CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

indra

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

EUROPE *for business*

INTECO Instituto Nacional de Tecnologías de la Comunicación

Fondazione ICSA

Zanasi & Partners

CONTACT DATA

http://cloudcert.european-project.eu
info@cloudcert.european-project.eu
http://en.wikipedia.org/wiki/CloudCERT

RESULTS OF CLOUDCERT TESTBED FRAMEWORK TO EXERCISE CRITICAL INFRASTRUCTURE PROTECTION

Edit:
Instituto Nacional de Tecnologías de la Comunicación S.A.
INTECO
Avenida José Aguado, 41- 24005 León. Spain
+34 987 877 189
www.inteco.es

Edition 2013

Electronic version available at:
http://cloudcert.european-project.eu/

INDEX

1. BACKGROUND and MOTIVATION 4
   - 1.1. Programme overview 5
   - 1.2. Motivation 5
   - 1.3. Scope 5

2. PROJECT DESCRIPTION 7
   - 2.1. Participants 8
   - 2.2. Objectives 9
   - 2.3. Benefits 9
   - 2.4. Target Groups 9
   - 2.5. Project European dimension and roadmap 10

3. WORK PACKAGES 8
   - 3.1. Work Packages overview 14
   - 3.2. WP1. Project Management 15
   - 3.3. WP2. Platform design 16
   - 3.4. WP3. Information and communication standards 20
   - 3.5. WP4. Secure framework definition 23
   - 3.6. WP5. Platform development 26
   - 3.7. WP6. Pilot experimentation 28
   - 3.8. WP7. Dissemination of project results 31

4. TECHNOLOGICAL SOLUTION 34
   - 4.1. Collaborative Platform 35
   - 4.2. Content Lifecycle 37
   - 4.3. Vulnerabilities Lifecycle 38
   - 4.4. WikiCIP 39
   - 4.5. Forum 40
   - 4.6. Bulletins Service 41

BACKGROUND and MOTIVATION

PROGRAMME OVERVIEW

The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU.

2004 In order to counteract these potential vulnerabilities the European Council requested in 2004 the development of a European Programme for Critical Infrastructure Protection (EPCIP). Since then, a comprehensive preparatory work was undertaken, which included the organisation of relevant seminars, the publication of a Green Paper, discussions with both public and private stakeholders and the financing of a pilot project.

2006 With this in mind, on 12 December 2006, the Commission adopted the communication on a EPCIP, which set out an overall horizontal framework for critical infrastructure protection activities at EU level. The proposed EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" was adopted on 12 February 2007.

2008 Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection set up a procedure for identifying and designating European critical infrastructures (ECIs). At the same time, it provides a common approach for assessing these infrastructures, with a view to improving them to better protect the needs of citizens.

2009 Finally, on 30 March 2009, the Commission adopted the communication on Critical Information Infrastructure Protection (CIIP) [COM(2009) 149], which gives details of the main challenges facing critical information infrastructures and proposes an action plan aimed at increasing their protection.

HOME/2010/CIPS/AG/20

The EU Programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks aims to encourage an exchange of know-how and good practices between the various agents responsible for crisis management and to organise joint exercises to enhance coordination between the relevant departments.

The European Commission elaborates annual work programmes to cover the priorities within every year. These programs include calls for proposals to determine action grants to be awarded to transnational and/or national projects expected to contribute to the achievement of the general as well of the specific objectives of the programme

As a result of this programme 2010 call for proposals, this project “**CloudCERT**” has been selected as one of the awarded projects.

MOTIVATION

As stated in EPCIP, stakeholders must share information on Critical Infrastructure Protection(CIP), particularly on measures concerning the security of critical infrastructure and protected systems, interdependency studies and CIP related vulnerability, threat and risk assessments. At the same time, there must be assurance that shared information of a proprietary, sensitive or personal nature is not publicly disclosed and that any personnel handling classified information will have an appropriate level of security vetting by their Member State.

To solve this real need, CloudCERT project aims at providing this secure information sharing Testbed framework in order to exercise unified coordination using same communication protocol standards for improving visibility of common threat awareness, vulnerabilities, advisories and alerts specific to CIP.

In order to achieve this goal, an important work must be carried out based conceptual CSIRT communication modelling and architecture; definition of secure information sharing; information standards and protocol definition; design of the Testbed platform and implementation; and finally deploy a pilot to check reality based on use case scenarios.

The scope of this project is restricted to the creation of the pilot platform CloudCERT to exchange CIP information. Therefore only covers the first stage of the roadmap in the long term exposure.

The final platform is an operational pilot, with a community of users and information useful enough to test its functionality and to perform simulation exercises for CIP information exchange.

The platform allows the exchange of CIP operational measures, methodologies, experiences and know-how between users acting as a repository of information, including at least the following types of information:

- Vulnerabilities.
- Notes, Notices and Alerts.
- Threat awareness.
- News.
- CIP Best Practices.
- CIP Lessons Learned.

The CloudCERT platform is technically based in a web application with user management, including strong authentication and secure exchange of information according to interoperable standards.

PROJECT DESCRIPTION

PARTICIPANTS

COORDINATOR

- INTECO - National Institute for Communication Technologies.

CO-BENEFICIARIES

- CNPIC - National Centre for Critical Infrastructure Protection.
- Europe for business.
- Fondazione Intelligence Culture and Strategic Analysis (ICSA).
- Indra Systems, Inc.
- INTECO - National Institute of Communication Technologies.
- Zanasi & Partners.

USER PARTNERS

- INTECO - National Institute for Communication Technologies.
- CNPIC - National Centre for Critical Infrastructure Protection.

OBJECTIVES

- To supply a **Testbed framework** approach to integrate mechanisms for coordinating partnerships and stakeholder efforts to effectively exchange information related to CIP and their security aspects.
- To **secure EU infrastructure** improving understanding of the relationships among its elements and the link between risk management and infrastructure protection.
- To provide the capability needed to **eliminate potential vulnerabilities** in the critical infrastructure by sharing vulnerability information.
- To **manage security** as a whole using a unified process of information exchange to determine the risk and d ecide upon a nd implementing actions to reduce risk to a de fined and acceptable level, at an acceptable cost.
- To **obtain value** derived from its information exchange by exercise implementation, measured in the effectiveness of preventing, deterring, and responding to cyber attacks on control systems within critical infrastructure.
- A **common reporting** and **information exchanging** on the six phases of the CIP life cycle in order to create a comprehensive solution.

BENEFITS

The expected **short term** impact is to provide CIP bodies with a testbed platform designed to support the Member States' CIP information exchange, coordination and supervision.

In the **midterm** CloudCERT will enhance the cooperation through the platform implementation in a real production environment and it will contribute to the minimization of cooperation obstacles for CIP operators and protection authorities in different countries in Europe.

In the **long term**, it is expected to contribute to the establishment of a European Homeland Security environment for the protection of European CIs.

TARGET GROUPS

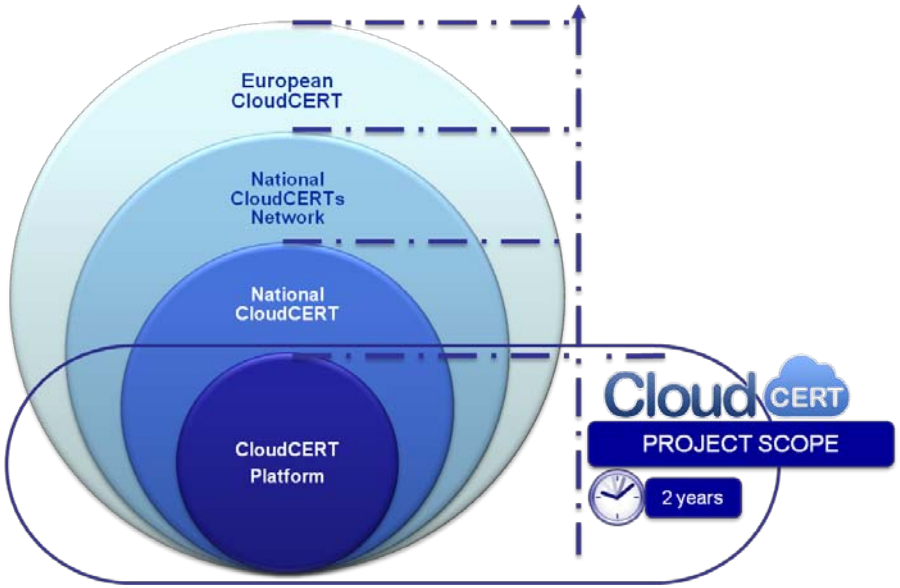
The main target groups and b eneficiaries of this project are:

- Member States through the authorities of Critical Infrastructure Protection.
- CERTs or CSIRTS competent in CIP.
- Operators or Owners of the Critical Infrastructure (CI).

CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

PROJECT EUROPEAN DIMENSION AND ROADMAP



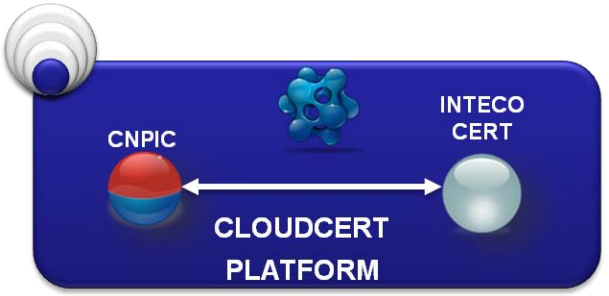
CloudCERT is a **transnational project**, which involves partners in at least two Member States.

The approach of the long-term project may be considered following a roadmap with the following stages:

- CloudCERT Platform.
- National CloudCERT.
- National CloudCERTs network.
- European CloudCERT.

To build a pan-European collaboration network, we propose a methodology based on successive incremental approaches, generating products in phases that will improve in each interaction. During the duration of the project (2 years) only the **pilot platform** is created with the goal in mind to build a National CloudCERT.

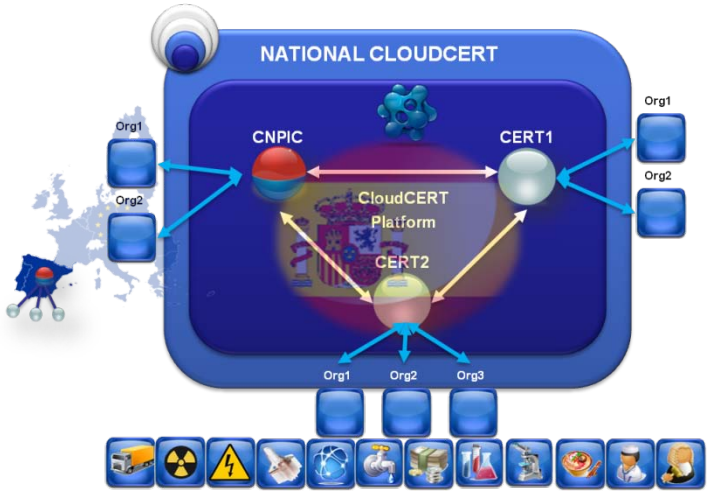
PHASE 1 - CLOUDCERT PILOT (CURRENTLY GRANTED BY EU)



In this first roadmap phase, the goal is the creation of the pilot platform to add as users of the platform, CIP actors within a country.

