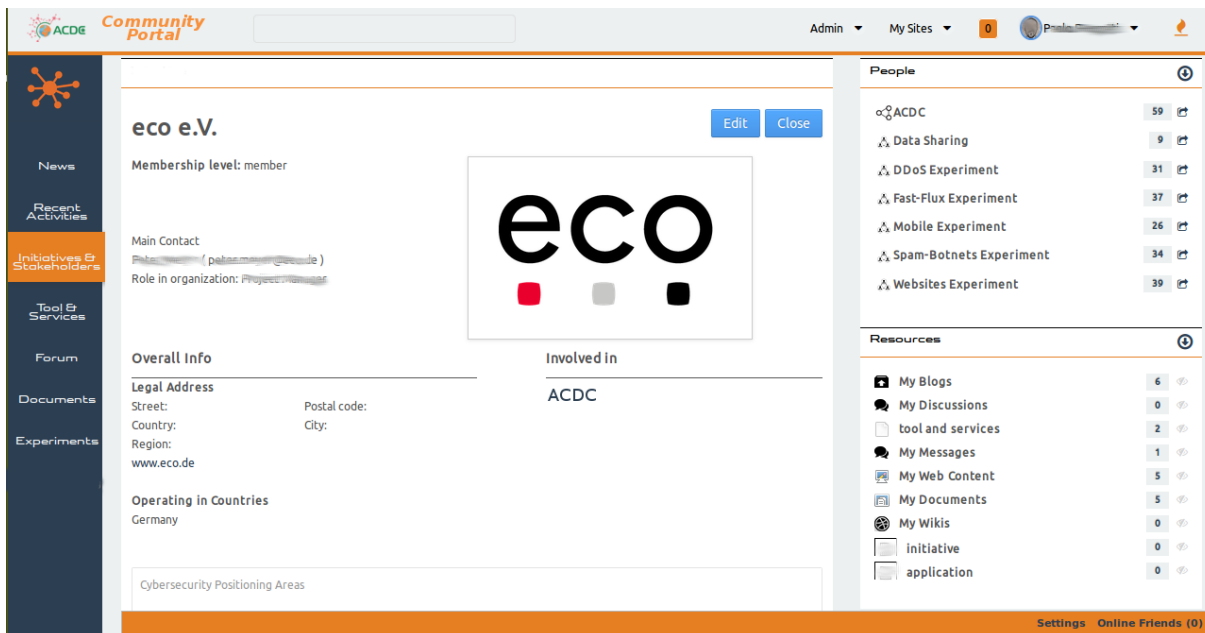


Figure 12 – Stakeholder Detail

Finally, a **graph view of relationships between stakeholders and initiatives is available in the Graph tab**. As the resulting graph may be large and difficult to browse, all the filters already present in the stakeholders and initiatives tab have been also replicated here. Furthermore, all the entities in the graph (stakeholders, displayed as rectangles, and initiatives, displayed as ellipses) are linked to the related detail for an easier access to the information.

