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

Deliverable	**D1.1.1 Overall Software Architecture Description**
Work package	WP1 Requirements & Specifications
Due date	M12
Submission date	31.01.2014 (Re-Submission 29.08.2014)
Revision	1.6
Status of revision	FINAL
Responsible partner	ECO
Contributors	Michael Weirich (ECO) Thorsten Kraft (ECO) Peter Meyer (ECO)
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	X
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)	

Rev.	Date	Author	Notes
V0.1	10/10/2013	Michael Weirich (ECO)	Initial structure of the document / table of content
V0.2	18/10/2013	Michael Weirich (ECO)	Revised table of content, provided details to bullet points.
V0.3	15/11/2013	Michael Weirich (ECO)	Revised, software description for the ABBZ
V1.0	20/01/2014	Michael Weirich (ECO)	Added sensors, CCH description, data input
V1.1	10/07/2014	Peter Meyer (ECO)	Refinement concept
V1.2	22/07/2014	Peter Meyer (ECO)	Introduction, Tools and Sensors v.1
V1.3	24/07/2014	Michael Weirich (ECO)	Centralized Clearing House
V1.4	07/08/2014	Peter Meyer (ECO)	Tools and Sensors v.1
V1.5	11/08/2014	Thorsten Kraft (ECO)	Security concept
V1.6	14/08/2014	Thorsten Kraft (ECO)	Overall Legal Concept

Glossary

ACDC	Advanced Cyber Defence Centre
CCH	Centralized (Data) Clearing House
SME	Small-and Medium Enterprises
DoW	Description of Work, Part B Form of the Amendment
NSC	National Support Centre
ISP	Internet Service Provider
DDoS	Distributed Denial of Service
DoS	Denial of Service
IdMS	Identity Management System
TI	Trusted Introducer
STIX	Structured Threat Information Expression
API	Application-Programming-Interface
SotA	State of the Art
HTTP	Hypertext Transmission Protocol

Index

1 Introduction

The ACDC project has a multi-stakeholder approach and sets a focus on standardized data formats, standardized reporting formats and compliance to European Law, allowing interested parties from different industries, research or public entities to join the common approach of fighting botnet. The project enforces community building by reducing technical and legal boundaries across Europe, opening the project and intelligence to an end-to-end approach of pan-European data sharing.

The ACDC project is an integrating project of existing components and most of the tools or sensors provided by ACDC partners are existing tools from their fight against botnets. The combinations of these puzzle pieces and the interaction with each other is the ACDC approach - one effective, centralized and collaborational solution against the rising threats of cybercrime.

The central component of the ACDC project is a Centralized Data Clearing House (CCH). The purpose of this centralized approach is to provide one centralized storage facility, collecting all relevant data that is necessary to detect and mitigate botnets. The CCH itself has no intelligence to provide the analysis of botnet-related data. Therefore, the CCH has been designed as an open platform, supporting the integration of external tools, sensors or any other components for an effective detection and analysis of botnet-and other cybercrime-related data.

This centralized approach has been chosen to combine the intelligence of all partners involved into the fight against botnets and to use this huge repository of data for an effective solution towards the detection and mitigation of botnets. This approach allows smaller organisation to get access to botnet-related information that their technology might able be able to detect, but failed due to a lack of appropriate and sufficient data. Larger corporations like Internet Service Provider own large datasets, but don’t have access to the intelligence from specialised technology providers or research facilities. Joint intelligence and expertise enhance the possibility of revealing connections between different data sources, which a single partner might not recognize on its own. A mutual database will also enhance a better detection of unknown threats, and offers big advantages to early warning systems. Trends and upcoming threats are seen by multiple partners with multiple sensors and technologies and will support a better view on the landscape of cybercrime.

The overall software architecture of ACDC follows the idea of keeping the infrastructure for collaboration and mutual data sharing as simple and flexible as possible. Interested stakeholders or partners should not be limited from participation as a result of offering inelastic formats, uncommon interface-requirements or inconvenient hardware or software needs.

Next to the requirements for an open and easy adaptable platform, the architecture of ACDC needs to provide an advanced security concept, as the provided service easily runs into a target of hackers or cybercriminals. The provided solution also needs to provide the contributing and participating partners a high level of trust to share their sensitive and proprietary data with other stakeholders. In addition, the ACDC project needs to take privacy and legal requirements into consideration of the overall provided solution. Finally, the conceptual design needs to be future-oriented, as ACDC is intended to become a sustainable solution even after the official end of the pilot in August 2015. An example for this future orientation is the groundwork for supporting IPv6, mobile devices and the internet of things.

2 About this document

This document describes the overall software architecture concept for the ACDC project. Its intent is to provide a high-level overview about the individual components interacting with each other as part of the integration approach.

This document is not a technical description going into the details of considerations, specifications, requirements or frameworks of this project. This document has the intent to act as guidepost through the associated deliverables of this project and how each these deliverables reflect the big picture.

The elaboration and planning of technical specifications, the definition of requirements, the technical implementation and framework, the conduction of experiments and any other relevant activities for the successful execution of this project have been identified in various task groups and documented in associated deliverables of this project.

The tasks and associated deliverables, reflecting the considerations and specifications from the overall software architecture perspective, have been worked out in detail in two different work packages of this project.

The first work package (WP1) is fully dedicated on defining the Requirements & Specifications for the entire project, mainly its technical infrastructure.

Each of the deliverables in this first work package will have two versions, as the development of the ACDC framework is an on-going process.

- The initial specifications and requirement will be defined within the first year of the project
- A 2nd and final iteration at the end of the project will address the full details, lessons learned during the project and the state of the art at the end of the project duration.

A deliverable 1.x.1 describes the first version, a deliverable 1.x.2 its iteration.

The second work package reflects the efforts of the Pilot Components and Technology Development and reflects the practical implementation of the requirements and specifications defined in the first work package.

The key document for this practical implementation is the deliverable **D2.3 Technology Development Framework outlining basic models for integration and delivery principles.**

This deliverable includes a comprehensive lists of all tools used within the ACDC project and the framework how these components interact with each other. The Sota software catalogue is included the Annex; this overall software description will refer to this overview in the next chapters.

The following table shows the deliverables mentioned in this document:

Deliverable	Name
D1.1.1 / D1.1.2	Overall Software Architecture Description
D1.2.1 / D1.2.2	Specification of Tool Group "Centralised Data Clearing House"
D1.3.1 / D1.3.2	Specification of Tool Group "Support Centre"
D1.4.1 / D1.4.2	Specification of Tool Group "Malicious or Vulnerable Websites"
D1.5.1 / D1.5.2	Specification of Tool Group "Network Traffic Sensors"
D1.6.1 / D1.6.2	Specification of Tool Group "End Customer Tools"
D1.7.1 / D1.7.2	Data Formats Specification
D1.8.1 / D1.8.2	Legal requirements
D2.3	Technology Development Framework outlining basic models for integration and delivery principles
D2.4	Executable Service Code
D2.5	Business Process Test Cases and Scripts
D3.1	Planning reports of the experiments
D3.2	Design report of each experiment
D4.1	Documentation of Botnet Metrics-Methodology and Development

Overview of task associated to the document correlating to associated deliverables.