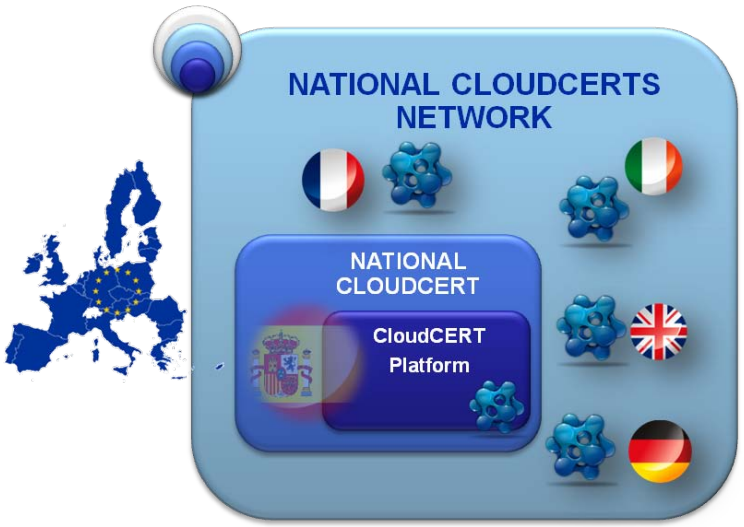
Due to project limitations, users of this platform will be the CERTS participants in the project (INTECO-CERT) as well as the participating National PIC Centres (CNPIC).

PHASE 2 - NATIONAL CLOUDCERT (OPPORTUNITY)



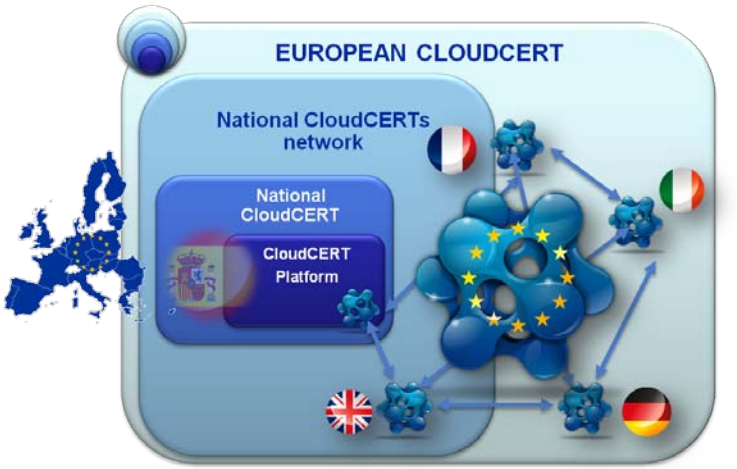
Once released the pilot, would lead to the exploitation phase of the platform. This phase can begin with the deployment of the platform in a real production environment with the aim of establishing a National CloudCERT that integrates the National CIP Center as well as major CERTS with CIP capabilities and other possible actors of interest and relevance.

PHASE 3 - CLOUDCERTS NODES (OPPORTUNITY)



The next roadmap stage could be t he replication without difficulty in other member countries to create national CloudCERT nodes. Differences in the regulatory framework of each country can condition the information exchange to take place. It would be desirable to add minor qualifications or conditions to modify the platform but not to dramatically change or alter its main purpose.

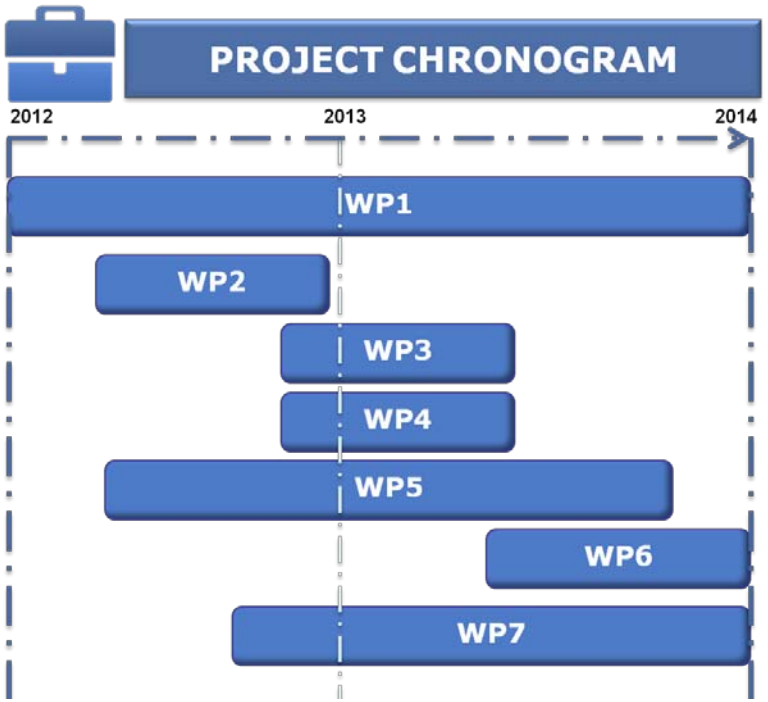
PHASE 4 - EUROPEAN CLOUDCERT (OPPORTUNITY)



If these roadmap steps are successful, a final phase could represent the interconnection of the National CloudCERT nodes, forming a European CloudCERT with the sum of all the national members, or a Pan-European CloudCERT involving the National CIP Centers.

WORK PACKAGES

WORK PACKAGES OVERVIEW



WP1: PROJECT MANAGEMENT

- Coordination of partners and their work.
- Risk management.
- Financial management.

WP2: CONCEPTUAL MODELLING AND ARCHITECTURE

- Design the system architecture based on the system conceptual definition of CloudCERT Platform.

WP3: INFORMATION AND COMMUNICATION STANDARDS

- Definition of the content and format of the information to be exchanged.
- Definition of the protocol for exchange of information.

WP4: SECURE FRAMEWORK DEFINITION

- To investigate current working practices for secure management and sharing of sensitive information and finally proposes a list of required features.

WP5: PLATFORM DEVELOPMENT

- To develop a s ecure sharing of sensitive information exchanges, catalogue and database of CIP vulnerabilities.

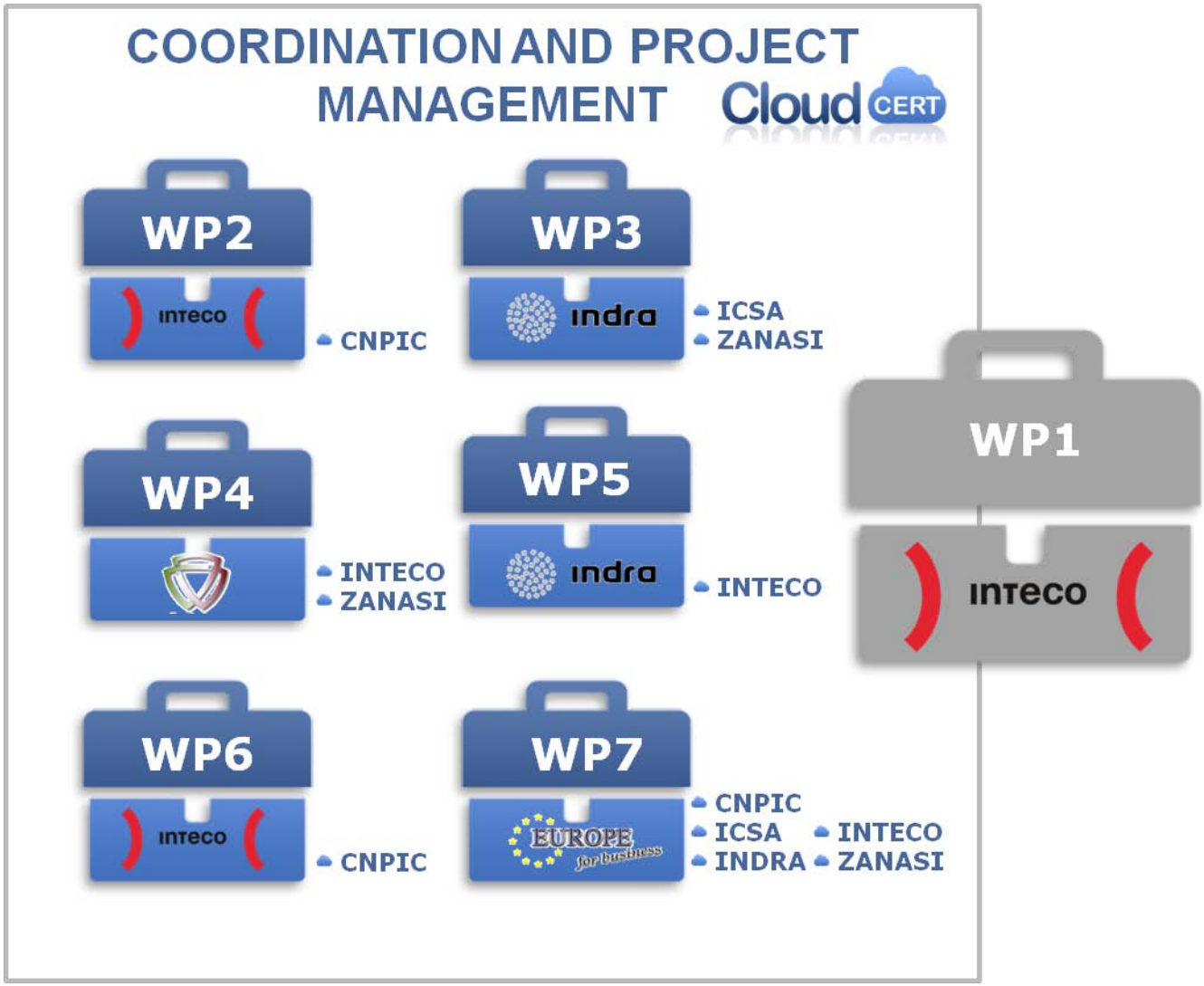
WP6: PILOT EXPERIMENTATION

- To test platform tool based on t he integration use cases.

WP7: DISSEMINATION OF PROJECT RESULTS

- Dissemination of the project results through publications, conferences, seminars.

WP1. PROJECT MANAGEMENT

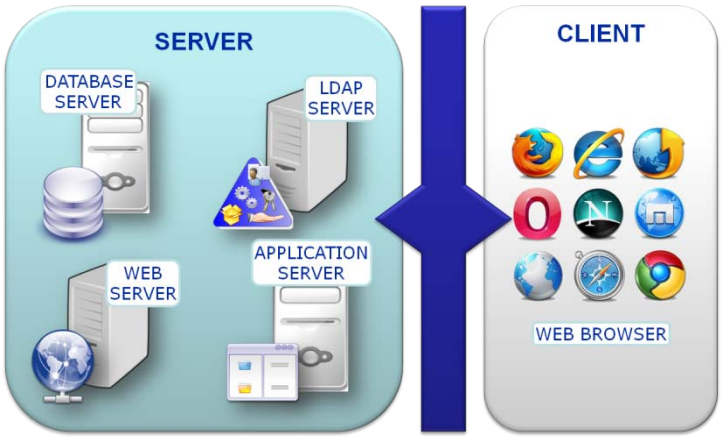


INTECO, as coordinator of CloudCERT Project, is the final responsible for the completion of all the work packages and the leading of project management activities.