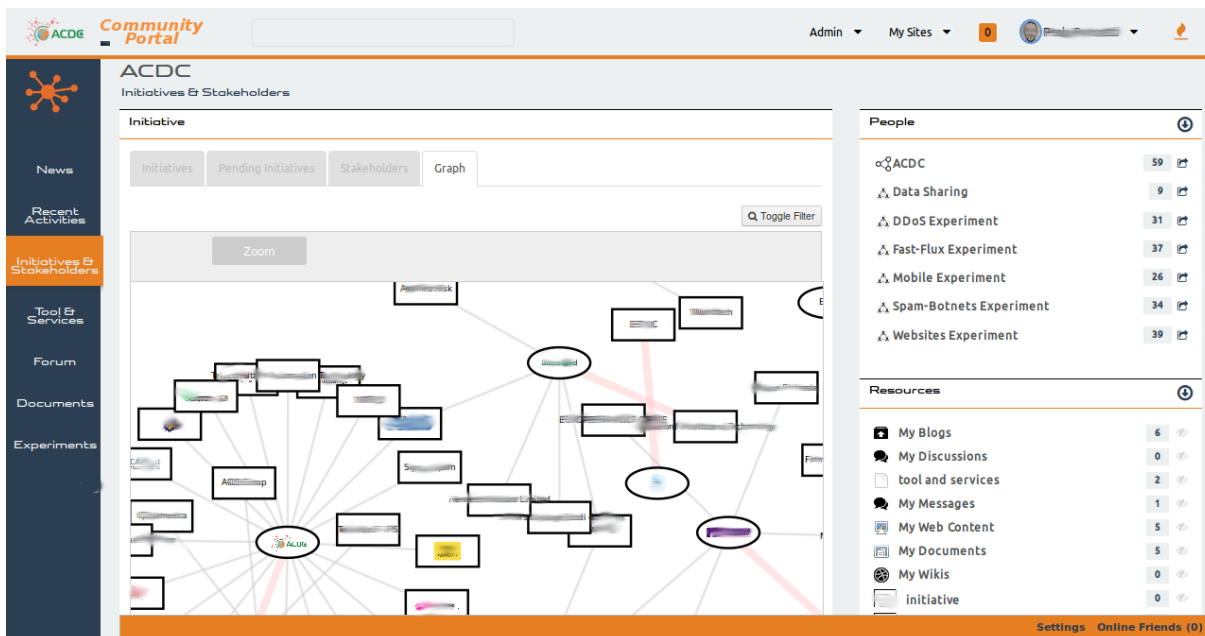


Figure 13 - Initiatives Graph

8.3. Tool & Services

As introduced in section 7.2, the **Tool&Services application** is used to discover the tools and services currently available to fight botnets. The application is structured in a single page. It

presents a list of the tool and services currently reported. Each entry of the list can be clicked to get additional information.

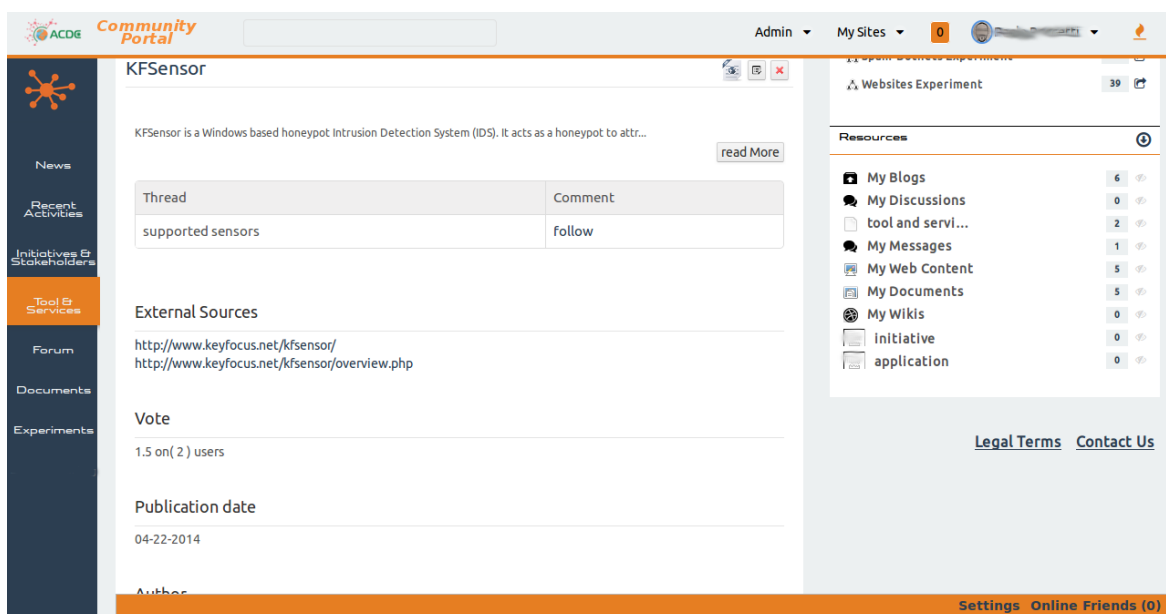


Figure 14 – Tool&Service Detail

Each tool entry includes a brief description of the tool functionalities, external links for further information, the publication date, additional notes on the tool, etc. Furthermore, each tool is categorized according to the categories introduced in deliverable D2.3 - *Technology Development Framework* [6].