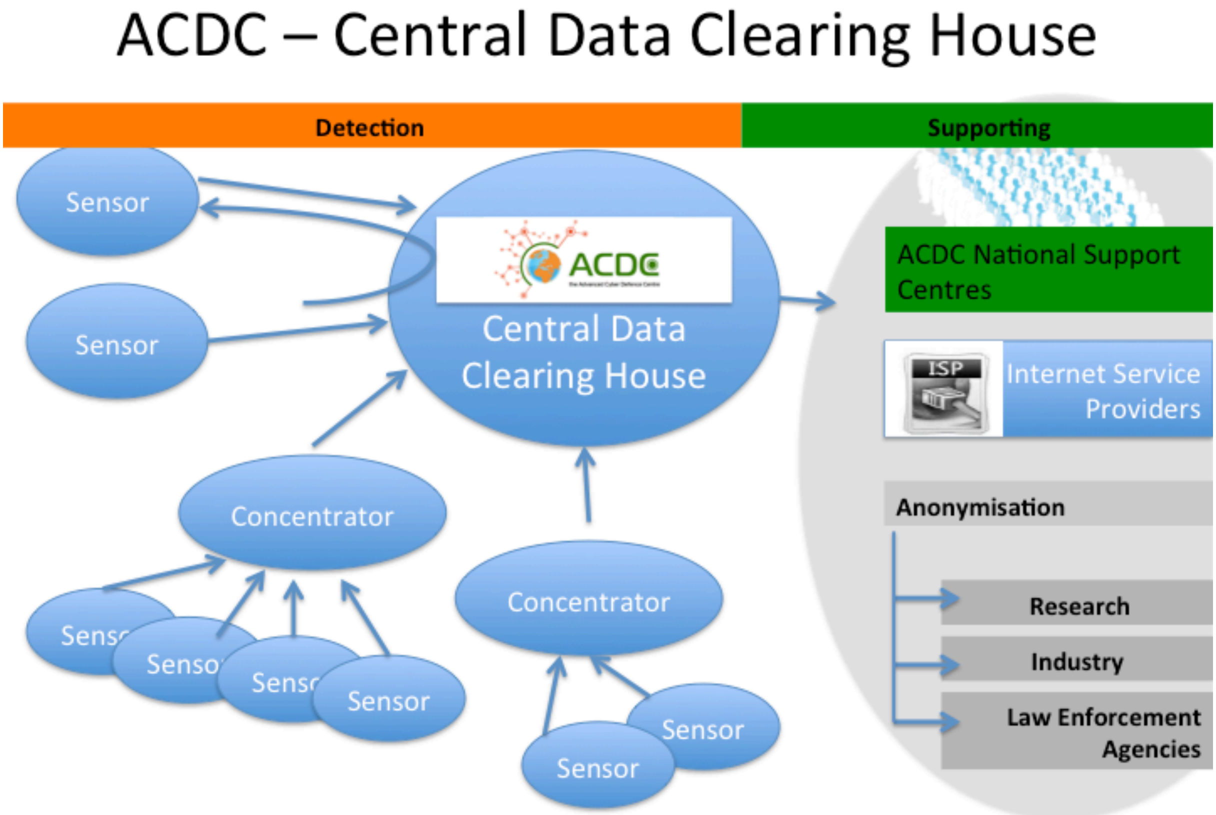
Task #	Task Name	Associated deliverable
Task 1.1.1	General Architecture	D 1.1.1, D 1.1.2
Task 1.1.2	Centralised Data Clearing House	D 1.2.1, D 1.2.2
Task 1.1.3	Support Centre	D 1.3.1, D 1.3.2
Task 1.1.4	Malicious or Vulnerable Website Analysis	D 1.4.1. D 1.4.2
Task 1.1.5	Network Traffic Sensors	D 1.5.1, D 1.5.2
Task 1.1.6	End Customer Tools	D 1.6.1. D 1.6.2
Task 1.1.7	Data Format Definition and Coordination of Application	D 1.7.1, D 1.7.2
Task 1.1.8	Malware Prevalence Analysis	D 1.7.2, D 4.1
Task 1.2.1	Legal analysis and requirements	D 1.8.1
Task 1.2.2	Follow-up of legal requirements	D 1.8.2
Task 1.3.1	Development of Botnet metrics	D 1.7.2, D 4.1
Task 2.1	Establishing and Management of Pilot Governance Group	D 2.1
Task 2.2	Developing Technology Framework	D 2.3
Task 2.3	Developing Pilot Component Task Forces	D 2.2
Task 2.4	Pilot Component Developments	D2.3, D2.4
Task 2.5	Change management	D2.3, D2.4 and D2.5
Task 2.6	Component Development Quality control management	D2.4, D2.5

3 The ACDC Concept - Centralized Data Clearing House (CCH)

The concept of ACDC is to provide one central database with open interfaces, allowing a wide range of external sensors getting connected to it. This connection can be either established directly or through so-called concentrators. Concentrators for example can be used, if an organisation or partner prefers to run the detection and analysis at his own environment, or if a special environment like STIX[1] is being used due to certain business requirements. The concept of ACDC also encourages mutual data sharing across different stakeholder groups. For this purpose, standardized formats have been defined to support the interaction of partners involved into detection, same as between those partners focussed on Support. This includes entities like Internet Service Providers or Critical Infrastructure Operators; National Support Centres have been integrated to support end-users. As an additional component of the infrastructure, a community portal has been developed to serve as a front end for the overall architecture. This community portal handles the access management, policy enforcements and user policies. Additionally, it also acts as a repository for knowledge gathered by the involved partners. One example for such knowledge is the display of statistics, metrics or emerging threat information on recent botnet activities or DDoS attacks, even in real-time.

The deliverable that describes the centralized clearing house is **D.1.2.1 Specification of Tool Group 'Centralized Data Clearing House'.**

The following graph shows the basic concept of the ACDC solution.



The CCH itself has been developed under the requirement to process large amounts of data in real-time and to store this big amount of data for further research purposes.

The database consists of two elements. The first component is a **Redis**[2] database, which only holds the dataset in the memory. It is used for real-time time data, real-time analytics and real-time communication. This solution has been chosen, as it allows processing the high volume of data that

[1] *https://**stix**.mitre.org*

[2] http://redis.io

[2] http://redis.io

[3] https://www.otrs.com

[4] http://en.wikipedia.org/wiki/ISO/IEC_27000

[5] https://www.trusted-introducer.org

has been estimated in the project. The **Redis** database gets supported by a **Cassandra** database, which stores the data that is necessary to run long-term measurement, providing statistics, or storage for possible law enforcement cooperation like the assistance in botnet takedowns.

Both databases are connected to each other. Each of the two databases has initially been setup as a cluster with two nodes and furthermore scalable to many additional nodes. The concept of **Cassandra** is to be spread over multiple data centers and sites and the data is replicated between all nodes. Additionally we are using the internal backup utilities of Cassandra as part of the back-up policy.

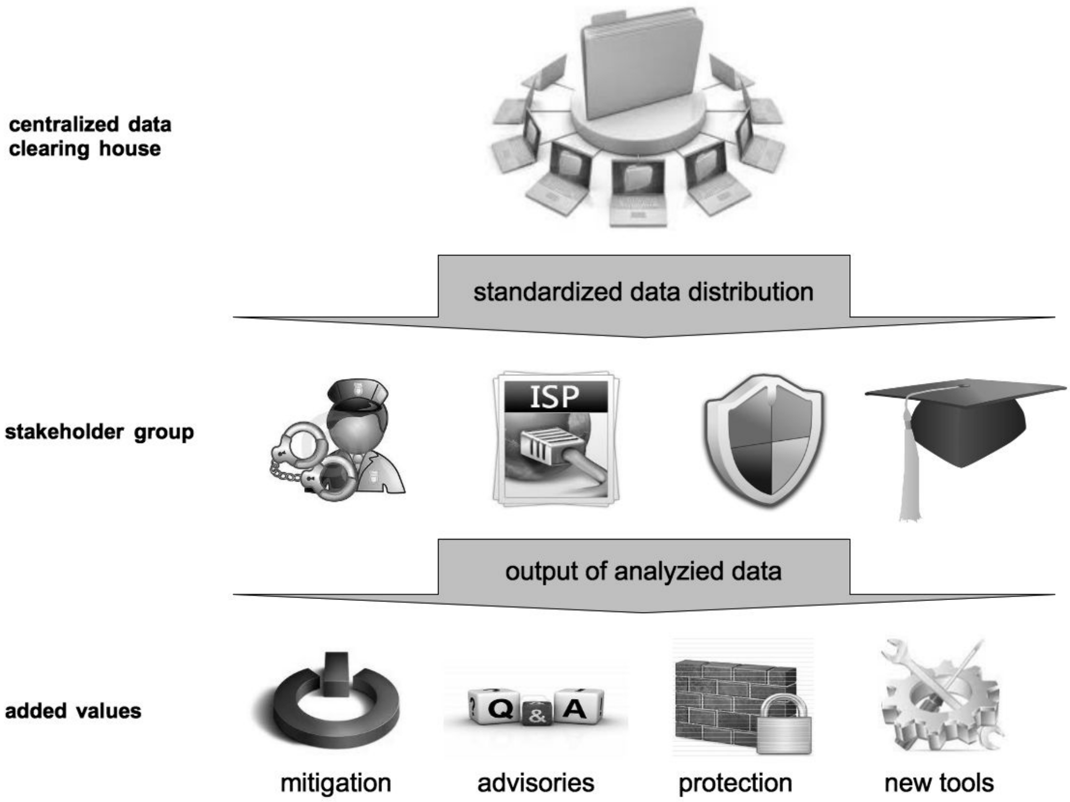
Another major requirement for this central data storage entity is a high security standard and architecture. Unrestricted access to such a massive data repository might be a big challenge for hackers or even government agencies from third countries.

The access management is handled through the community portal, but enforced by the CCH, whereby it has been specified that each device connected to the CCH requires an own **API-Key**. This centralized concept has been also introduced to cover possible disturbances through corrupted data, abuse attempts or other failures.

The detailed security concept of the CCH is described in the associated deliverable **D1.2.1**, and the concept of the overall security concept is been described within an own chapter in this document.

Besides collecting data, the CCH also distributes data to different partners and stakeholders. Each partner has own requirements for data reporting. An ISP for instance needs to be informed about compromised domains or IPs in his ASN, while research facilities only need to receive statistical data, Law enforcement might get need dashboard on the threat landscape, Anti-Virus companies to retrieve Malware samples or infected files etc. For this purpose, common standard output formats have been defined. These formats and definitions have been addressed and defined in the **Deliverable D1.7.1 – Data Format Specification.**

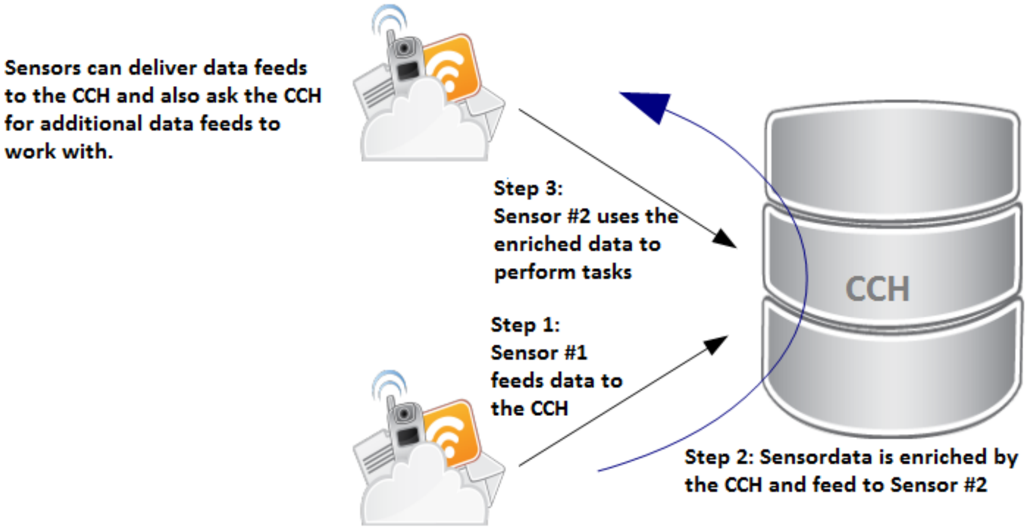
The following graph shows an abstract how the multi-channel data distribution has been applied into the overall software concept of ACDC.