WP2. PLATFORM DESIGN

ARQUITECTURE MODEL

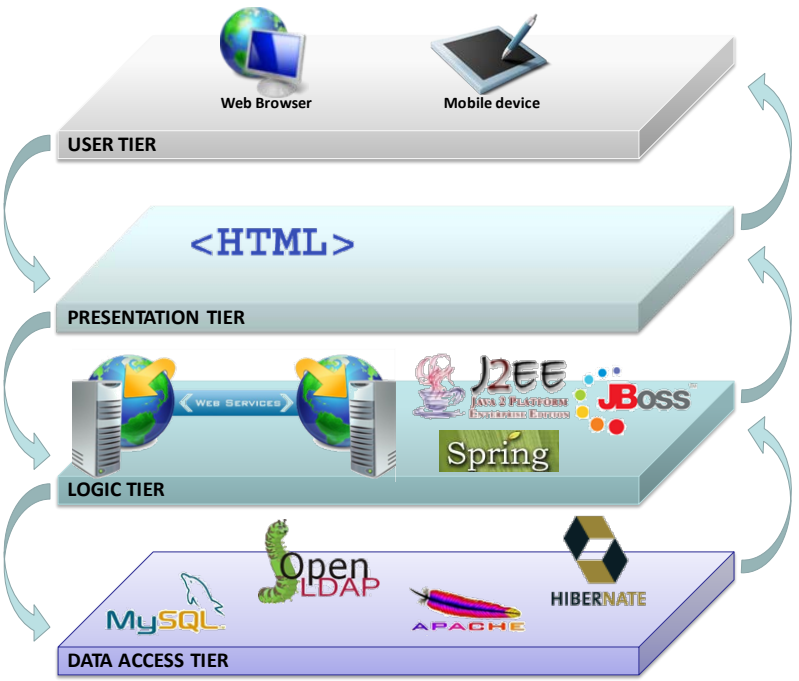
CloudCERT is based on a client / server architecture. The model of the different components of the CloudCERT platform is based on the standard J2EE.



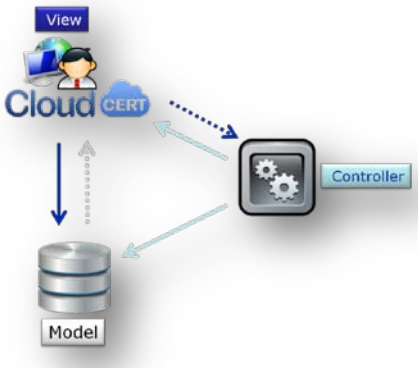
LOGICAL MODEL

The logic model components of the platform are grouped in the following types:

- **Data persistence.** CloudCERT has a complex data model. To handle this model, some Frameworks have been used to manage the model in an efficient manner.
- **Application Security.** All tasks relating to application security are based on information stored on LDAP.
- **Application flow control management**. CloudCERT uses the Struts Framework. Struts are a support tool for developing Web applications under the standard MVC under the platform J2EE.
- **Web Services**. They are deployed in AXIS CloudCERT. AXIS is a SOAP implementation developed by Apache and meeting OASIS and W3C standards.
- **Presentation layer**. It is based on the use of the frameworks: Struts and DWR.



MVC OUTLINE

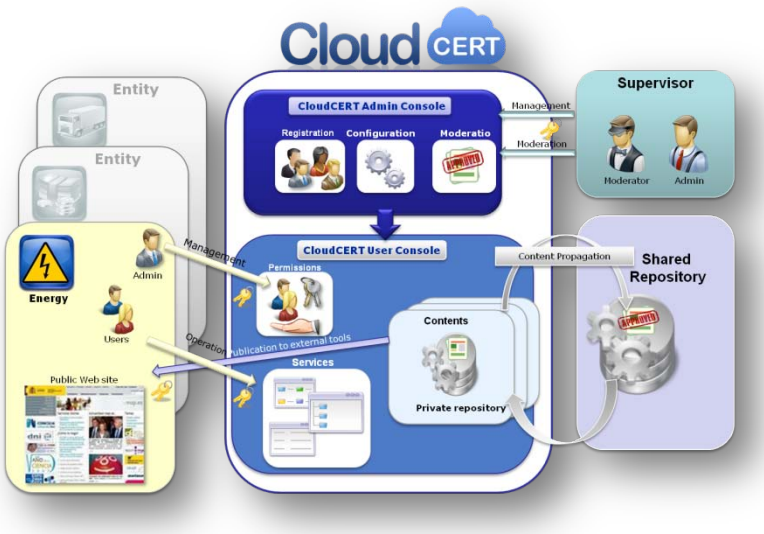


As the vast majority of existing J2EE applications, the Model - View - Controller has been adopted in the CloudCERT platform.

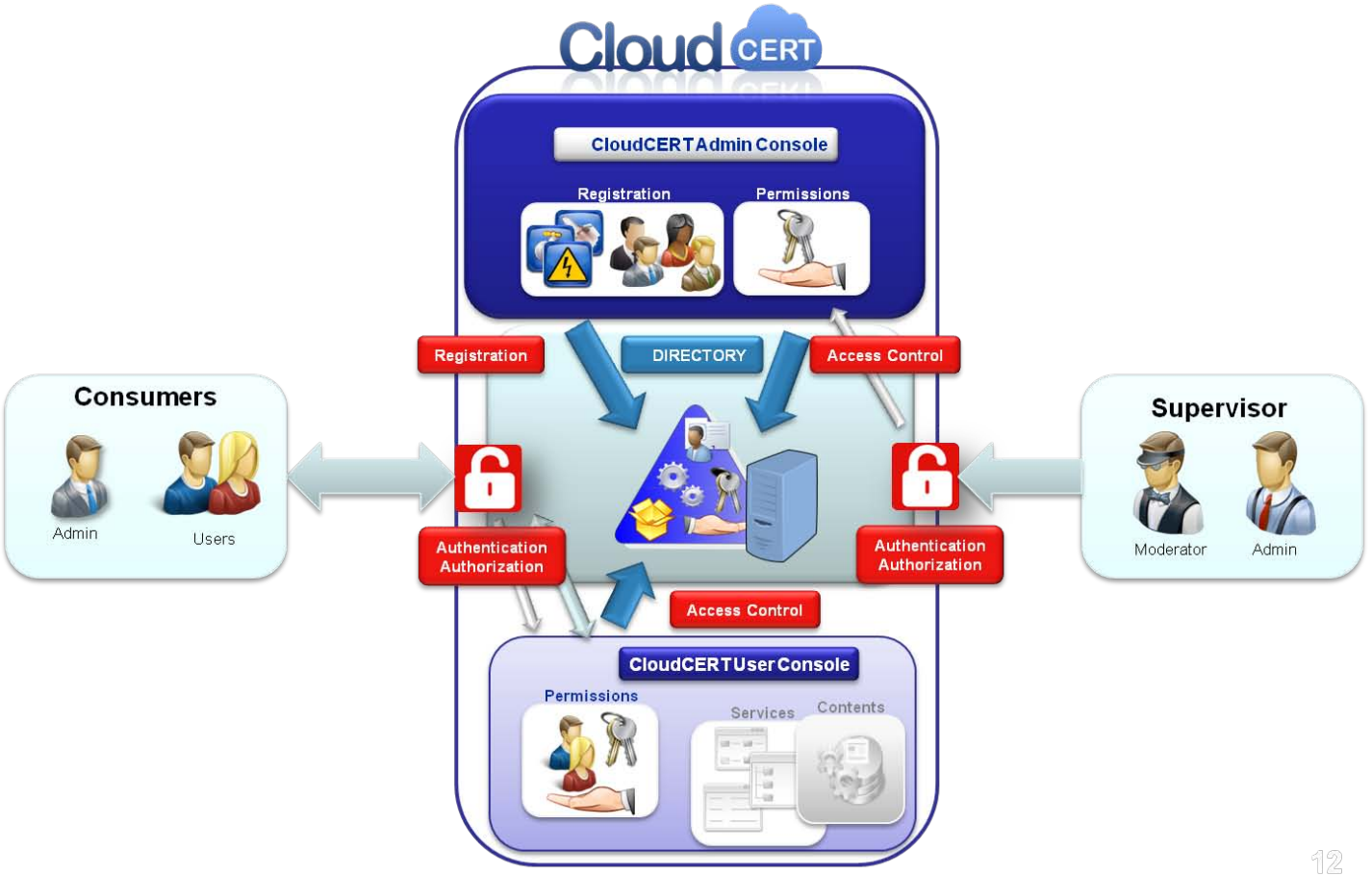
FUNCTIONAL DESIGN

Applications and modules forming CloudCERT platform include:

- **CloudCERT Authentication Module**: Central Authentication Service (CAS).
- **Password Management Module**: module password change management and activation of user accounts.
- **CloudCERT User Console**: application Management Console for different entities.
- **CloudCERT Administration Console**: application management for CloudCERT Platform (services, web services, entities, and contents).
- **CloudCERT WEB Services.**



SECURITY

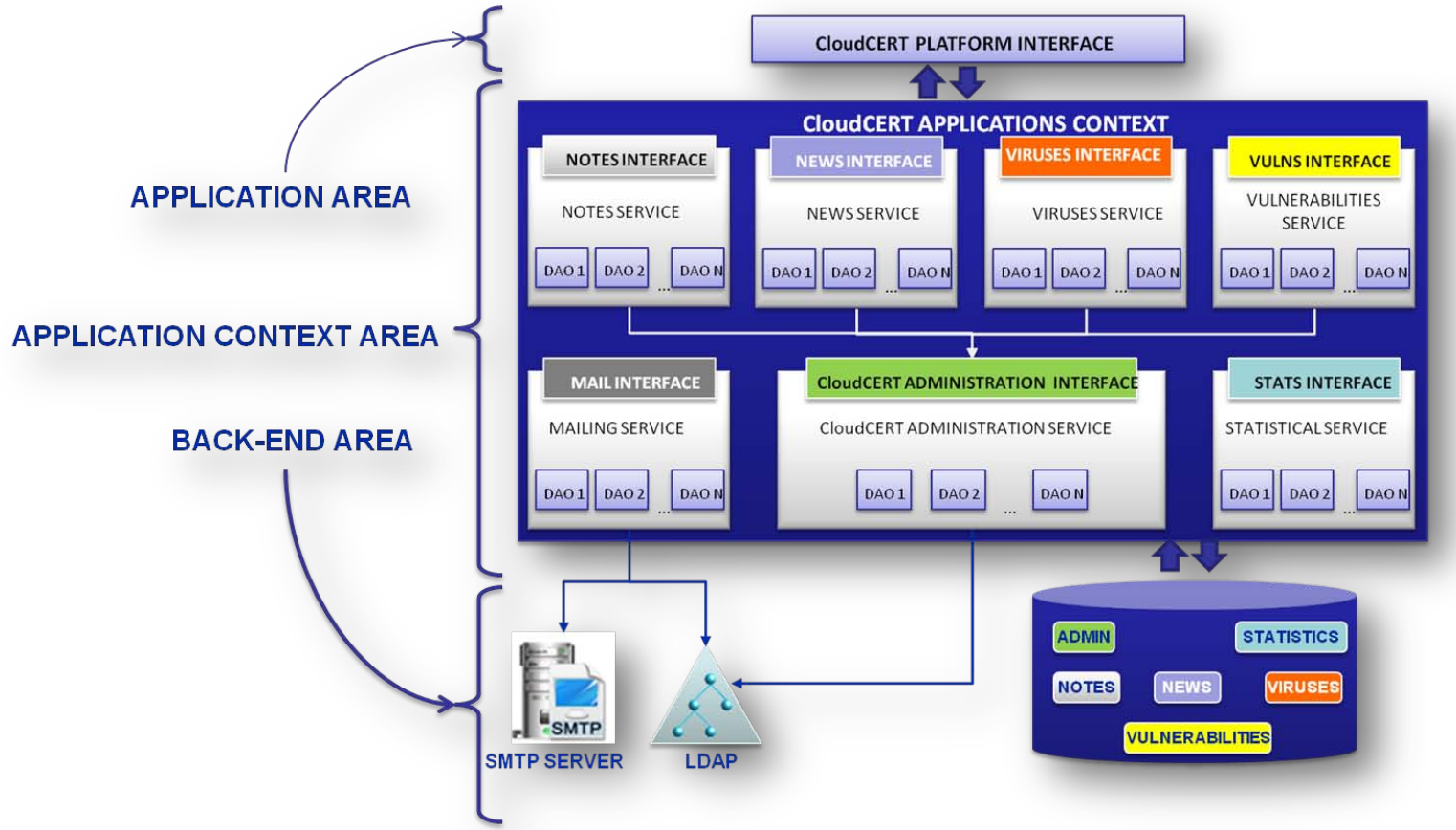


All questions regarding to application security are based on information stored on LDAP. The following Frameworks have been used to manage the CloudCERT security:

- **Spring Security.** Module belonging to Spring Framework allows application logic to maintain the security code free, providing authentication and authorization mechanisms for J2EE applications. Moreover Spring Security supports authentication on Central Authentication Service (CAS) providing a client API to interact with the CAS server.
- **Spring LDAP** module belonging to the Spring Framework provides interaction mechanisms to simplify operations on any type of LDAP server.