Beside information already described, two additional features have been implemented in the Tool&Service application to stimulate the community interaction: **tool voting** and **link to the Forum**.

Through the **tool voting** system community participants can express their opinion about each of the tools in the list. This gives potential tool users an indication about what is the community opinion about each tool. Votes may vary on a range from 0 to 5, and the average vote for each tool is also influenced by the number of votes collected for the tool itself: a tool with very few votes (e.g. less than 5) of highest value (e.g. all 5) score less than a tool with a high number (e.g. more than 50) of good votes (e.g. average value 4).

Beside voting, the community interaction around tools is also supported by linking back discussions about each tool in the Forum. **Link to Forum** gives community participants a way to request and provide community support on tool aspects, usage and previous experiences made by other community members. To this aim, a dedicated category is created in the forum each time a new tool is added to the list. The titles of discussions in the corresponding category are listed back in the the tool detail. A “follow” button allows community participants to move to the forum and follow/contribute to tool discussion of interest.

The inclusion of new tools and services in the list follows the **Publication Workflow** (introduced in section 5.3). ACDC participants can either suggest for new tools or services to be included, or report about changes in tools, as well as errors in tool description, or external links to be fixed. Once a new suggestion is submitted, by filling the related form, Tool Managers are notified and

will find the corresponding report in their administrative page, where they can access the suggestion details and approve/deny it.

8.4. Data Access Manager (DAM)

NOTE: As the DAM is still under development, the level of detail provided in this section is considerably different from the previous ones, that refers to application already deployed in the portal.

This section describes the functionalities supported by the Data Access Manager (DAM) application. This application interacts with the Central Clearing House (CCH) to request and push authentication and access control information for data stored in the CCH itself. The DAM application is currently being implemented in the context of WP2. Nevertheless, the DAM interface functionalities are reported in this document, as they're part of the ACDC Community portal functionalities.

Following diagram provides an architectural overview of the DAM component. The data exchange between the DAM module and the CCH will be done through REST technology (Representational State Transfer) over an SSL connection. HTTP requests are protected by authentication based on an access token (API-Key) shared between the CCH and the Community portal at deployment time.

