D7.2

Design of the Pilot Products – First Release

WP7 – Pilots

Coco Cloud

Confidential and Compliant Clouds

Due date of deliverable: 01/11/2014
Actual submission date: 31/10/2014
Resubmission date: 31/07/2015

31/07/2015

Version 1.4

Responsible partner: ATOS
Editor: Cesar Mediavilla
E-mail address: cesar.mediavilla@atos.net

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

SEVENTH FRAMEWORK PROGRAMME

The Coco Cloud project is supported by funding under the Seventh Framework Programme of the European Commission, Objective ICT-2013.1.5 – Trustworthy ICT. GA #610853

Authors: Cesar Mediavilla

Approved by: Samson Y. Esayas (UO), Julien Debussche (2B)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.0	30.04.2014	Cesar Mediavilla	ATOS	Initial version with proposed Table of Contents
0.1	19.05.2014	Cesar Mediavilla	ATOS	Integration of the first feedback from the WP7 participants
0.2	03.06.2014	Francesco Di Cerbo	SAP	Initial draft for Section 2
0.2 b	10.06.2014	Francesco Di Cerbo	SAP	Updates to Table of Contents
0.3a	10.09.2014	Cesar Mediavilla	ATOS	Review of the ToC, section 3.5
0.3b	10.09.2014	Roberto Sanz	GHQ	Healthcare pilot contributions
0.4	19.09.2014	Francesco Di Cerbo	SAP	Updates to section 2
0.5a	23.09.2014	Cesar Mediavilla	ATOS	Executive Summary & Introduction
0.5b	07.10.2014	Francesco Di Cerbo	SAP	Updates to section 2 and 3
0.6	07.10.2014	Cesar Mediavilla	ATOS	Integrated version
0.7	10.10.2014	Carlos Cavero & Miriam Quintero	ATOS	Review of all the document
0.7	10.10.2014	Roberto Sanz & Alejandro Mañas	GHQ	Update of Healthcare Pilot
0.7	10.10.2014	Francesco Di Cerbo	SAP	Improvements in section 4.4.2
0.7	10.10.2014	Alberto Menini, Lorenzo Blasi	HPIS	Review of the document
0.8	10.10.2014	Cesar Mediavilla	ATOS	Integrated version of the deliverable
0.9	13.10.2014	Francesco Di Cerbo	SAP	Update of Mobile pilot based on Alberto Menini’s comments.
1.0	23.10.2014	Samson Y. Esayas / Francesco Di Cerbo	UO / SAP	SAP implementation of UO’s feedback.
1.0	23.10.2014	Cesar Mediavilla	ATOS	Integration of text produced by HPIS regarding Public Administration Pilot.
1.1	24.10.2014	Roberto Sanz & Alejandro Mañas	GHQ	GHQ implementation of UO’s feedback.
1.1 2B	28.10.2014	Julien Debussche / Benoit Van Asbroeck	2B	Review of the document

1.2	28.10.2014	Francesco di Cerbo; Roberto Sanz & Alejandro Mañas: Cesar Mediavilla	SAP;
			GHQ;
			ATOS
				Implementation of 2B comments

1.3	31.07.2014	Francesco di Cerbo; Roberto	SAP;
			GHQ;
				M18 Reviewer comments: identification and modification

		Sanz & Alejandro Mañas; Carlos Cavero & José Ruiz; Mirko Manea	ATOS; HPIS	
1.4	31.07.2014	Carlos Cavero & José Ruiz; Mirko Manea	ATOS; HPIS	Identification, modification and update of GHQ Requirement Analysis goals

Executive Summary

The second deliverable of WP7, D7.2, gathers all the information needed to implement the two pilots provided by the partners GHQ (Healthcare, Section 4) and SAP (Mobile in a corporate business context, Section 5), including each one of the specific architectures and the components that set up the pilot products. This document has been developed based on the specifications and requirements for each pilot defined in the D7.1 [1] and the general architecture depicted in D3.2 [2]. Therefore, the specific architectures are consistent and coherent with the Coco Cloud reference architecture, and have considered the requirements for the Data Sharing Agreement (D4.1) [3] and the Legal aspects defined in WP2.

We have defined a general evaluation framework to compare the success of each pilot and the specific architectures. Due to the different requirements and properties, described mainly in D7.1, and the specific architecture and components, described in detail in this document, the evaluation framework has been personalised per each pilot.

Finally, we have included a schedule and guidelines to get the pilots live and evaluate the pilot's outcomes.

Regarding the Public Administration Pilot, due to a change in current legislation, the chosen approach in D7.1 needs to be revised. AGID is currently reshaping one of the business cases that will be included in the next deliverable.

Table of contents

Table of Figures

Introduction

1.1. Focus of the document

The current document focuses on the detailed description of the software components for the pilots and operational business scenarios. The operational business scenario descriptions are based on the specifications and requirements reported in D7.1, and each one of the specific architectures has been depicted taking into account the reference architecture reported in **D3.2 – First version of Coco Cloud Architecture**. **D4.1 – DSA specifications, methodology and techniques** is also another deliverable related to the design of pilot products. In addition, the legal and regulatory aspects have been considered in the final provision of each specific architecture, thanks to the collaboration with WP2.