OVERALL CONTEXT DESIGN

Using the persistence of Database and LDAP, CloudCERT has defined a global context accessible by different applications:



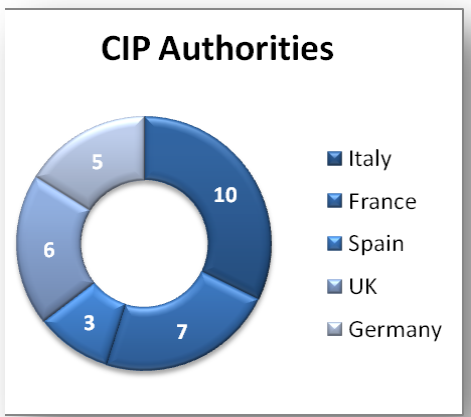
- **Application Area.** Where is included all presentation logic and flow control.
- **Area of application context.** The context that defines the various services offered by a public interface to the applications they support or other services.
- **Back-End Area.**
  - CloudCERT platform Database.
  - CloudCERT LDAP.
  - SMTP Server.

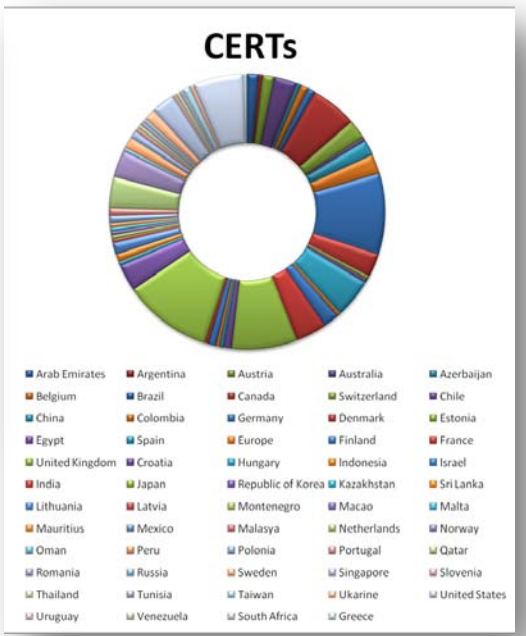
WP3. INFORMATION AND COMMUNICATION STANDARDS

INFORMATION CONTENTS ONTOLOGIES

- **NOTES:** manage and share all the information related to entities' institutional events of general interest into the CloudCERT Platform's network.
- **NEWS:** introduce, manage and s hare all those public news that it is considered of general interest.
- **WARNINGS:** introduce, manage and share all those cases considered as Alerts with special interest.
- **VIRUSES:** introduce, manage and s hare all those virus of special interest.
- **VULNERABILITIES:** manage and s hare all those vulnerabilities of special interest.
- **RSS ITEMS:** consult all those RSS items considered as of special interest.

POTENCIAL USERS FOR CLOUDCERT





PROTOCOLS FOR INFORMATION EXCHANGE AND INFORMATION DESCRIPTION STANDARDS

GENERAL PURPOSES TECHNOLOGIES FOR INFORMATION SHARING

Amongst the broad range of **protocols for information sharing** that have been developed over the years, three protocols have been selected partly because of their wide usage across different kinds of organisations, and partly because of their flexibility, which can be successfully exploited within the context of the CloudCERT:

- EDI (Electronic Data Interchange).
- XML (eXtensible Markup Language).
- SOAP (Simple Object Access Protocol).

INFORMATION EXCHANGE STANDARDS SPECIFIC FOR SECURITY PURPOSES

The CloudCERT project specifically focuses on helping the administrators of critical infrastructures and critical information infrastructures to better defend themselves in face of cyber-security menaces. Security flaws are (and will surely be in the near future) a threat to the operation of IT infrastructures.

As soon as new flaws are discovered, informing users and administrators about the issues identified is a vital task both for IT vendors and for security teams. The common way to circulate this information is by means of “security advisories”, technical documents that describe in detail the characteristics of the issue, its potential impact, and often also provide a list of possible solution.

This section focuses on the most popular standard **formats for security advisories**:

- CAIF (Common Announcement Interchange Format).
- EISPP (European Information Security Promotion Program) Common Advisory Format.
- DAF (Deutsches Advisory Format).
- OpenIOC (Open Indicators of Compromise).
- IODEF (Incident Object Description Exchange Format).
- VERIS (Vocabulary for Event Recording and Incident Sharing).
- STIX (Structured Threat Information eXpression).

ALTERNATIVE SOLUTIONS PLAN

CONTENTS EXCHANGE EVALUATION

Contents that include worthy information about alerts with special interest into CloudCERT's network are adequate to be transmitted with **SOAP** (Simple Object Access Protocol) over **HTTPs** (Hypertext Transfer Protocol Secure):

- Warnings.
- Viruses.
- Vulnerabilities.

However, the following contents are not adequate to be shared:

- **Notes**. This content is used by CloudCERT's users for sharing information related to entities' institutional events into its own network platform.
- **News**. This content is used by CloudCERT's users for sharing URL links related to entities' public news without any special interest outside its own network platform.
- **RSS Items**. This content is used by CloudCERT's users for sharing RSS items from different public feeds.

INDICATORS

It is important to manage carefully all the contents sharing with other organizations. For this purpose, a dashboard module was been necessary to integrate into CloudCERT Platform allowing to the administrator to patrol a set of indicators related to this activity.

The identified indicators suitable to be monitored were:

- Number of elements produced during a specific period of time.
- Number of elements read during a specified period of time.
- The Top N most read contents.
- The Top N organizations most active producers.
- The Top N organizations most active readers.
- The Top N organizations most active importing contents (from shared repository to own repository).
- Monthly distribution of most active days of producing/consuming contents.

WP4. SECURE FRAMEWORK DEFINITION

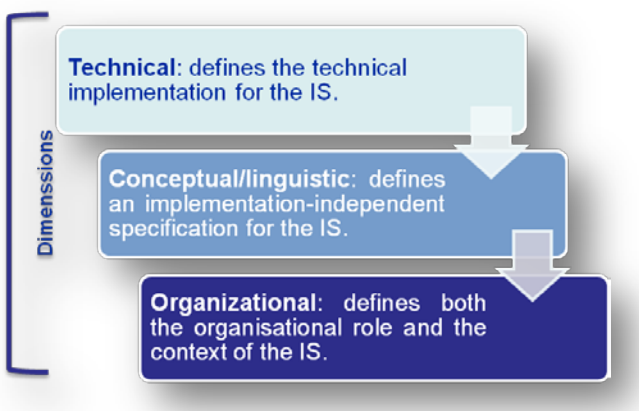
WORKING PRACTICES FOR SECURE MANAGEMENT AND SHARING OF SENSITIVE INFORMATION

The CloudCERT platform is intended to facilitate the exchange of **sensitive information** regarding CIP across various kinds of stakeholders with all security guarantees. Hence the first activity of the work package is a survey to investigate the working practices for the safe handling and sharing of sensitive information.

INFORMATION SECURITY

In this chapter the domain of information security and its main associated issues, with a par ticular focus put on Information Systems is introduced.

- **Confidentiality**: improper disclosure of information should be de tected and prevented.
- **Integrity**: information should not be modified by unauthorised subjects.
- **Availability**: information should be available to authorised subjects whenever required.



INFORMATION SHARING FOR CIP

This chapter reviews what has been done to enable effective information sharing, within the context of CIP, by the governments of two of the most prominent countries in the world: the United States and the United Kingdom.

CRITICAL INFRASTRUCTURE PROTECTION

Two countries have been taken as example and their CIP plans described and analysed in detail: the policies elaborated by the United States and the Italian situation:

- National Strategy for Homeland Security.
- Italian National Strategic Framework for the security of cyber-space.

CLOUDCERT SECURITY REQUIREMENTS

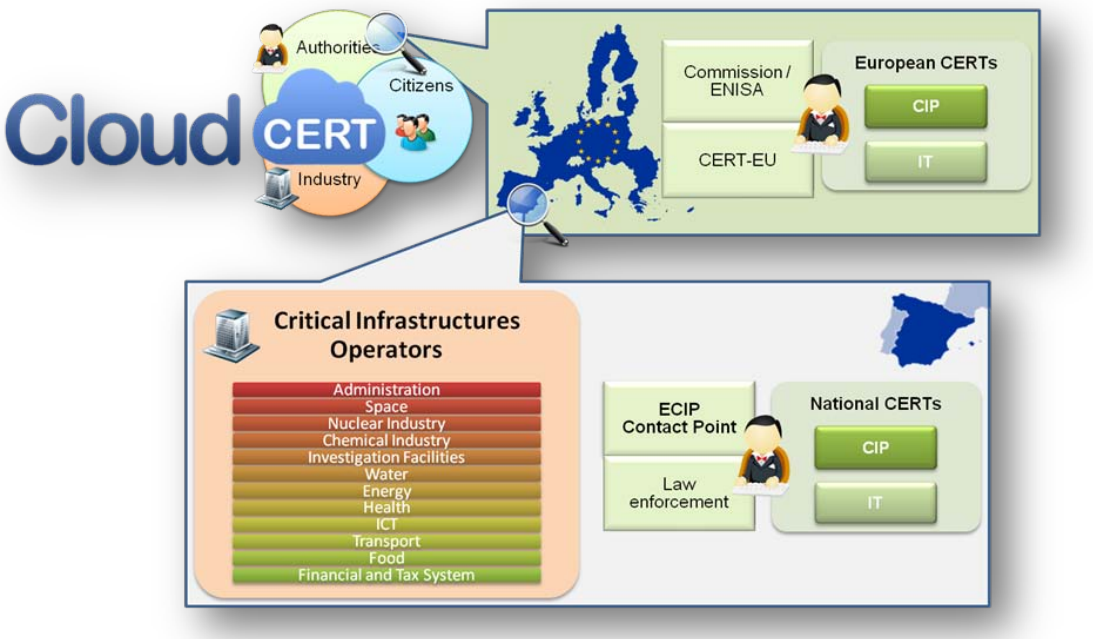
The main objectives of this deliverable are:

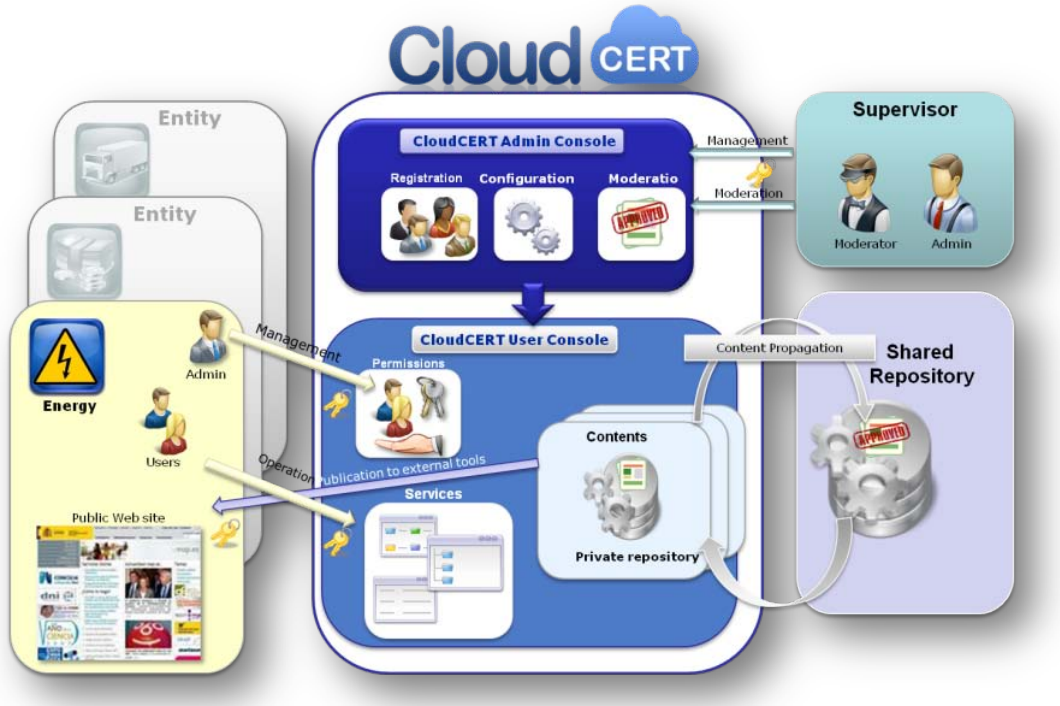
- Identify the main scientific sources in the field of PIC.
- Identify hypothetical methods and procedures to extend and strengthen collaborative processes of the system.
- Identify hypothetical methods and procedures to extend and strengthen the capacity of coordination between system stakeholders throughout the life cycle of the IC.

All with the ultimate goal of upgrading the operating model of governance in order to assign roles, responsibilities and objectives of the system stakeholders.

The CloudCERT stakeholders are grouped in three main categories:

- **Authorities** (public sector): authorities competent in information security and t he protection of critical infrastructure including legal and operational level. Herein includes policy and regulators makers as well as law enforcement teams.
- **Industry** (private sectors): critical infrastructure operators including theirs main suppliers (products manufacturers and services developers).
- **Citizens** (target audience): consumers of services provided by critical infrastructure.



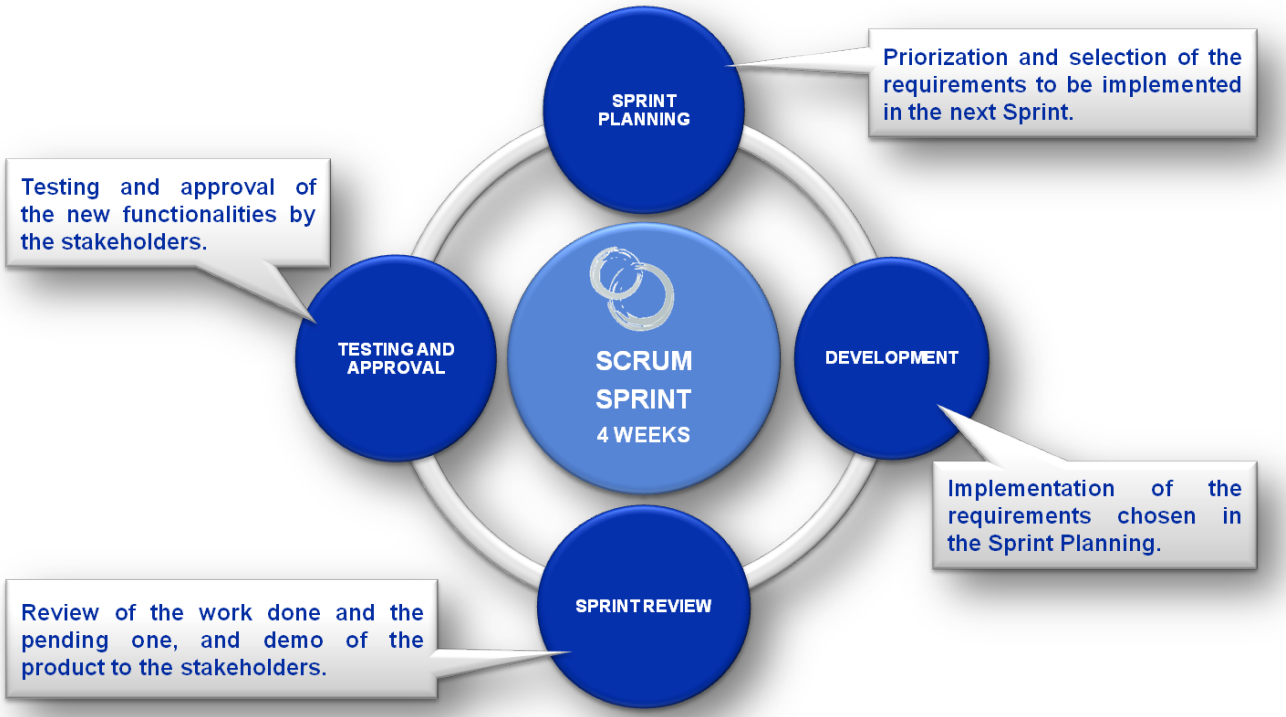


These stakeholders interact with CloudCERT platform based on a model of governance regulated as described below:

- Different **entities** can access the Platform: CERTs, law enforcement teams, and critical infrastructure operators. Every entity has its own space to allocate contents and can import contents from the shared repository. They can automatically export contents to external tools such as their own internal website.
- A **supervisor** organization:
  - **Manages** the platform by registering organizations and their administrator user, as well as by configuring and managing the available services. Supervisor configures entities permissions to contracted contents and services.
  - Supplies **moderation**. All contents to be part of the **shared repository** must be propagated for the moderator supervision. Moderation also involves publications in tools such as forums, wiki, etc.
- Every entity has one **administration user** who can create users and assign permissions for his/her Entity. Contents of the entity's private repository can be published into a shared repository with the approval of the supervisor.
- **Users** can interact with contents and services of the platform.

WP5. PLATFORM DEVELOPMENT

During this phase of the pilot project is implemented. For this purpose, the following tasks are performed:



REQUIREMENTS AND ANALYSIS

The software requirements specification aims to:

- Identify, asking the final users, the requirements and functionalities of the CloudCERT platform.
- Incorporate the requirements of the security framework and t he exchange of sensitive information.
- Define and priorize the requirements for the CloudCERT platform.

DEVELOPMENT

Following the agile methodology **scrum**, the development phase includes:

- Implementation of the requirements acquired in the previous phase, to create a functional pilot.
- Creation of the user and a dministration documentation of the pilot developed.

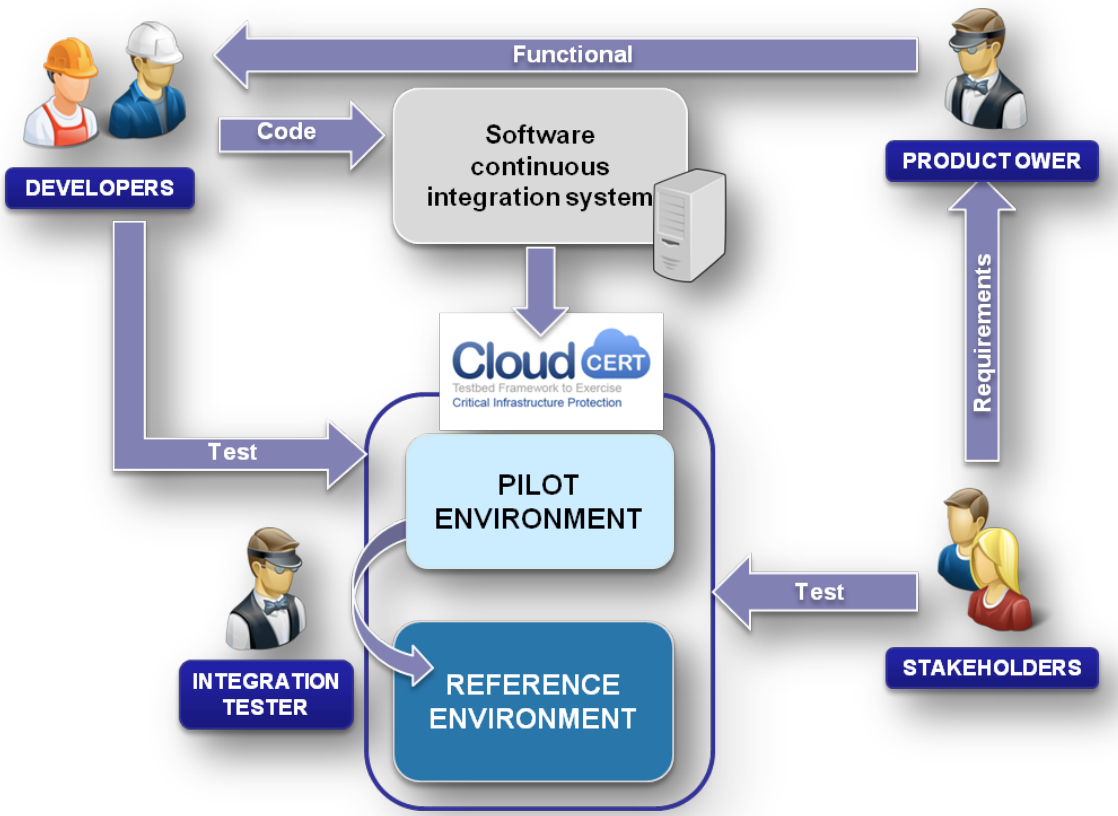
PLATFORM SETUP AND CONFIGURATION

During this phase, the developing and testing environments are provided and also installation and configuration manuals are created.

ENVIROMENTS

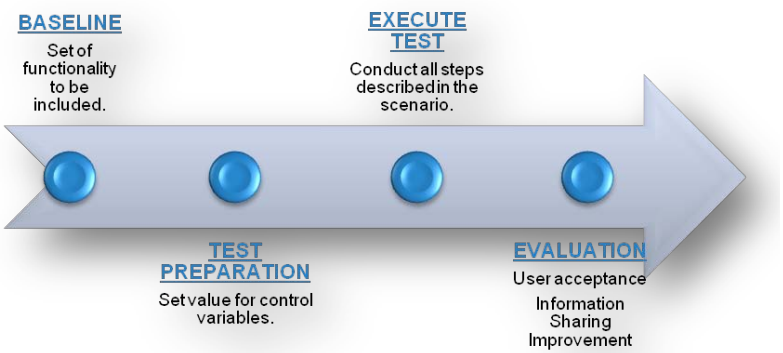
The **Pilot environment** is used to upload and test new developments, and to verify them after every sprint.

When the test phase is over and everything has been verified, the new release is deployed to **Reference environment**, containing a more stable version of CloudCERT Platform.