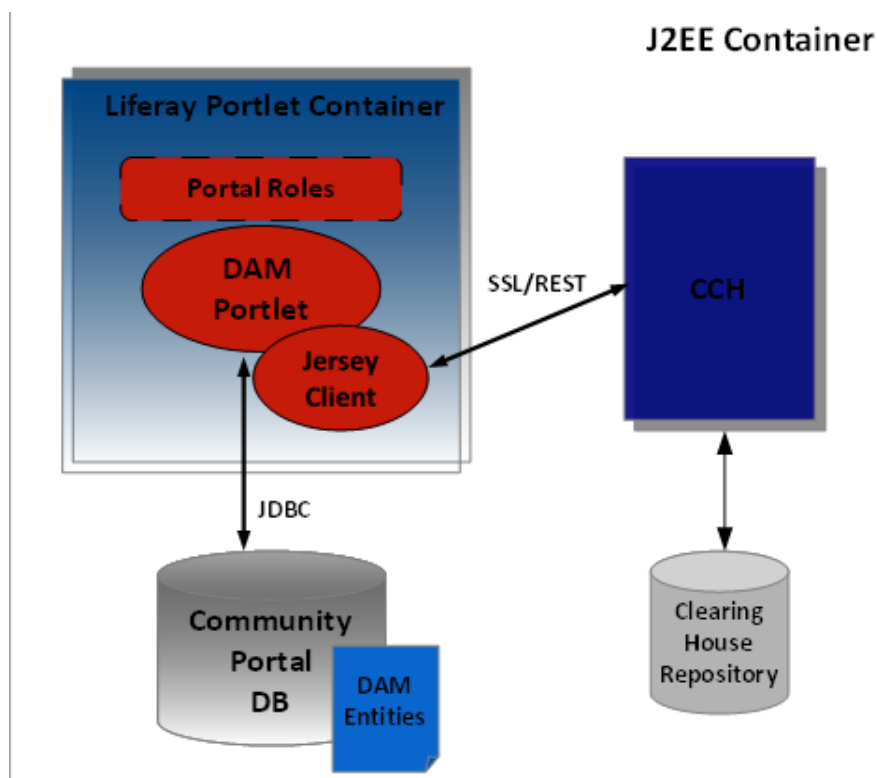


Figure 15 – DAM Architecture

The DAM and the community portal provide an interface to require and manage keys provided from the CCH. The CCH provides the service layer (based on REST notation), used by the DAM as a backend.

Only additional information about access tokens and connection parameters are stored in the community portal (DAM Entities in the picture), while the rest of data (including the access tokens itself) are provided by the CCH at runtime. This avoids the community portal to store all the list of access tokens that enables interaction with the CCH, thus avoiding being a single point of attack.

Stakeholders willing to connect their systems to the CCH needs to be authorized by CCH Managers to do so. The process to give access to CCH functionalities to a new Stakeholder is shown in the diagram below.

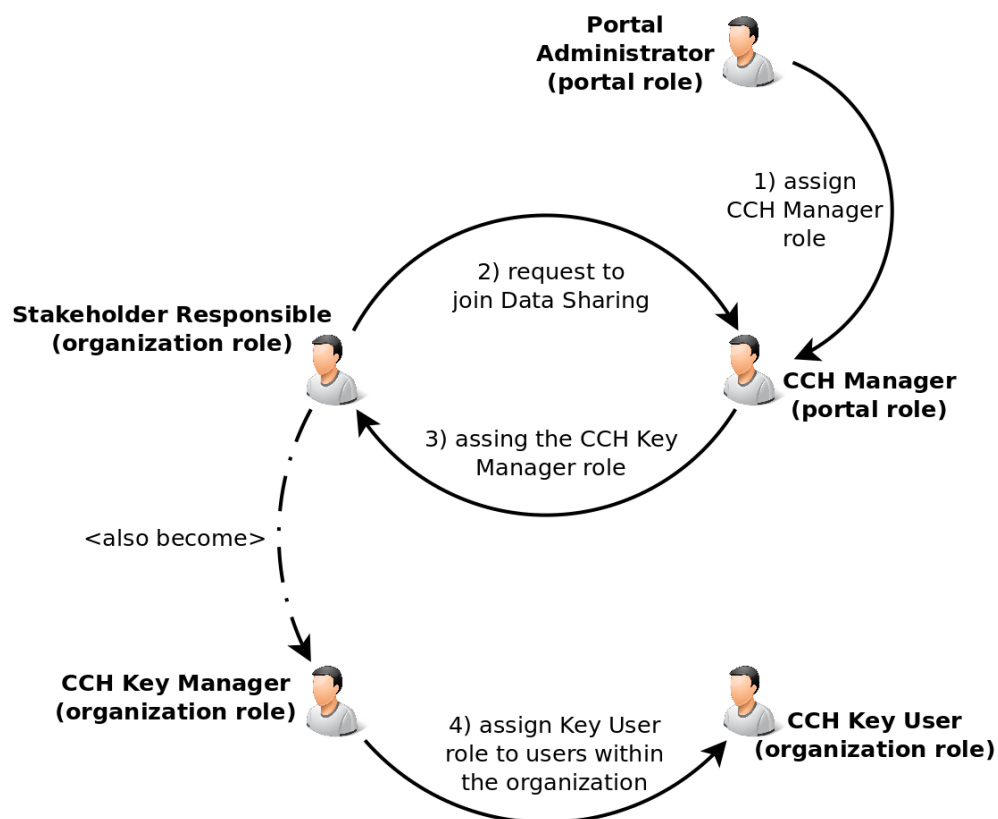


Figure 16 – DAM Role Model

Similarly to other parts of the ACDC Community portal, the access to DAM functionalities is bound to a set of roles in the community platform. Roles are of two types: *regular* (i.e. assigned across the whole community portal) and *organizational* (i.e. assigned in the context of a given organization). The assignment (and revocation) of roles is depicted by arrows in the diagram above, and follows the arrows numbering in the picture. At the end of step 4 the CCH Key User is able to use DAM functionalities to create API-Keys. These keys can be used to authenticate Stakeholders systems to the CCH. The set of functionalities granted to each role is listed below.