The core concept of Coco Cloud is to improve the security of information over traditional Cloud deployments. Particular emphasis is placed on privacy, security, and performance requirements [4], in addition to functional ones. For this reason, three pilots coming from different domains have been chosen: Public Administration information exchange, Healthcare images and medical data access, and corporate business data exchange through Mobile devices. D7.2 includes all the information needed to launch the pilot in two of three domains (Mobile and Health) and test the validity of the general Coco Cloud architecture, as well as the specific components required per each pilot. Further on, the information for the Public Administration Pilot will be included (see Section 3).

We have established a methodology framework to evaluate the results of the pilots, which has been personalised by each one of the pilots.

1.2. Document Structure

The deliverable is structured as follows:

- **Section 1** defines the scope and structure of the document, as well as the definitions and abbreviations used throughout the document.
- **Section 2** presents the methodology framework to evaluate the pilot products and the general architecture.
- **Section 3** explains the situation with the Public Administration business case.
- **Sections 4 & 5** gathers all the information related to the Healthcare and Mobile pilots, including an overview of the pilot scope, the specific architecture and description of the components and the specific evaluation methodology for this pilot.
- **Section 6** states the references to external contents used in the text.

1.3. Definitions and abbreviations

AgID / AGID	Agenzia per l'Italia Digitale
BO	Business Objects
CAD	*Codice dell'Amministrazione Digitale* (Digital Administration Code)
DICOM	Digital Imaging and Communications in Medicine
DSA	Data Sharing Agreement
DSL	Digital Subscriber Line

GQM	Goal, Question, Metric
GPS	Global Positioning System
NEMA	National Electrical Manufacturers Association
PA	Public Administration
PACS	Picture Archiving and Communication System
PDF	Portable Document Format
RIS	Radiology Information System
SSL-VPN	Secure Sockets Layer Virtual Private Network
TMT	Technology, Media and Telecommunications
WiFi	Synonym for Wireless Local Area Network (WLAN)

2. General Evaluation Framework

2.1. The GQM Approach

The approach that is proposed for the evaluation of Coco Cloud pilots is GQM [5], an acronym that stands for “Goal, Question, Metric”. It consists of a measurement approach based on the definition of measureable goals. This objective is met, by explicating the different facets of each goal through a set of questions and metrics. GQM permits to understand, quantitatively, if an objective is met or not. GQM approach is composed by two processes: a top-down refinement of goals into questions and then into metrics, and a bottom-up interpretation of the collected data [6,7]. GQM was initially applied for the evaluation of software development projects, but its flexibility allows for its application in multiple contexts.

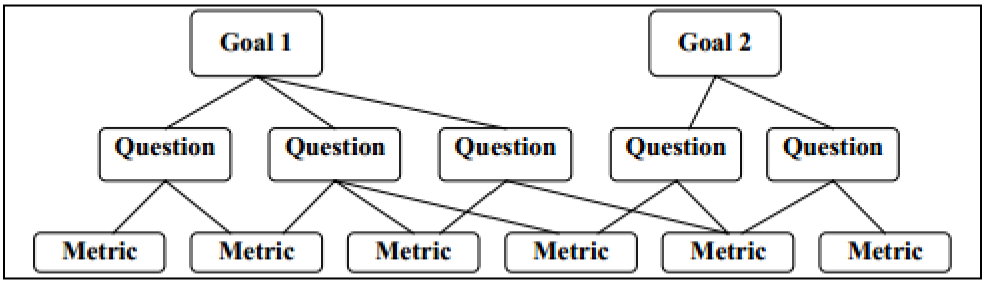


Figure 1: Relations among Goals, Questions and Metrics as defined in [1]