WP6. PILOT EXPERIMENTATION

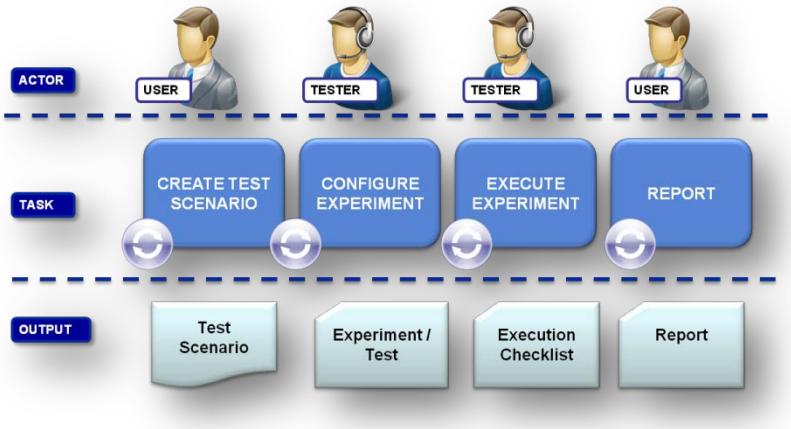
WP6 activities are focused on experimentation and evaluation based on the integration use cases, over the Pilot Platform developed and installed on previous WPs. Activities include functional testing and product acceptance, as well as simulation exercises for exchanging information between users of the platform to experiment and demonstrate on simulated cases, exchange of information on vulnerability discovery, security alerts and warnings and report security incidents.

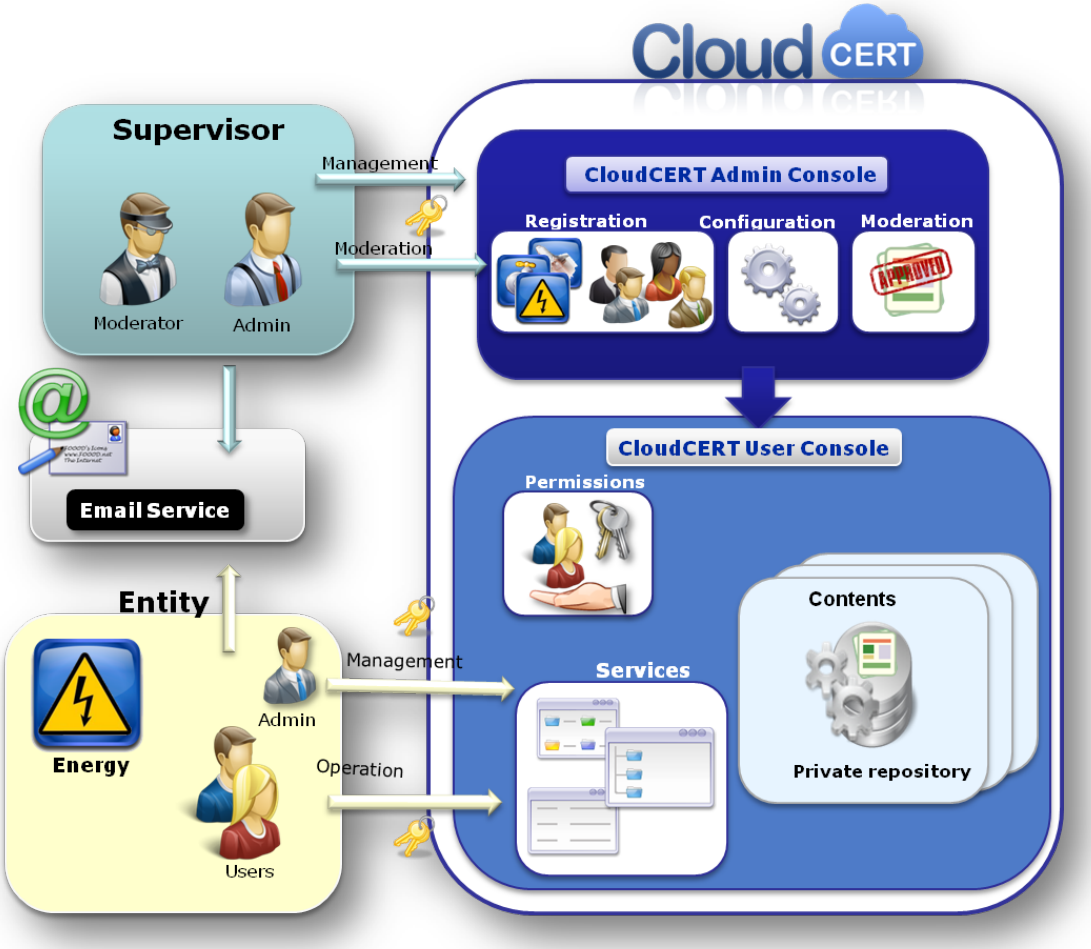


The purpose of evaluation and experimentation is to use scenario experimentation as a basis for evaluating the contribution of the CloudCERT platform solution to improving collaboration and cooperation among CIP actors in sharing cyber-security information, and thereby testing functionality and available work flows for communication to be held.

The goal of the evaluation, which is based on the results from the experimentation, is to:

- test CloudCERT (whether information sharing processes are correctly supported);
- verify how much CloudCERT addresses the challenges and needs of the domain in terms of collaboration and cooperation;
- and evaluate the potential improvement in CIP enabled by CloudCERT.





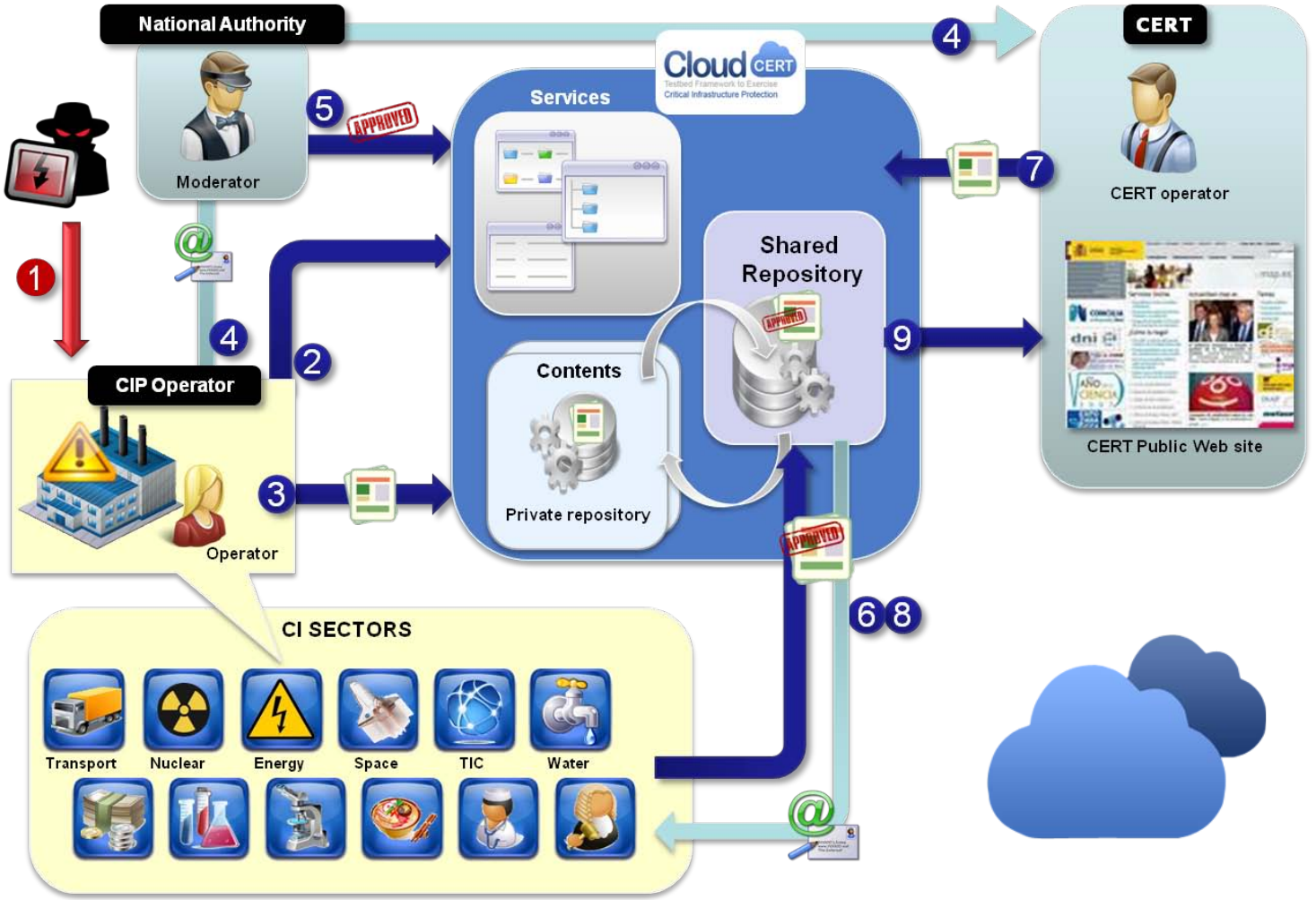
TOOLS FOR EXPERIMENTATION

- **CloudCERT Administration Console.** Lets the whole management of CloudCERT platform functionalities.
- **CloudCERT User Console**. Facilitates the creation, implementation and operation of new entities to respond to security incidents.
- **Email client tool.**

ACTORS

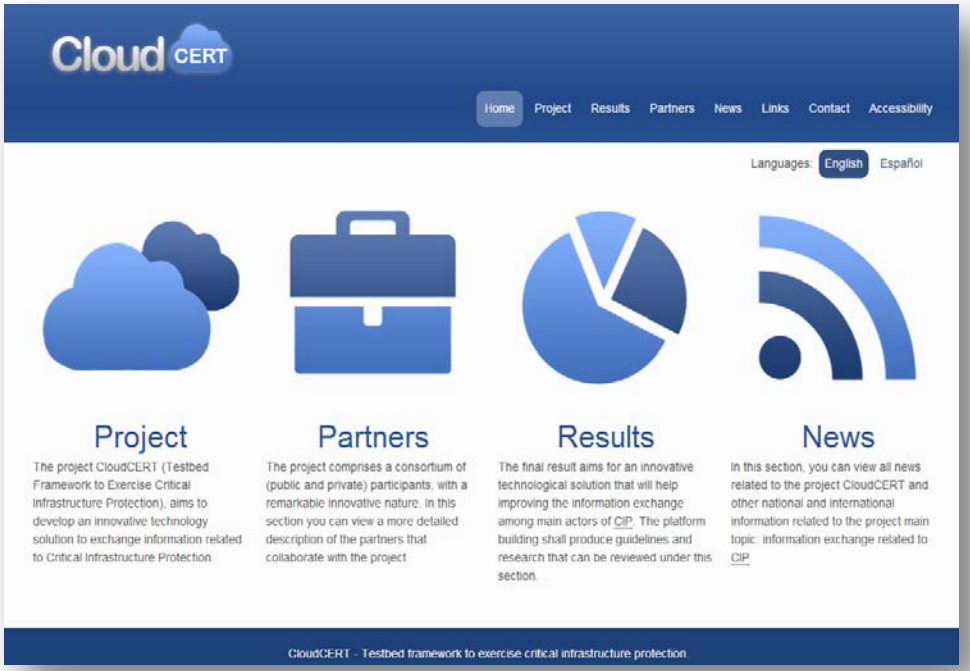
- User – CI Operator.
- Administrator – CI Operator.
- Moderator. – CERT / Authority
- Administrator.- Authority

USE CASE SCENARIO EXAMPLE



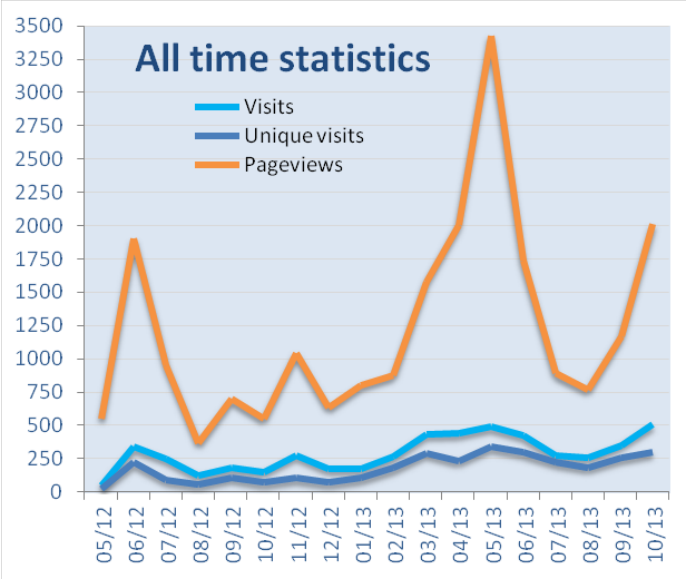
1. Operator **detects a vulnerability** on a pr oduct and intrusion on internal network.
2. Searches for information and reads **Incident Handling procedure** in wikiCIP.
3. Creates a **warning** and **posts** in Forum.
4. Official Incident **reporting**.
5. CNPIC **validates** the warning.
6. **and 8.** Warning visible in CloudCERT and by email through the bulletin.
7. CERT **solves** the warning and c loses Forum post with a workaround.
9. Warning is published in **external web site**.