Portal Administrator

It is a regular role already present in the Community Portal. This role is able to manage any resources in the portal. Concerning the DAM, this role can assign the CCH Manager role to a user of the community portal.

CCH Manager

This role is able to define connectivity between CCH and DAM and it allows to use the Group Management functionalities. This role can:

- Assign the role of CCH Key Manager to the user responsible of a member organization
- Set / Update access token for connection between DAM and the CCH
- Manage group parameters and join organizations to the groups. At the moment four groups have been defined:
 - Unverified – organizations that have not yet been assigned to any other group
 - CERT – Computer Emergency Response Team
 - ISP – Internet Service Providers
 - Antivirus – Antivirus companies

Each group has a set of parameters such as: TTL (time to leave), Limit of data query, Max numbers of active keys and Type of data retrievable, that are better detailed in the CCH documentation.

CCH Key Manager

This organizational role allows the user to manage keys belonging to the organization. In fact only a key manager can perform following actions:

- Get list of CCH Api keys of the organization
- Set/unset CCH Key User role to other users of the organization
- Invalidate Api key of a CCH Key User in the organization

CCH Key User

This role can be set to any user of the organization. The role allows the user to require Api-Key to the CCH, and manage sharing policies for provided data. The following is the list of actions a CCH Key User is entitled to perform:

- Create a new Api key, specifying if the key is in read (data retriever) or write (data provider) mode. If the key is in read mode means that the user wants to read information of others organizations. Instead, in write mode means that a user wants to provide data with a given data schema, specified at key creation time.
- Get list of created keys grouped by read or write mode.
- Update key
- Invalidate key
- Get Key (from a recovery process)
- Manage sharing policies:
- View pending request from and to Organizations
- Approve / Deny request of data sharing
- View list of sharing policies in place and revoke them.

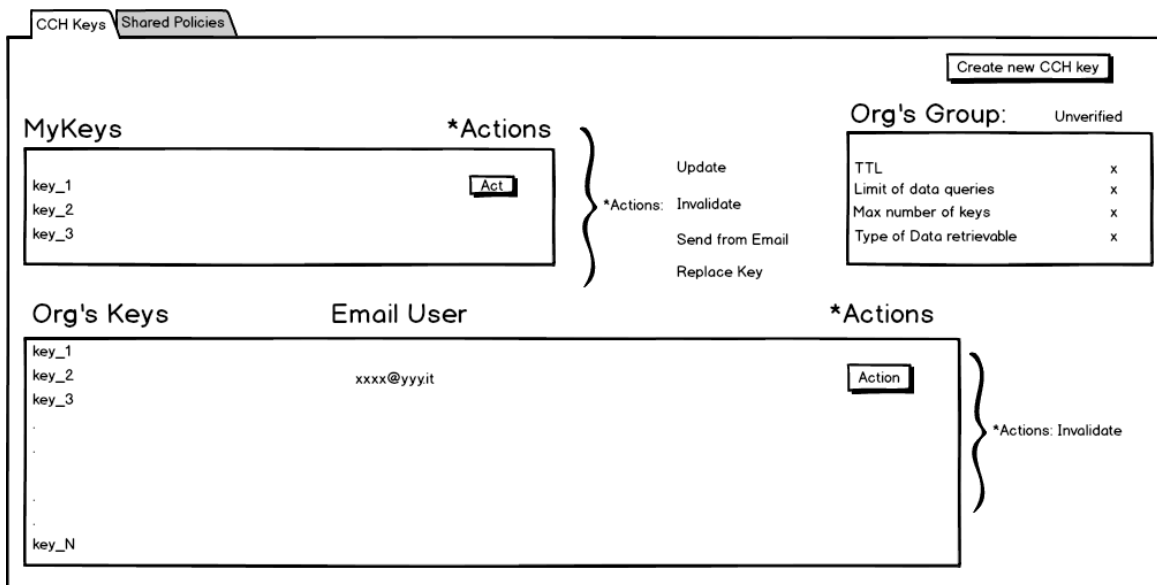
According to the set of roles, and corresponding functionalities, listed above **the DAM application has been divided in three tabs: Key Management, Group Management and Sharing Policies Management.**