4 Tools and Sensors

The ACDC software framework will be supported by collections of tools contributed by ACDC partners. Each tool will be required to collect and store data internally to support the analysis, detection and reporting goals required by the functionality provided.

A key component for the detection of botnets and other malicious activities are external sensors. These can be installed on end-user devices like a smartphone, on a corporate firewall, a honeypot, a website or internet server, a third party data feed or even in the internet of things, like a car or a fridge. Each of these devices is required to register with its own API-Key, allowing it to deliver data or to retrieve data from the CCH. The only exception for the distribution of individual API-Keys refers to sensors installed on end-user devices. These need to be routed through a middleware/concentrator to avoid any leakage of any API-Key on the Internet.


Sensors can deliver data feeds to the CCH and also ask the CCH for additional data feeds to work with.
Step 3: Sensor #2 uses the enriched data to perform tasks
CCH
Step 1: Sensor #1 feeds data to the CCH
Step 2: Sensordata is enriched by the CCH and feed to Sensor #2

4.1 End Customer Tools

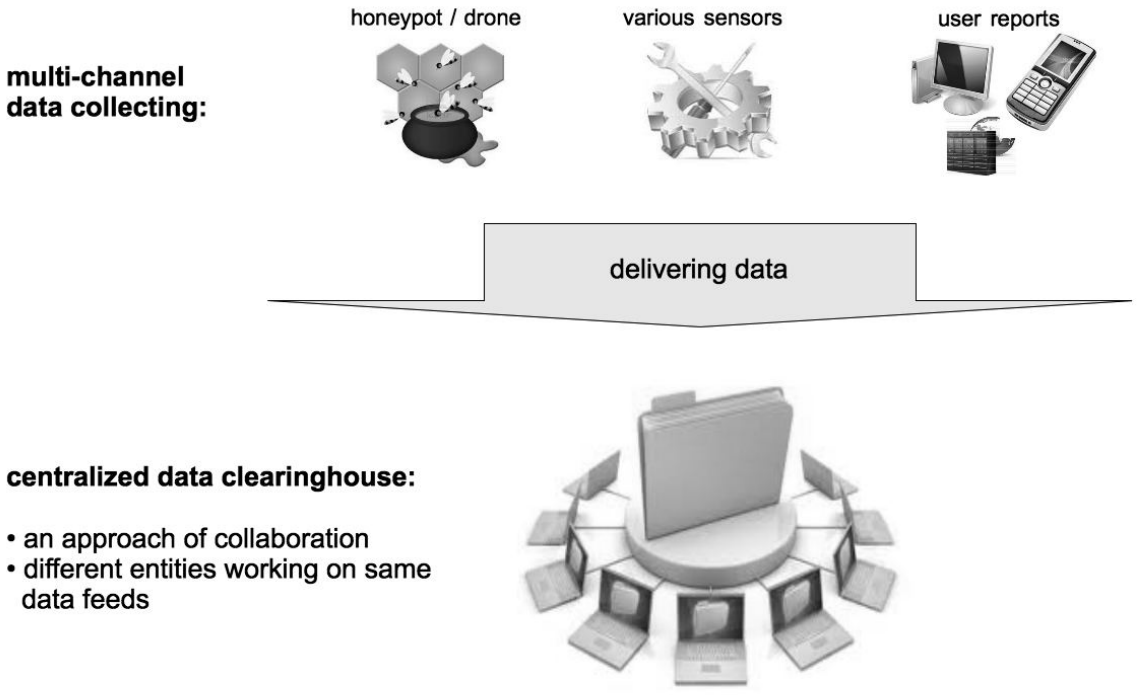
The specifications for end-user reporting tools have been addressed in the deliverable **D1.6.1 End Customers Reporting Tools Requirements.**

This document outlines the special requirements for tools like browser plugins, allowing users to report malicious websites or emails plugins to report Phishing or Spam emails. The document includes the specifications for type of data that is relevant for research or detection purposes, under consideration of privacy requirements. The document also addresses the specification for existing tools that might need an adaption for ACDC, same as recommendations for the usage new developed tools.

The deliverable also covers the risks associated to erroneous submissions, e.g. of legitimate emails instead of Spam. Additionally to the defined criteria, the CCH will only accept submissions from end-users, if they get routed through a middleware/concentrator. This has been specified due to the risk of getting an API-Key from an end-user tool leaked in the Internet.

The legal aspects of personal data in regards of privacy are being addressed in the first iteration of Deliverable **D1.8.1 – Legal Requirements**

The following graph shows an abstract, how the multi-channel data collecting from different sources will be implemented into the CCH.


multi-channel data collecting:
honeypot / drone
various sensors
user reports
delivering data
centralized data clearinghouse:
• an approach of collaboration
• different entities working on same data feeds

4.2 Tools for Malicious or Vulnerable Websites analysis

As further described in the deliverable **D1.2.1 "Tool Group Centralized Data Clearing House",** the CCH has no own intelligence to analyse botnets, malware or any other security related events. External analytical tools will provide the actual detection of these cyber-crime related events.

The set of analytical tools include Malware scanners from the Anti-Virus-Industry, behaviour detectors used by e.g. Internet Service Providers as part of their internal infrastructure, the intelligence of pattern matching or heuristics, web reputation analytics, blacklists and many more. An overview and classification of these tools is included in deliverable **D2.3 Technology Development Framework outlining basic models for integration and delivery principles.**

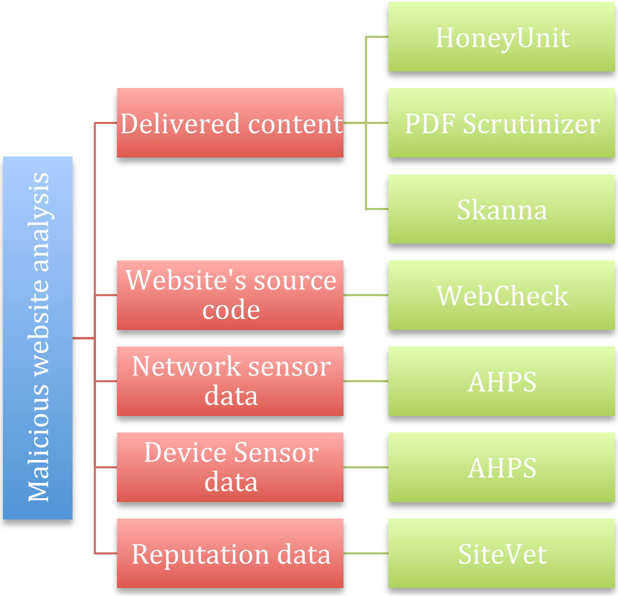
The specification and requirements for tools with the purpose to detect malicious or vulnerable websites are covered within the deliverables **D1.4.2 / D1.4.2 Specification of Tool Group "Malicious or Vulnerable Websites.**

The development of effective tools to detect malicious or vulnerable websites is a massive challenge, as the malware authors and cyber criminals also continuously develop new malware, trojans or add exploits to web browsers that infect computers or mobile devices. Web servers distribute their malware and use or replicate the HTTP protocol for their botnet's command and control.

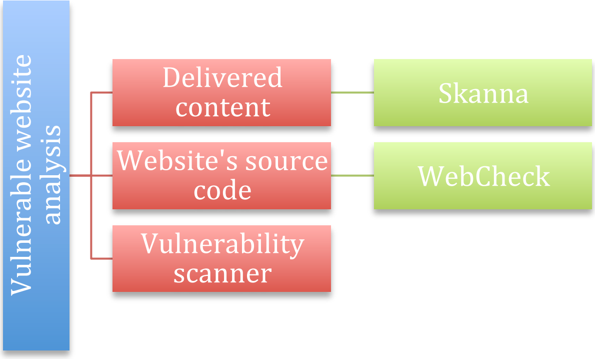
The versatility of potential modifications of malware further complicates a fast and reliable detection of compromised websites. As malicious website and vulnerabilities like zero-day exploits often come along in symbiosis, ACDC has taken the challenge to approach to combine the research and mitigation here.

Several ACDC partners have been active in the detection of malicious or vulnerable websites for many years and also own and use a lot of existing tools. The deliverable **D1.4.2** specifies the different requirements for the big portfolio of tools, ranging from source code analysis, web reputation scores, plugin monitoring, device sensors or vulnerability scanners.

These following two charts are part of **D1.4.2** and it gives a brief overview to the tools contributed to the ACDC Malicious or Vulnerable Website Analysis Tool Group.