WP7. DISSEMINATION OF PROJECT RESULTS



Most relevant indicators of CloudCERT project website http://cloudcert.european-project.eu/ :

- More than **200** news published.
- More than **5.000** visits (accumulated).
- More than **40** resources shared.
- More than **22.000** pageviews (accumulated).



WIKIPEDIA

- English: http://en.wikipedia.org/wiki/CloudCERT
- Spanish: http://es.wikipedia.org/wiki/CloudCERT
- Italian: http://it.wikipedia.org/wiki/CloudCERT

EVENTS

2012

- CRITIS12 Conference on Critical Information Infrastructures Security. http://critis12.hig.no/

2013

- Young Researchers Innovation Week
- ENISA 8th CERT workshop.
- Protezione delle Infrastrutture Critiche – Telecomunicazioni.

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Keywords	CERT, CSIRT, Critical Infrastructure Protection (CIP), Critical Infrastructure (CI), Information Sharing, Infrastructure Security
Funding Agency	European Union
Project Type	4rth Annual Work Programme adopted under the Council Decision No 2007/124/EC, Euratom, of Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007–2013" as part of the General Programme on "Security and Safeguarding Liberties".
Reference	HOME/2010/CIPS/AG/20

FINANCIADO POR LA UE

Innova.- Inteco publica la web del proyecto 'Cloud Cert' sobre protección de infraestructuras críticas

LEÓN, 14 Jun. (EUROPA PRESS) -

El INTECO presenta la web de un consorcio europeo en defensa de las infraestructuras críticas

PROYECTOS

Cloud CERT de INTECO: innovación internacional para la seguridad de las infraestructuras Críticas

FINAL CONFERENCE

CloudCERT Final conference to disseminate the European project results to the target audience.

- **Date:** 22 November 2013.
- **Location:**
  - Spanish Secretary of State of telecommunications and information society (SETSI). Madrid (Spain)
- **Target audience:**
  - CloudCERT project stakeholders.
  - Spanish Critical Infrastructure Operators including main suppliers' vendors.
  - Other European CERTs and law enforcement teams involved in CIP.
- **Admission:**
  - Free admission by invitation and broadcasted via video streaming http://www.cloudcert.webcastlive.es.

TECHNOLOGICAL SOLUTION

COLLABORATIVE PLATFORM

CAN BE CLOUDCERT INTERESTING FOR YOU?

- If your organization is a **CERT or a CI Operator**, you can use this platform to handle with Critical Infrastructure incidents and share cyber security information.
- If your organization's constituency as **CERT or Authority** includes **critical infrastructure operators**, you can get a customize platform to provide services and tools for your critical infrastructure protection constituency (forum, wiki, etc).
- If your organization has to interact with **National Authorities for Critical Infrastructure Protection**, and depending on its national competencies you can assign within the platform the most proper role: coordination, supervision, participation, etc.

CONTENTS

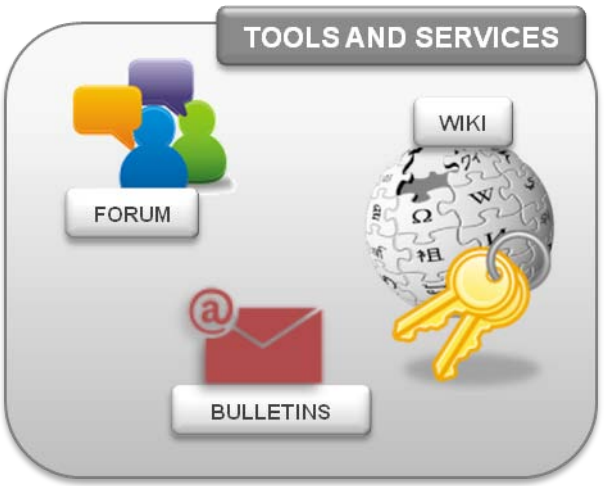
CloudCERT platform lets you create and propagate security contents such as:

- Notes.
- News.
- Warnings.
- Viruses.
- Vulnerabilities.
- RSS items.

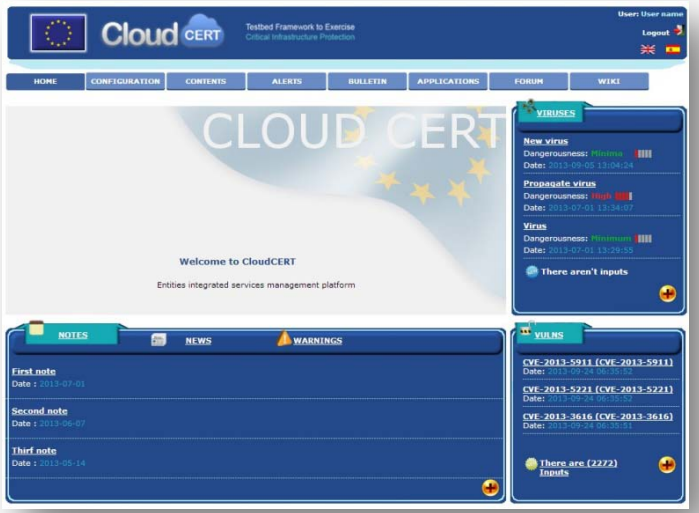
SERVICES AND TOOLS

CloudCERT platform lets users to share information to prevent security incidents through its services:

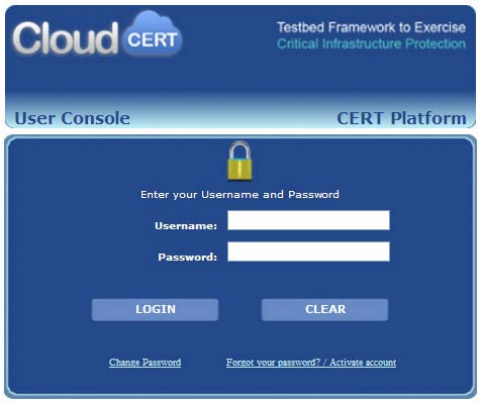
- Forum.
- WikiCIP.
- Bulletins Service.



PRODUCT SHEET



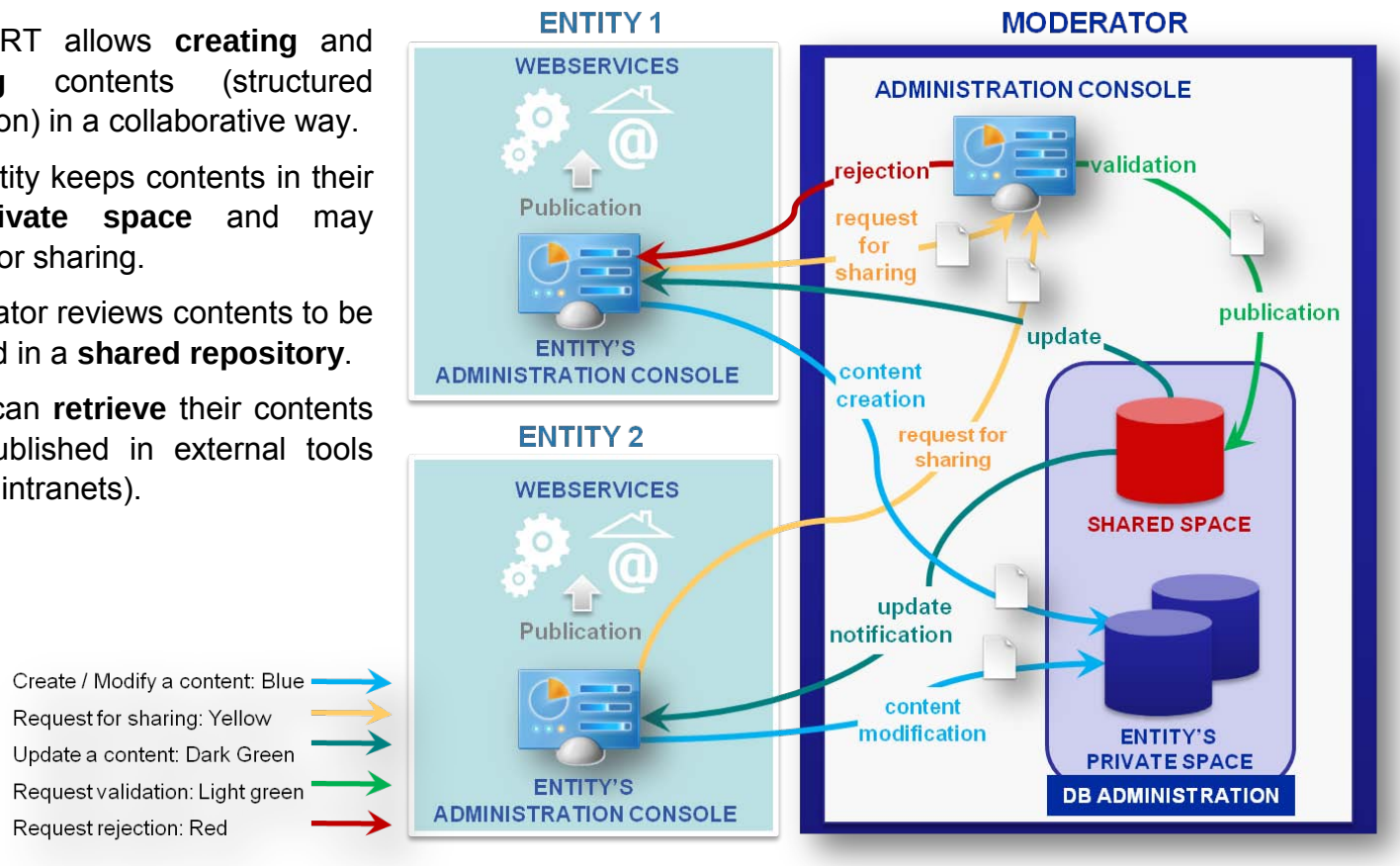
- **Collaborative platform** to manage a s hared repository of cyber security information cooperating in an efficient way.