The Key Management tab allows the CCH Key User to get the list of owned keys and, if it holds the CCH Key Manager role, also allows to get the list of all keys created by users of the organization. Moreover, the user interface allows the user to:

- *Create new CCH key* (for CCH Key Manager and CCH Key User) - This action allows creating new keys on the CCH. It displays a form in which the user can choose the type of required key (read or write). The created key is associated to the email address of the user and to the CCH group the organization belongs to. As mentioned above, only the CCH Manager can assign organizations to CCH groups. If the required key is in write mode, the form

provides an input field in which the user has to fill with the link to the data schema associated to the data sent by using the key.

- *Add a new CCH Key User* (for CCH Key Manager only) - This functionality displays a form with the list of users of the organization. Each user can be selected from CCH Key Manager to assign him/her the CCH Key User role in the context of the organization, thus enabling the use of DAM functionalities described above.



The interface shows the 'CCH Keys' tab selected. It features a 'Create new CCH key' button in the top right. The main content is divided into three sections:

- MyKeys:** A list of keys (key_1, key_2, key_3) with an 'Act' button.
- Org's Group:** A table showing parameters and their values:

Parameter	Value
TTL	x
Limit of data queries	x
Max number of keys	x
Type of Data retrievable	x
- Org's Keys:** A list of keys (key_1, key_2, key_3, ..., key_N) with an 'Email User' field (xxxx@yyy.it) and an 'Action' button.

Additional actions available include: Update, Invalidate, Send from Email, and Replace Key.

Figure 17 – DAM Key Management

The key management tab displays information about (i) keys owned by the user (My Keys), (ii) the group the organization belongs to (My Group) and (iii) the list of keys of the organization the user belongs to (My Organization). The latter information is only available to users with the CCH Key Manager role. Each section provides a set of actions for key administration (create key, update key, invalidate key, replace key, etc.)

To ensure a higher protection of keys, they are shown directly to the user at creation time only. Later retrieval of the key values adopts the following process: to get a key value, the user requires it from the portal than, in turn, sends an email to the user address with a redirect link. When the user clicks on the redirect link, the DAM component checks the authenticity of the request and, if everything is correct, shows the key value to the user in the browser. This provides a better protection, as an attacked needs, at the same time, to get control of the portal account and of the mailbox of the user.

The **Group Management tab** is only accessible to users with the CCH Manager role. This part of the interface allows to:

- *Manage connection keys to the CCH* - To communicate with the CCH (see section "How the CCH and DAM communicates"), DAM component has to be configured with appropriate parameters such as Access token, Host, Port and Base URL. Once the access token has been set, it can be only accessed by using the recovery process put in place for keys (see section above).
- *Set parameter values for CCH groups* - This section allows the CCH Manager to set parameters for the group, namely the time to leave, the limit of data query, the max numbers of active keys and the type of data retrievable. The CCH Manager will be notified by a message once the parameters are successfully set.

- **Assign Organizations to CCH groups** - When the CCH Manager assign an organization to a CCH group then the organization will inherit all the configuration parameters for that group. This action must be performed to enable CCH Key Users of the organization to create new keys.