Tools that are used for malicious website analysis.



Tools that are used for vulnerable website analysis.

The legal aspects of personal data in regards of privacy and the analysis tools of this chapter are being addressed in the first iteration of Deliverable **D1.8.1 – Legal Requirements**.

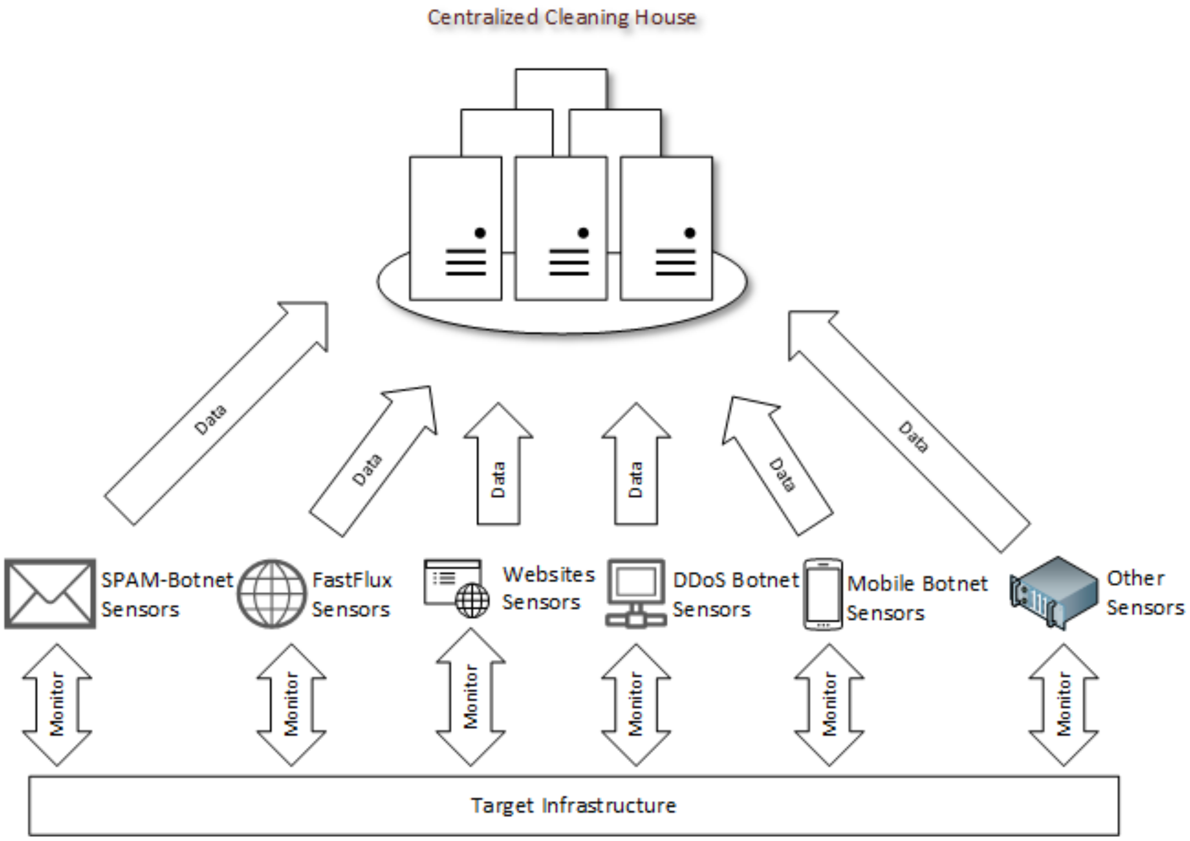
4.3 Network Traffic Sensors

Another important factor for the detection of botnets is the deployment of sensors for monitoring network traffic. The specifications for these sensors are described and defined in deliverable **D1.5.1 Network Traffic Sensors.**

Additionally to the sensors for end-users tools or on websites and webservers, the Network Traffic Sensors are the components within ACDC responsible for detecting infected systems. The network traffic sensors will contribute to the detection of Spam Botnets, Fast-Flux Botnets, Malicious and Vulnerable Websites, Distributed Denial of Service Botnets and Mobile Botnets. The detection of these threats will also be proved through the experiments that have been defined within the third work package.

Deliverables addressing the experiments are **D3.1 Planning reports of the experiments & D3.2 Design report of experiments.** Both documents also include an overview on the particular tools, software and hardware that has been utilized to run the five experiments defined in the project plan.

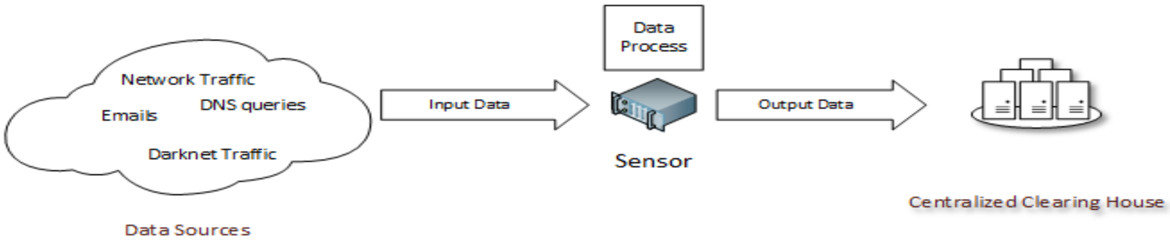
The following graph from deliverable **D1.5 Network Traffic Sensors** illustrates the interaction of the Network Traffic Sensors on the General Architecture of the ACDC from a functional perspective.



The sensors continually monitor and analyse the data flowing on the target infrastructure of the members that choose to participate in ACDC with their detection tools, in order to analyse and detect any signs of infection or bot related activity and report them to the Centralized Clearing House.

The target infrastructure is the set of networks, systems or information, belonging to each of the participating members, that contain information to be processed by the Sensors, such as email messages, network traffic data, etc. This is the primary source of information for the Network Traffic Sensors.

The following graph shows the overall sensor data flow to the CCH:



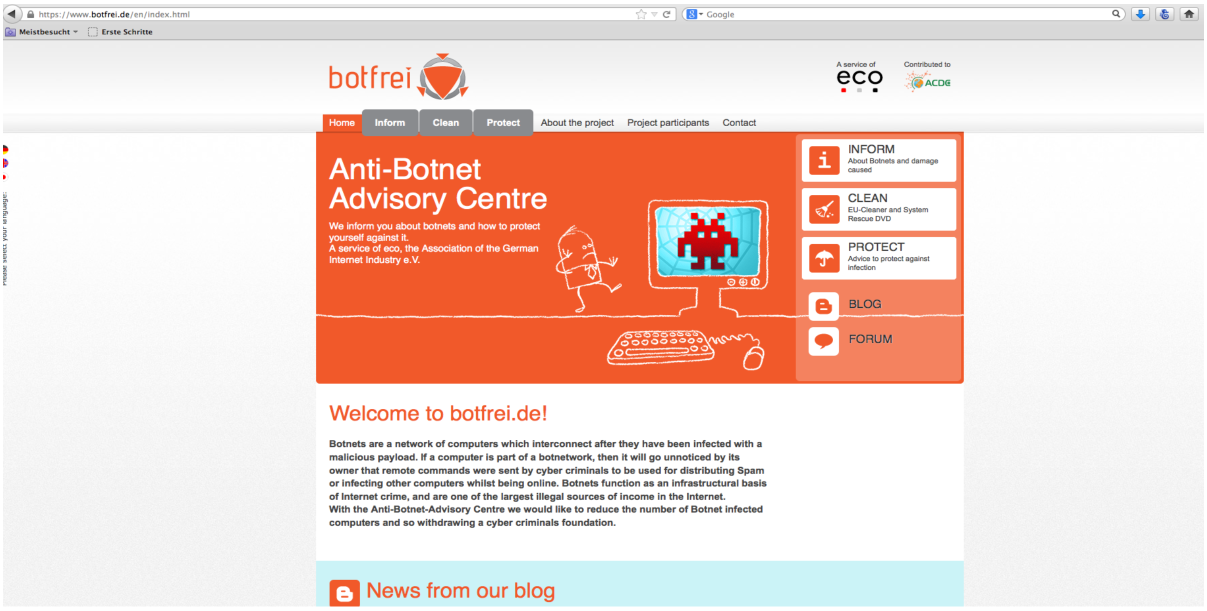
The deliverable also specifies the requirements for data input and output of the sensors connected to the CCH, same as it covers security specification along with privacy issues.

Additional data flow charts have been included to address the data flow of the particular sensors on detecting the data relevant to the five experiments and additional network sensors provided by the partners. Their specification and further information is included in the Sota catalogue, which is included as an Annex in deliverable **D2.3 Technology Development Framework outlining basic models for integration and delivery principles**.

4.4 Dissemination Tools for End-Users

4.4.1 Support Centres

National Anti-Botnet Support Centres are considered as a dissemination tool within the ACDC project. The project itself has the goal to provide eight national support centres and a central landing page called botfree.eu. The deliverable **D1.3.1 Tool group Support Centres** specifies the criteria defined for the National Anti-Botnet Support Centres. The document D1.3.1 defines the requirements for the operation of such a NSC, ranging from a basic website to a premium service with phone support, online chat, email support, a ticket system like OTRS[3] and other free tools and services.



Anti-Botnet Advisory Centre

We inform you about botnets and how to protect yourself against it.
A service of eco, the Association of the German Internet Industry e.V.