- **Cloud** paradigm based on pr ivate and **shared repositories**.
- **Multi-language** application and contents translation interface.
- Personalized **services** (contracted).
- **Scalable** platform that allows new content, services, tools and workflows
- **Secure environment**:
  - Authentication mechanism based on username and password: Central Authentication Service (CAS).
  - Authorization based on permissions and roles.
  - Secure sessions managements.
  - Confidentiality and data protection guaranteed.

CONTENT LIFECYCLE

- CloudCERT allows **creating** and **updating** contents (structured information) in a collaborative way.
- Every entity keeps contents in their own **private space** and may request for sharing.
- A moderator reviews contents to be published in a **shared repository**.
- Entities can **retrieve** their contents to be published in external tools (such as intranets).

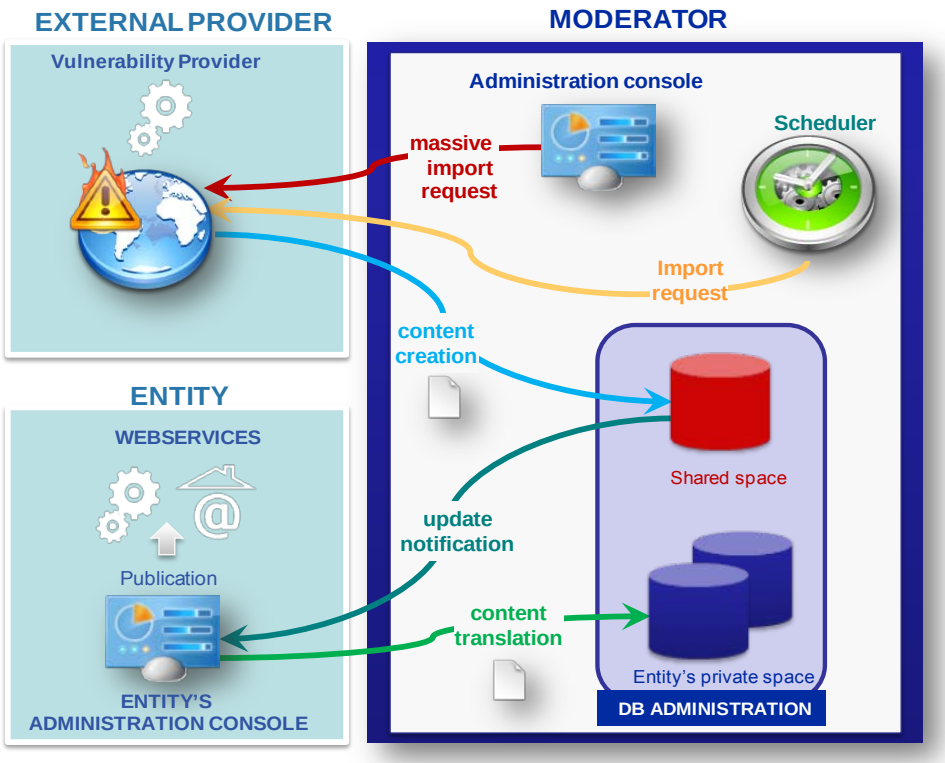


Contents may be in the following states during its life cycle:

- Created.
- Modified
- Shared.
- Updated.
- Validated.
- Rejected.

VULNERABILITIES LIFECYCLE

- Vulnerabilities are a specific type of content provided via **external sources** (such as NIST).
- A scheduled job automatically **imports** vulnerabilities in the system.
- Moderator can also **request a massive import** (for a period of time) into the system.
- Entities can **translate vulnerabilities** into their own private space.



Therefore, a vulnerability may be in the following states during its life cycle:

- Imported.
- Notified (update).
- Translated.

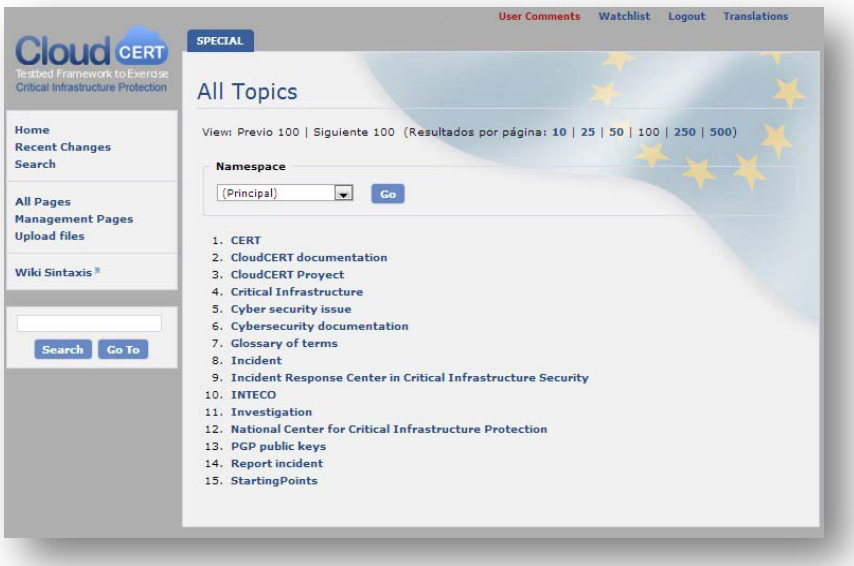
WIKICIP

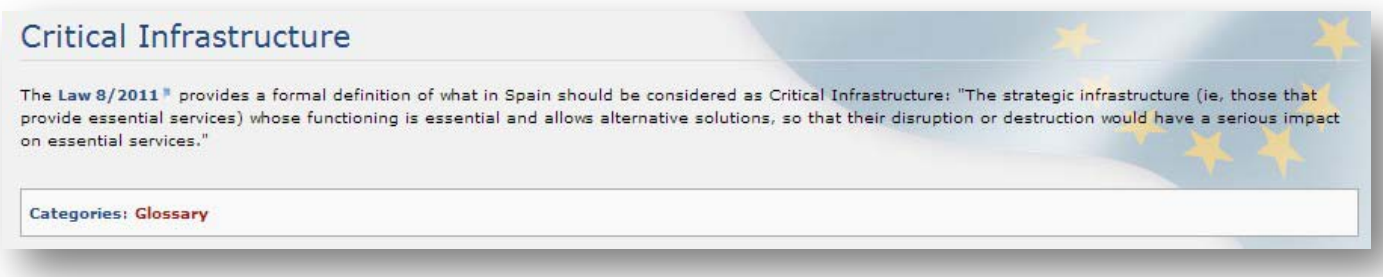
A wiki is a flexible system and allows the administrator to define any page hierarchy. WikiCIP allows maintaining **unstructured contents** in a collaborative manner with the following structure elements available:

- **Index** – Index page that displays links to different wiki pages with a similar topic.
  - **Page** – Individual pages about a specific topic.

WikiCIP has the following topics' structure:

- **CloudCERT documentation**:
  - Generic presentation of the project and main resources.
    - User manual.
    - Administrator manual.
    - Developer manual.
- **Cybersecurity documentation**:
  - Operating procedure to cybersecurity incidents.
  - Legal framework.
  - CIP interesting links.
- **Glossary.** Main terms related to Critical Infrastructure Protection.

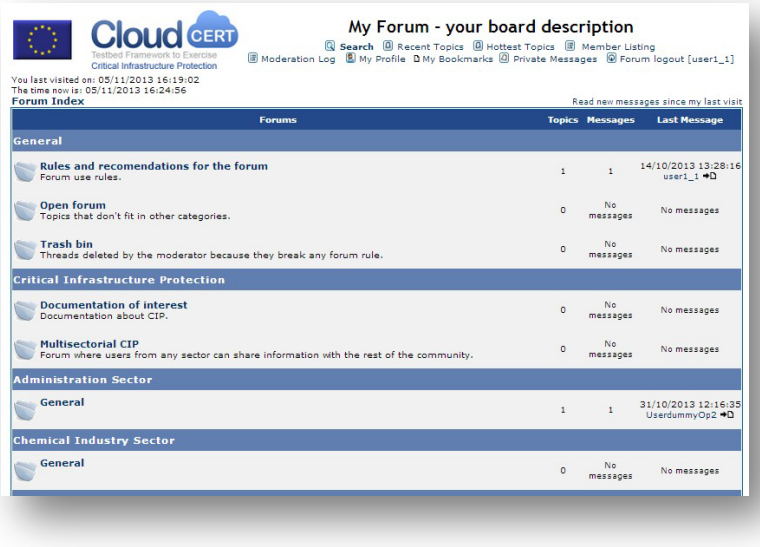




FORUM

The forum service allows unstructured information exchange with the following grouping elements available:

- **Category**. It is the top element of the hierarchy and usually used to group several related forums. This is a logical group, and ever forum inside a category has its own lifecycle.
  - **Forum**. A forum is a group of threats or discussions about the same topic.
    - **Thread** or **Topic**. It is the discussion itself, the messages from the users, talking about a specific topic.



CloudCERT Forum has the following categories:

- **General**. Forums for general information.
- **Critical Infrastructure Protection**. Where users can discuss and s hare general information on critical infrastructure protection with the rest of the community.
- Each critical infrastructure operator has a forum reserved for its **sector** (according to CIP Spanish national law classification) where users can share information with other relevant actors in that sector.
  - Administration.
  - Space.
  - Nuclear Industry.
  - Chemical Industry.
  - Investigation Facilities.
  - Water.
  - Energy.
  - Health.
  - Information and Communications Technology (ICT).
  - Transportation.
  - Food.
  - Financial and Tax System.

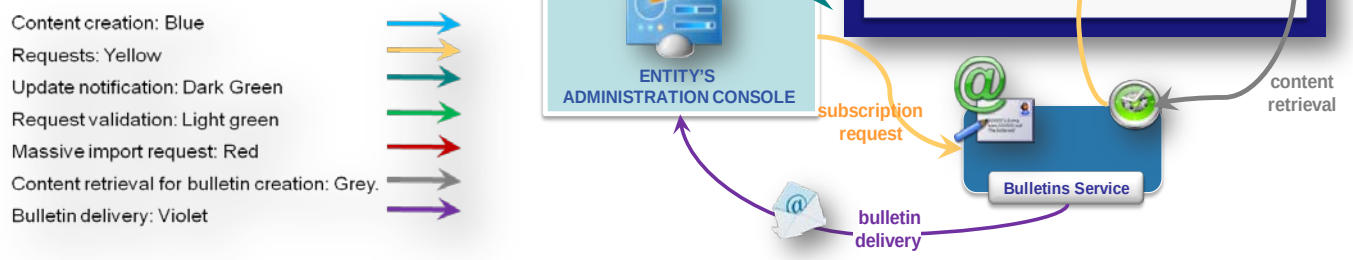
BULLETINS SERVICE

The Bulletins Service is an external service that communicates with CloudCERT Platform to **receive user subscriptions**, and **get security contents stored** in CloudCERT databases to create the bulletins. Bulletins service is responsible for creating and formatting the bulletins, and delivering the bulletins to the final users according to their preferences.

Each CloudCERT registered entity, can subscribe users (users previously registered or external users) to different security bulletins (newsletters), in order to receive bulletins periodically to their email inboxes.

The subscription could be processed by the administrator of the entity or by the final user.

- Bulletins service allows users to be informed regarding content updates via email notifications.
- A subscription process to select bulletin type and contents is required.
- The bulletins service collects contents, creates the customized bulletins and delivers to every final user.



CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

CloudCERT - Testbed framework to exercise critical infrastructure protection.

HOME/2010/CIPS/AG/20.
With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme. European Commission - Directorate-General Justice, Freedom and Security