CCH Keys
Pending Request
Shared Policies
Manage Groups

Access Token

☒

CCH's Groups

Unverified
ISP
CERT
Antivirus

TTL
Limit of data queries
Max number of keys
Type of Data retrievable

Stakeholder	Stakeholder Responsible	CCH's Group
Org_1	firstName - lastName - xxx@kk.it	Unverified
Org_2	firstName - lastName - xxx@kk.it	ISP
Org_3	firstName - lastName - xxx@kk.it	Unverified
Org_n	firstName - lastName - xxx@kk.it	Antivirus

Figure 18 – DAM Group Management

The **Sharing Policies Management tab** allows the CCH Key Users to manage the sharing policies that constraints the access by other organizations to the data provided to the CCH. In order to manage links between organizations, the user interface is composed by 3 different sections. First contains the outgoing requests for data sharing (My Requests), second displays incoming requests for data sharing (Pending Requests) and third shows sharing agreements between organizations already in place (Sharing Policies).

CCH Keys
Shared Policies

My Requests

Request To	I/O	Schema	Status▼
Org_1	In-bound		pending
Org_2	Out-bound	schema1	deny
Org_3	In-bound		pending

Create new Request

Pending Requests

Request To	I/O	Schema	Actions ▼
Org_5	In-bound		approve/deny
Org_6	Out-bound	schema1	approve/deny
Org_7	In-bound		approve/deny

Sharing Policies

Org Name	Action ▼
Org_x	Unlink
Org_y	Unlink
Org_z	Unlink

Figure 19 – DAM Sharing Policies Management

The My Requests view contains the list of requests to others organizations. A column called “I/O” specifies if the data flow is “inbound” (i.e. data are provided by the other organization and accessed by the requester) or “outbound” (i.e. data are provided by the requester and accessed by the other organization). Another column “Status” regards the status of the request (pending or deny). **The Create New Request functionality allows the CCH Key Users to request for a new sharing policy.** First of all the user get the list of the organizations that are connected to the CCH. Once the user selects an organization, a sharing request will be send to the CCH Key Manager of that organization for approval. If the request gets approved by the other party, the CCH will be notified to apply the new policy to the two keys involved in the data exchange. The new sharing policy is then shown in the sharing policies section (see below).

The Pending Requests section shows the incoming requests from others organizations. After an analysis of the data sharing request, the user owning the involved key can approve or deny the request. The requesting organization is then informed about the decision.

The Sharing Policies section shows all the sharing policies already in place between keys belonging to the user and other organizations. This section also allows the user to unlink sharing policies from his/her own keys. This is implemented by sending a request of unlink to the CCH. Form that time the keys get unlinked and the sharing policy is deleted. One important aspect regarding the unlink action is that it doesn’t delete the key, but just set it as unlinked.

9. Conclusion

The deliverable describes the first release of the ACDC portal. The additional functionalities with respect to the initial plan in the DoW have considerably enhanced the platform to position it as the central entry point to activities in ACDC. Additional developments have been undertaken to support this evolution, and the ACDC platform has been deployed internally (i.e. for consortium partners) in March 2014, to be then opened to members with signed Letters of Interest at the ISD conference in September 2014 [8]. Current version of the platform implements the main use cases introduced in deliverable D6.3.1 - Involvement model for users in ACDC [3], while the remaining ones are being developed and will be deployed in the coming months. Additionally, social analytics will be defined for the platform by end of 2014 (refer to D6.2.2), after some months of adoption and initial platform usage and reported by 31st January 2015, allowing for 4 months of usage after launch event.

Specific activities (described in the updated release of deliverable D6.3.2 and in recommendation 1.7 to 1st review meeting) have also been put in place to foster adoption and usage.

10. References

- [1] http://en.wikipedia.org/wiki/Don_Tapscott
- [2] http://www.ted.com/talks/don_tapscott_four_principles_for_the_open_world_1.html
- [3] D6.3.1 - Involvement model for users in ACDC, 2014
- [4] Role-Based Access Controls, <http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf>
- [5] OPENNESS, <http://openness.eng.it/>
- [6] D2.3 - Technology Development Framework, 2014
- [7] D6.1.1 - User Profiles and Categorization, 2014
- [8] Internet Security Days 2014, <http://isd.eco.de/en/>