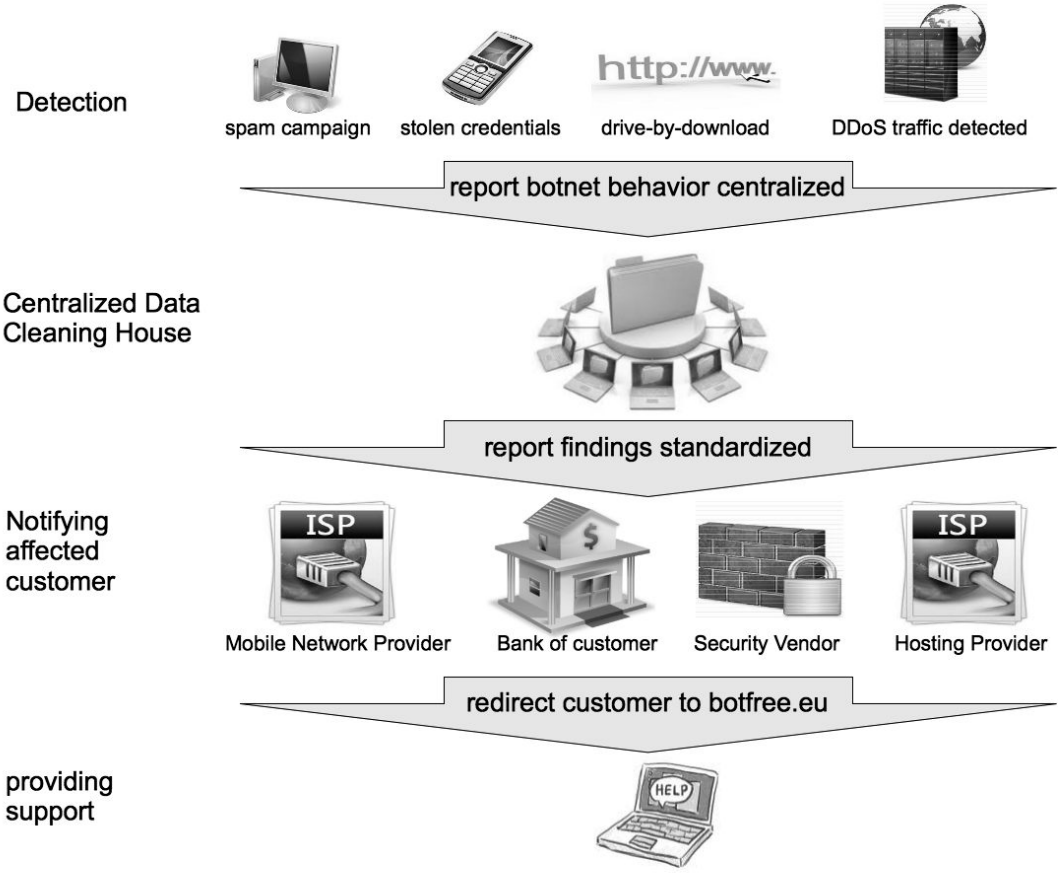
Welcome to botfrei.de!

Botnets are a network of computers which interconnect after they have been infected with a malicious payload. If a computer is part of a botnetwork, then it will go unnoticed by its owner that remote commands were sent by cyber criminals to be used for distributing Spam or infecting other computers whilst being online. Botnets function as an infrastructural basis of Internet crime, and are one of the largest illegal sources of income in the Internet.
With the Anti-Botnet-Advisory Centre we would like to reduce the number of Botnet infected computers and so withdrawing a cyber criminals foundation.

News from our blog

The following chart illustrates the workflow between the detection in the CCH and the NSC. ACDC or CCH do not contact an end-user directly, as personal data will not be stored in the database due to the legal constraints and national, same as European privacy standards. For example, only an ISP can make associations to an infected device and the impacted end-user. ACDC offers him the solution to point his customer to a national Anti-Botnet support centre.

[3] https://www.otrs.com



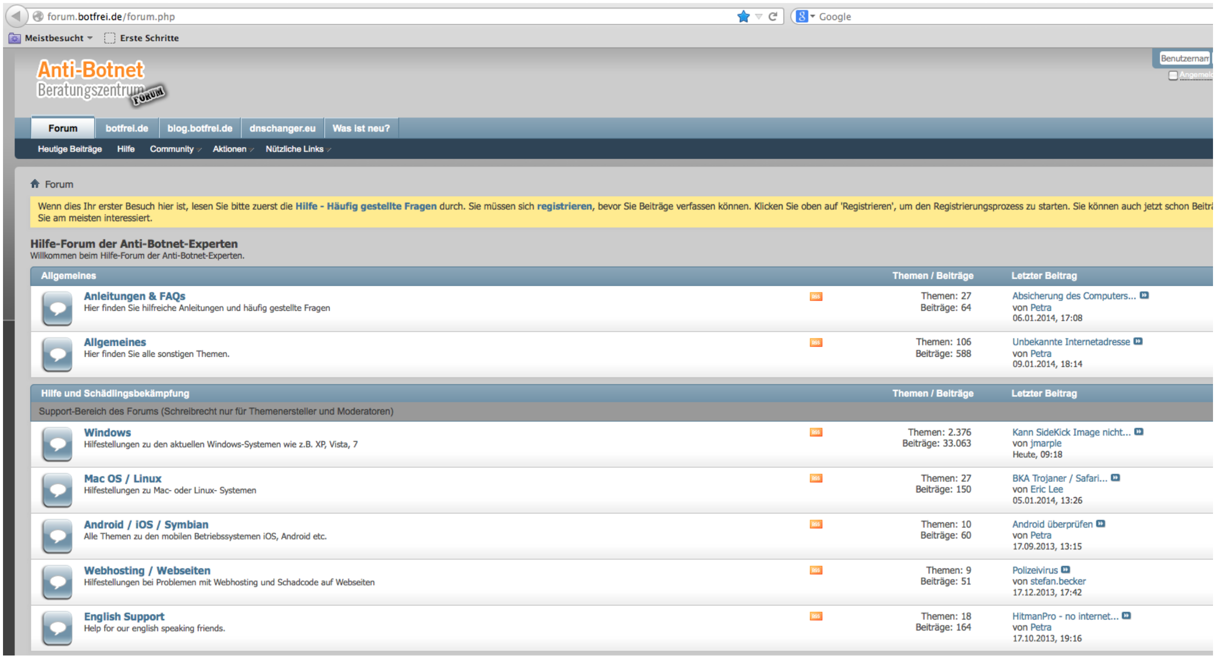
4.4.2 EU-Cleaners

Based on the requirements defined in **D1.3.1 Tool group Support Centres**, free dissemination tools should be distributed to end-users. ACDC has build two partnerships with industry partners, providing such removal tools for download at the national support centres. These two tools, Avira EU-Cleaner and Hitman.Pro EU-Cleaner have been initially provided to the German Anti-Botnet Support Centre botfrei.de and have now been made available to the National Support Centres under the umbrella of ACDC. The current specifications for dissemination tools within ACDC only specify the cost free availability of such a tool. Detailed requirements for the provision of tools within the support centres will be defined at the end of the project in **D1.3.2**. The outcome will be based on the exploitation and Sustainability Action plan for ACDC **(D5.2.1: Exploitation Plan / D5.2.2: Sustainability Action Plan***)*

Further information about these tools can be found on https://www.botfrei.de/en/eucleaner.html. The tools are also part of the Sota Catalogue in the Annex of deliverable **D2.3**

4.4.3 Support Forum

ACDC plans to provide support forums as part of the national anti-botnet support centres. The specifications for such a forum are part of deliverable **D1.3.1 Tool group Support Centres**. Right now, only the German Support Centre botfrei.de has an active support forum at http://forum.botfrei.de ACDC intends to establish a pan-European, multilingual forum at the central support page botfree.eu at the end of the project.



Wenn dies Ihr erster Besuch hier ist, lesen Sie bitte zuerst die **Hilfe - Häufig gestellte Fragen** durch. Sie müssen sich **registrieren**, bevor Sie Beiträge verfassen können. Klicken Sie oben auf 'Registrieren', um den Registrierungsprozess zu starten. Sie können auch jetzt schon Beitr
Sie am meisten interessiert.

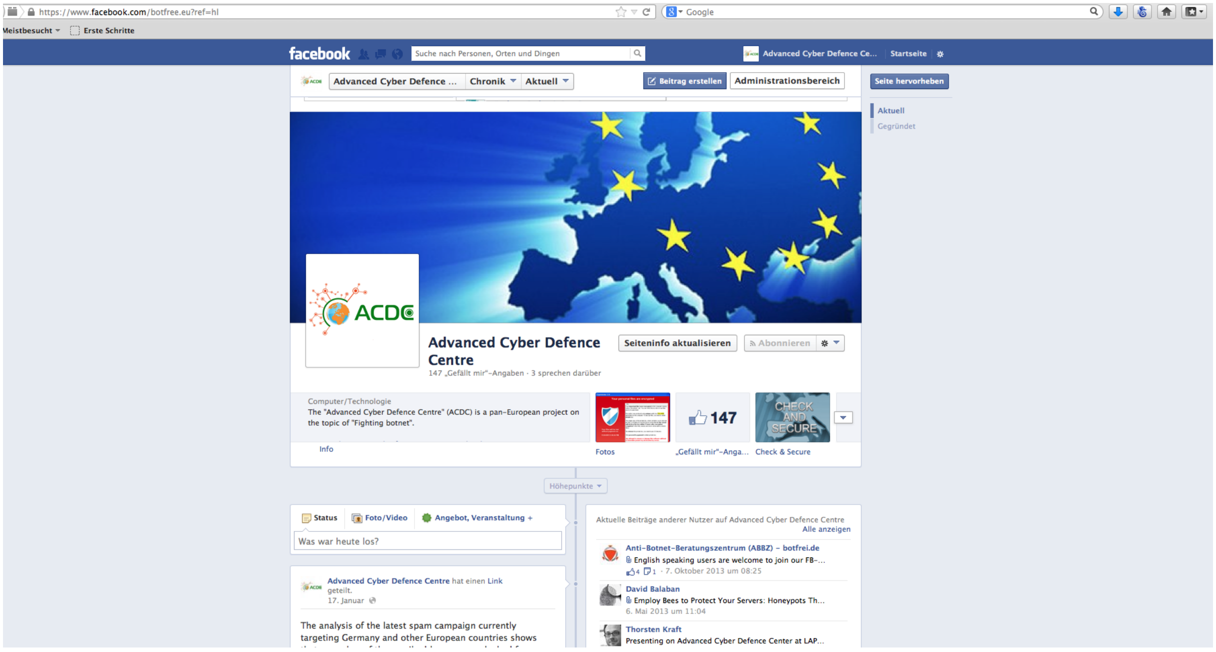
Hilfe-Forum der Anti-Botnet-Experten
Willkommen beim Hilfe-Forum der Anti-Botnet-Experten.

Allgemeines	Themen / Beiträge	Letzter Beitrag
Anleitungen & FAQs Hier finden Sie hilfreiche Anleitungen und häufig gestellte Fragen	Themen: 27 Beiträge: 64	Absicherung des Computers... von Petra 06.01.2014, 17:08
Allgemeines Hier finden Sie alle sonstigen Themen.	Themen: 106 Beiträge: 588	Unbekannte Internetadresse von Petra 09.01.2014, 18:14

Hilfe und Schädlingsbekämpfung	Themen / Beiträge	Letzter Beitrag
Support-Bereich des Forums (Schreibrecht nur für Themenersteller und Moderatoren)		
Windows Hilfestellungen zu den aktuellen Windows-Systemen wie z.B. XP, Vista, 7	Themen: 2.376 Beiträge: 33.063	Kann SideKick Image nicht... von jmarple Heute, 09:18
Mac OS / Linux Hilfestellungen zu Mac- oder Linux- Systemen	Themen: 27 Beiträge: 150	BKA Trojaner / Safari... von Eric Lee 05.01.2014, 13:26
Android / iOS / Symbian Alle Themen zu den mobilen Betriebssystemen iOS, Android etc.	Themen: 10 Beiträge: 60	Android überprüfen von Petra 17.09.2013, 13:15
Webhosting / Webseiten Hilfestellungen bei Problemen mit Webhosting und Schadcode auf Webseiten	Themen: 9 Beiträge: 51	Polizeivirus von stefan.becker 17.12.2013, 17:42
English Support Help for our english speaking friends.	Themen: 18 Beiträge: 164	HitmanPro - no internet... von Petra 17.10.2013, 19:16

4.4.4 Social Media

As part of the dissemination strategy, ACDC will use Social Media as a tool for dissemination. Currently the activity in social media focuses on Twitter (@antibot), but the activities also include a presence on Facebook and Google+ and a security blog. The concept and strategy is part of the social media strategy in deliverable **D6.2.2: ACDC Social Analytics Tool, Online Tools**



Advanced Cyber Defence Centre
147 „Gefällt mir"-Angaben · 3 sprechen darüber

Computer/Technologie
The "Advanced Cyber Defence Centre" (ACDC) is a pan-European project on the topic of "Fighting botnet".

Advanced Cyber Defence Centre hat einen Link geteilt.
17. Januar

The analysis of the latest spam campaign currently targeting Germany and other European countries shows

Aktuelle Beiträge anderer Nutzer auf Advanced Cyber Defence Centre

Anti-Botnet-Beratungszentrum (ABBZ) – botfrei.de
English speaking users are welcome to join our FB-...
4 1 · 7. Oktober 2013 um 08:25

David Balaban
Employ Bees to Protect Your Servers: Honeypots Th...
6. Mai 2013 um 11:04

Thorsten Kraft
Presenting on Advanced Cyber Defence Center at LAP...

The final outcome of the services and a description of tools that have been utilized as part of the Social Media activities, including content management systems, tracking tools, social media accounts etc., will be part of the final iteration of the **Overall Software Architecture (D1.1.2)**

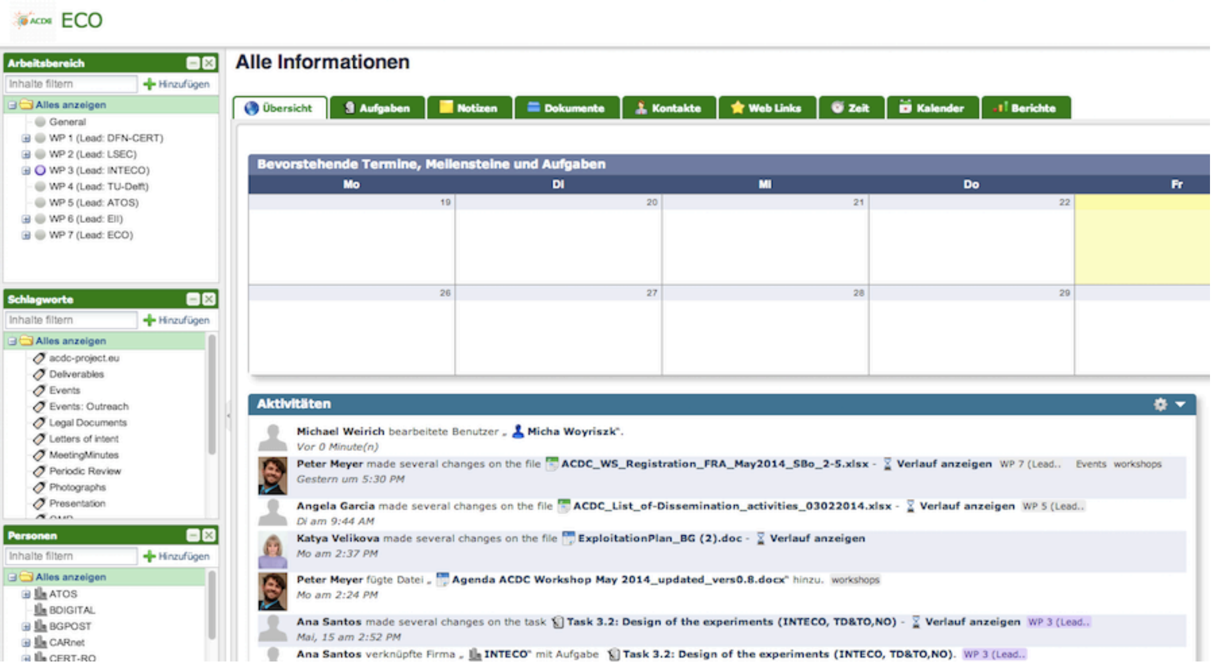
4.5 Project-Internal Tools

4.5.1 Community Portal

A set of collaborative tools has been provided to the project partners to facilitate the cooperation within the project and to assist in the coordination work.

The description and requirements have been described in the deliverable “**D7.1 Project internal IT communication infrastructure”.** ACDC has chosen the open source tool Feng Office. Further information on this software tool can be retrieved from http://www.fengoffice.com/web/wiki/doku.php

The login is password protected and accessible via: https://workspace.acdc-project.eu (SSL secured). The project coordinator ECO handles the administration and user management.



Michael Weirich bearbeitete Benutzer „ **Micha Woyriszk**“.
Vor 0 Minute(n)

Peter Meyer made several changes on the file **ACDC_WS_Registration_FRA_May2014_SBo_2-5.xlsx** - **Verlauf anzeigen** WP 7 (Lead.. Events workshops
Gestern um 5:30 PM

Angela Garcia made several changes on the file **ACDC_List_of-Dissemination_activities_03022014.xlsx** - **Verlauf anzeigen** WP 5 (Lead..
Di am 9:44 AM

Katya Velikova made several changes on the file **ExploitationPlan_BG (2).doc** - **Verlauf anzeigen**
Mo am 2:37 PM

Peter Meyer fügte Datei „ **Agenda ACDC Workshop May 2014_updated_vers0.8.docx**“ hinzu. workshops
Mo am 2:24 PM

Ana Santos made several changes on the task **Task 3.2: Design of the experiments (INTECO, TD&TO,NO)** - **Verlauf anzeigen** WP 3 (Lead..
Mai, 15 am 2:52 PM

Ana Santos verknüpfte Firma „ **INTECO**“ mit Aufgabe **Task 3.2: Design of the experiments (INTECO, TD&TO,NO).** WP 3 (Lead..

ACDC Workspace - Feng

4.5.2 Mailing Lists

A part of the project internal IT communication infrastructure as described in deliverable **D7.1**, a mailing server has been provided to the project partners. The co-coordinator Technikon administrates the policy, mailing lists and the infrastructure of the mail server. Dedicated mailing lists for the specific work packages, task-groups or participants of particular experiments have been established, aside of special mailing lists for administration or financial stakeholders.

5 General Security Requirements for ACDC tools

In this section we approach the security requirements from the global perspective of a system that may become an ACDC tool and under the light of relevant laws, standards and best current practices.

Since ACDC is developing components that are integrated into real environments, all ACDC subsystems should feature a number of general functions and protection schemes to prevent structural security failures. Within such set of properties, especial attention deserves the distributed nature of most of the tools to be developed by ACDC (e.g. network sensors, end-customer tools, etc.) and, in some cases, the fact that ACDC software/hardware may be connected to the public Internet (e.g. crime detection agents). Therefore, we shall try to define general security requirements that rely on the set of security aspects identified by ISO/IEC 27000[4].

[4] http://en.wikipedia.org/wiki/ISO/IEC_27000

In particular we define the security architecture for systems providing end-to-end secure communications, and introduces different security dimensions of a communication system.

Each ACDC component must have built-in mechanisms to address the requirements established for each of the described dimensions. The general requirements for each dimension are described in the following paragraphs.

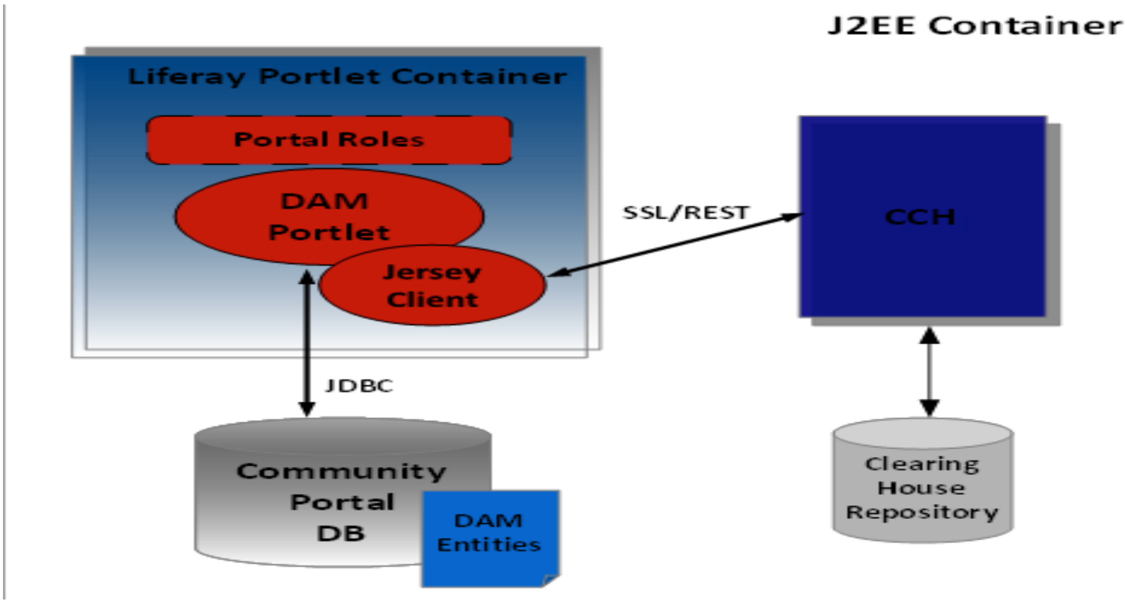
5.1 Access Control (Authorization)

The ability to control the level of access that individuals or entities have, to both network and information systems, must be properly defined by system managers. This strongly depends on the types of users that ACDC defines, the respective access capabilities for each user group, and the confidentiality levels established for each piece of information. There must be appropriate mechanism to enforce such access control (e.g. firewalls, file systems permissions, secure log-in) including physical control of access. Furthermore the system must have a mechanism to fully trace and record the actions and the information accessed by each user at all times. Each ACDC component must have built-in access control mechanisms which interaction with them is possible.

A single authorization check can grant access to all the functionalities of an application or system (i.e. login). However access control has a broader definition and can be applied before accessing to each resource of a system. In particular, a good mechanism to avoid cases of abuse is to clearly define what the usage limits of an application are. In this case a proper authorization scheme is to define the allowed queries to the database instead of granting full access to a database containing personal data.

5.2 Authentication

Authentication must guarantee that the system being accessed is the intended one and that the user is who claims to be. The authentication mechanism in ACDC should combine the use of a solid state-of-the-art Identity Management System (IdMS), including a verification process to approve an applicant. For this reason Trusted Introducer (TI)[5] and the Community Portal to centralize the authentication is very useful in this context. Therefore ACDC components must be prepared to work in this type of IdMS environment and the whole ACDC platform must be supported by an IdMS.



Sample of the idMS implementation in the community portal.

[5] https://www.trusted-introducer.org

5.3 Non-Reputation

Due to the value of the digital data managed by ACDC tools, the capability to prevent system users from denying that data files were accessed, altered or deleted, might be useful for specific ACDC tools and sensors to enable highly-secure logging and auditing processes.

5.4 Data Confidentiality

The protection of information from unauthorized disclosure shall be made by restricting per-user-group access to every type of information dealt with and by encrypting the information at least on transmission and possibly on storage. Both should be compulsory requirements in ACDC.

5.5 Communication Security

To ensure that communication only flows from a source to the intended destination, all communication must be made with encrypted sessions (e.g. TLS/SSL[6], SSH). In order to avoid man-in-the-middle attacks, the aforementioned technologies must support and employ mutual authentication by means of certificates or pre-shared keys.

5.6 Data Integrity

The ability to protect data from unauthorized, uncontrolled, or accidental alteration during storage or transmission is another essential feature. In order to guarantee the chain of custody, all ACDC tools and sensors that may gather or store electronic evidences must implement mechanisms to guarantee that this data has not been altered by any system user or any other third party. In the case of processed information to be employed as evidence, both raw data and processed information must be protected from tampering.

5.7 Efficiency

Efficiency is one of the requirements, which are connected with security. It is defined as a relationship between the results achieved and how well the resources have been used. It means that the aim to be achieved by the secure system also depends on the kind and quality of used methods and services. During the design process of ACDC tools (security solutions and requirements directly connected with security) this requirements should be taken into account.

5.8 Reliability

Reliability is defined as the ability of a system to perform its functions for a period of time. The reliability of the system is one of the high-level requirements. It means that it consist of a few different requirements (i.e. availability and communication security). It is a good point to start a design process and it can be a source of another, more specific requirements. This is obvious that the ACDC tools should meet this requirement connected with security.

5.9 Availability

The development of protection or back-up mechanisms for network/software/hardware is also a desirable property of any IT system, as well as to defend from Denial of Service (DoS) attacks. This falls out of the scope of the ACDC work plan, but provisions can be made in all the deliverables that describe implementations on how the subsystem can be protected to increase its availability.

5.10 Privacy

Privacy may be defined as an entity‘s ability to control how, when, and to what extent personal information about it is communicated to others. In order to support privacy it is important to understand what personal information is and to be aware of the ways that personal information can be controlled and processed. Privacy and legality of ACDC is handled in Deliverable **D1.8.1 Legal Requirements** and on an on-going-review process. The technical requirements in this dimension are simply: to implement whatever is required to fulfil all the privacy requirements.

[6] http://en.wikipedia.org/wiki/TLS/SSL

6 Overall Legal Concept

This overall legal concept has been integrated into the legal work and has been addressed in deliverable **D1.8.1 Legal Requirements.** Conclusions and recommendations from this and the general legal requirements have been incorporated into all ACDC-related tasks, developments and deliverables.

In order to cope with sensitive issue related to privacy and data protection, ACDC partners shall follow the following guidelines:

Whenever personal data is processed, various legal bases must be complied with. In addition to European directives, the national law of Germany must be followed as well.

The CCH as the central storage facility of the ACDC project collects and transfers IP addresses (static and dynamic) and domains to stakeholders of the entire project. In the following, the resulting legal problems are discussed.

6.1 Dynamic IP addresses and personal data

Whether dynamic IP addresses can qualify, as personal data is disputable, because a clear assignment is not possible, unlike in the case of the static IP address. The starting point for the difference of opinion is the element of "determinability" according *Section 3 I Federal Data Protection Act.*[7] The assignment of a dynamic IP address through the Internet access provider is merely temporary. In this way, the anonymity of the Internet user is guaranteed. Even if the IP addresses can be identified by the server operator, a long-term association between the address and a name, which would result in the user becoming known, is not possible. From the IP address as such there exists no direct relationship to a particular person, so that this first needs to be ascertained.

As the access provider in their own right undertakes the allocation of IP addresses, and because it is relatively uncomplicated for the access provider to ascertain this relationship between an IP address and the person, the above-mentioned cases where other persons, such as the mailbox provider, collect and forward dynamic IP addresses, remain disputable.

6.1.1 Relativity of the Relationship to the Person

One argument/legal opinion deals with the relativity of the personal reference, and applies according to Section 3 I Federal Data Protection Act for the assessment of the determinability, based on whether the responsible party can ascertain the relationship to a natural person with the means normally available to them and without disproportionate effort. In particular, a differentiation is made on the basis of whether the de-anonymization is possible with proportionate effort. This should, however, only be possible for the access provider. A third party (here, the mailbox provider) is only able to identify the user behind the IP address with the help of the access provider, who, in turn, is legally not permitted to provide this information to third parties. The theoretical possibility of an identification of the user does not correspond to the aforementioned definition of determinability.

6.1.2 Objectivity of the Relationship to the Person

According to this argument/legal opinion, it is not relevant whether a disproportionate effort is required to de-anonymize the IP address. It is sufficient simply that the theoretical possibility of a link of any form exists between the email address and a natural person. This is regardless of that fact that the determinability of the person in the legal sense is only possible when the person is identified using legal means. In this argument, the Data Protection Act is specifically designed to protect against the misuse of data, meaning that such a limitation of the term determinability would not be justifiable. The objectivity of the relationship to the person is also supported by *recital 26 of the Data Protection Directive 95/46/EG.*[8] The Art. 29 Working Party also assume the absolute definition of the term. In *recital 26 of the EU Data Protection Directive 95/46/EG*, it is unambiguously defined that all means that could be used by the party responsible for the processing, or by any other party who could be reasonably considered, are to be taken into account in order to establish whether a person is determinable.

As it cannot be ruled out that third parties possess the additional knowledge required for the ascertainment of the relationship to the person, it depends in actuality on the judgment of the

[7] http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

[8] http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-The-Recitals-Page-1/90.htm

probability of a potential identification. Dynamic IP addresses can also be used by third parties, with the help of log files of the Internet Service Provider's (ISP) individual connections, leading potentially to the identification of the individual person. Therefore, it must be assumed that it is possible to ascertain the relationship to the person for dynamic IP addresses and that the data protection laws are applicable.

6.1.3 Interim Result:

In our opinion, there are better arguments for the objectivity of the relationship to the person. In any event, when in doubt, for the superordinate purpose of the protection against phishing and spam, it should be assumed that dynamic IP addresses represent personal data. As it cannot be ruled out that third parties possess the additional knowledge required to ascertain the relationship to the person, it comes down to a judgment of the actual potential of a possible identification.

6.1.4 Domains and other data

Domains are sequences of letters and characters that are associated with an IP address. Even domains can therefore have a personal reference, especially if e.g. contained the name of a natural person. Thus the relevance of the data protection law is in the affirmative

6.2 Legality of data processing

In Germany personal data processing is legal, if the prior consent of the data subject is granted or it is permitted by law.

6.2.1 Prior consent

According to *Section 4 of Federal Data Protection Act* [9] the collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented. Further, the collector of personal data must comply with *Section 4 a of Federal Data Protection*, in particular the Data subjects shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent.

6.2.2 Permission by law

According to *Section 28 (1) of Federal Data Protection Act* the collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible when needed to create, carry out or terminate a legal obligation or quasi-legal obligation with the data subject, in so far as this is necessary to safeguard justified interests of the controller of the filing system and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use, if the data are generally accessible or the controller of the filing system would be entitled to publish them, unless the data subject's legitimate interest in his data being excluded from processing or use clearly outweighs the justified interest of the controller of the filing system.

6.2.3 Justified interests:

The data processing is necessary within the meaning of based on the collection, storage and transmission of strange data, so data subjects can be informed and further investigation can be initiated.

Whether the legitimate interests of the person concerned predominate, must be examined in the context of a balance of interests. Here the informational self-determination must be considered, which results from *Article 1 und 2 of Basic Law for the Federal Republic of Germany (Grundgesetz, GG)*[10]. An argument against an overriding legitimate interest of the person concerned is that only conspicuous data will be stored.

Moreover, it is precisely in the interest of the person concerned, when he gets informed about the conspicuousness regarding his data. The person concerned may take further steps for investigation

[9] http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

[10] http://www.iuscomp.org/gla/statutes/GG.htm#1

and can take action to prevent further abuses its data. As far as the data processing serves the recognition and containment of data misuse and moreover, to avoid massive damage and major disruption to the telecommunications infrastructure, the collection and transmission of personal data is justified.

As a result, the data processing in accordance with the principles set out above is admissible. It is possible either to take action on the data subject's prior consent or a statutory basis.

6.3 Country data-protection authorities

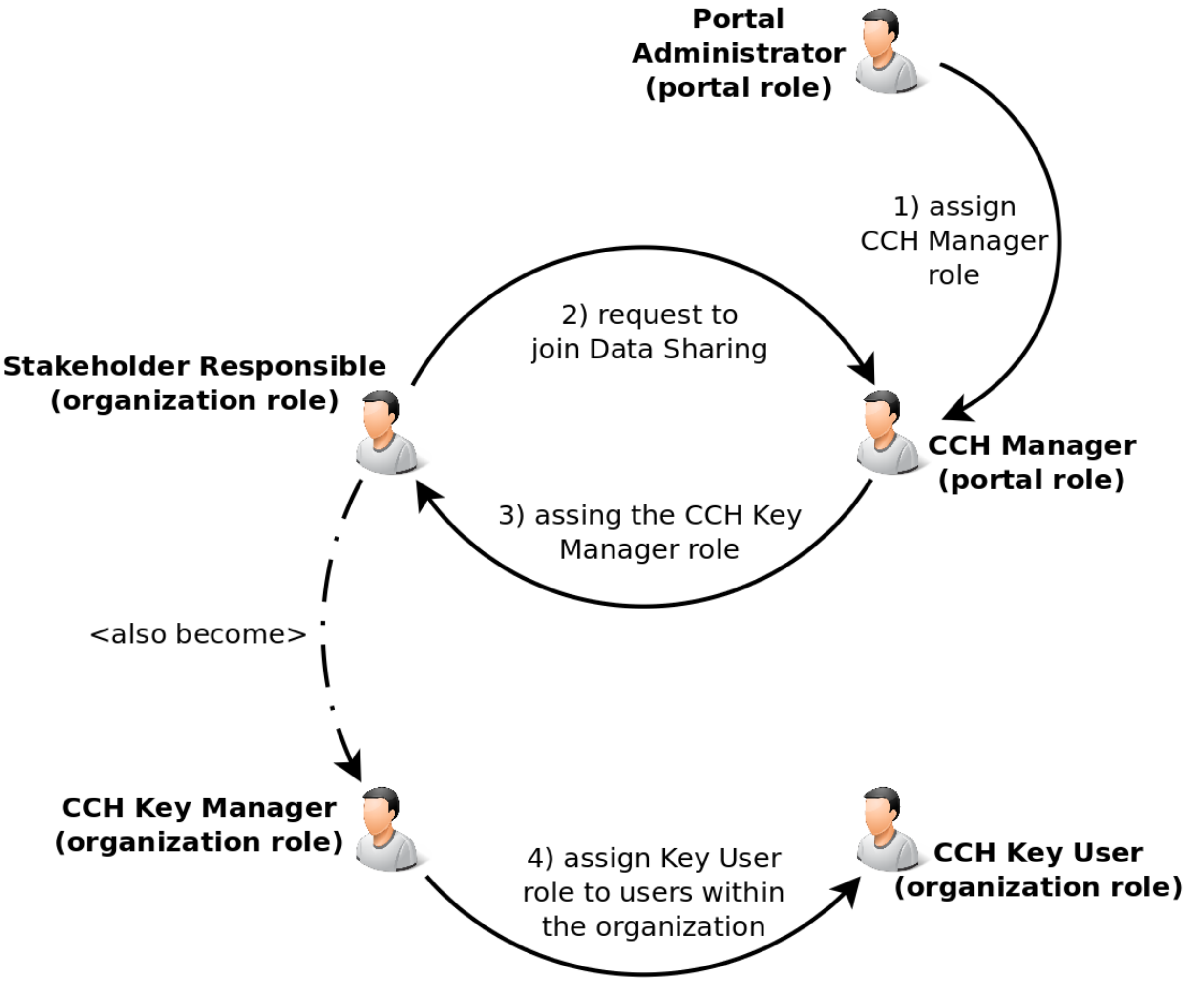
In the country of each ACDC partner, there is at least one data protection body responsible for dealing with issues that relate to privacy and data protection. Such authorities are competent with all national regulations and legislation in force. The data protection authorities need to be consulted by the ACDC tool providers to gather information about all country-specific issues connected to privacy and data protection.

7 Policy Management

This guidance provides the ACDC policy statement on data sharing and additional information on the implementation of this policy and we expect grantees to follow these rules to conduct the work described in the application for an API Key.

In ACDC's view, all data should be considered for data sharing. Data should be made as widely and freely available as possible while safeguarding the privacy aspects and protecting confidential and proprietary data. To facilitate data sharing and to enforce the before mentioned goal, ACDC operates a Centralized Clearing House (CCH), with respect to data sharing vary across countries.

The CCH as the core component is the logical entity or place that enforces policies for admission control and policy decisions in response to a request from a user wanting to access a resource shared across the ACDC platform and therefore defined as the Policy Decision Point (PDP). The PDP component in the CCH decides whether or not to authorize the user based on the description of the user's attributes.


Portal Administrator (portal role)
1) assign CCH Manager role
2) request to join Data Sharing
Stakeholder Responsible (organization role)
CCH Manager (portal role)
3) assing the CCH Key Manager role
<also become>
CCH Key Manager (organization role)
4) assign Key User role to users within the organization
CCH Key User (organization role)

Beyond basic authorization and authentication, the ACDC approach supports API subscription approval policies, sent to the CCH PDP to enforce these policies. How this works is described in deliverable covering the implementation of the Community Portal, **D6.2.1 ACDC Social Platform deployed, Online platform**