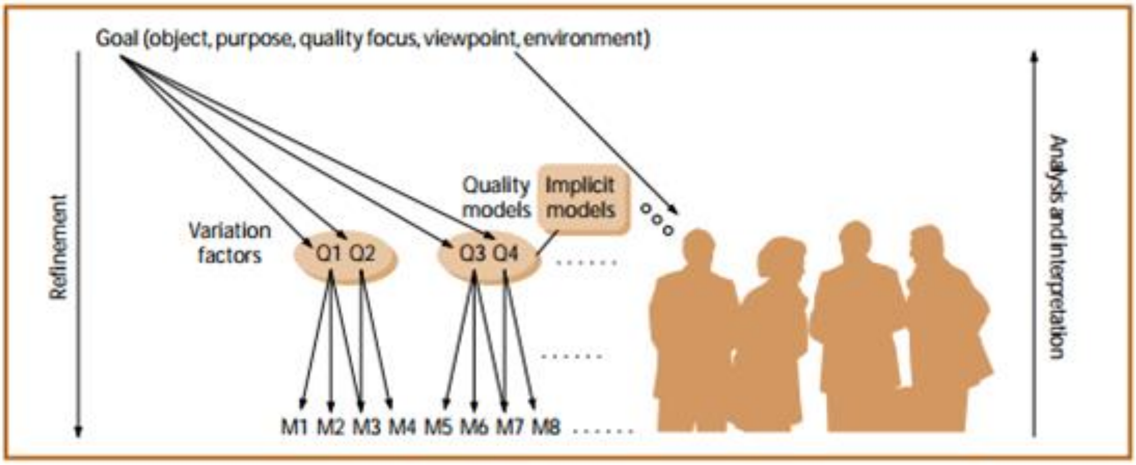


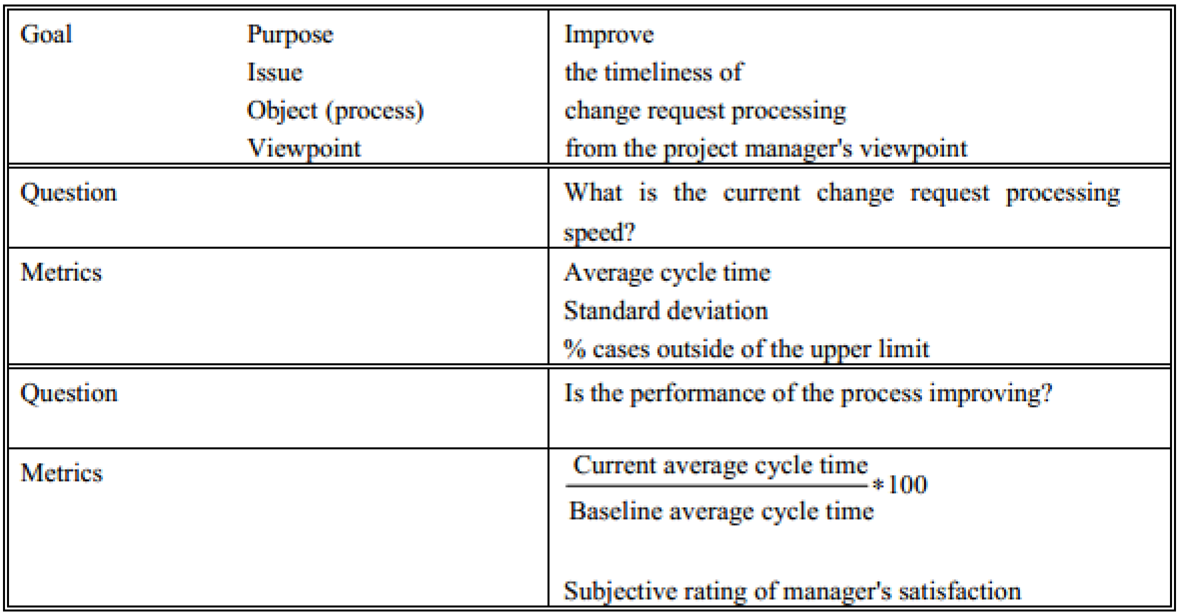
Figure 2: GQM process as defined in [4]

Within the GQM approach, a goal describes the purpose of the measurement. It is composed of the following five dimensions [8,9]:

- Object of study: defines the primary target of analysis or study.
- Purpose: represents the rationale behind the analysis.
- Quality focus: represents the specific attribute of the object of study that will be analysed.
- Viewpoint: represents the stakeholders of the study.
- Context: represents the environment in which the analysis will take place. The context of the study helps determining how generalizable the results might be.

In addition to the goals, GQM is also composed of a set of questions and metrics. A set of questions refines goals and reflects implicit models of the context. A set of metrics allows answering research questions by means of objective or subjective measurement [8].

An example of GQM is the following:



Goal	Purpose Issue Object (process) Viewpoint	Improve the timeliness of change request processing from the project manager's viewpoint
Question		What is the current change request processing speed?
Metrics		Average cycle time Standard deviation % cases outside of the upper limit
Question		Is the performance of the process improving?
Metrics		$\frac{\text{Current average cycle time}}{\text{Baseline average cycle time}} * 100$ Subjective rating of manager's satisfaction

Figure 3: a GQM example, as proposed in [1]

2.2. *Application of GQM in Coco Cloud*

The following process will be adopted:

- Definition of a set of common Goals for all Pilots: for example, in relation to the successful adoption of Coco Cloud contributions in pilots' applications.
- Definition of pilot-specific Goals able to evaluate the satisfaction of each pilot's stakeholders (consistently with pilot-specific objectives defined in D7.1).
- The Goal refinement phase (Questions) takes place in a pilot-specific manner. However, certain common Questions can be part of a global GQM for the whole project.
- The Metrics identification phase will be in part pilot-specific, in part common to all pilots: for example, we can use certain metrics associated to Coco Cloud software logs, or a set of common evaluation techniques (e.g. user satisfaction in a software usability assessment).

Among the possible evaluation techniques, we may use usability evaluations, as well as questionnaires for the relevant pilot's stakeholders.

2.3. *Common Evaluation Objectives*

This section will develop a GQM for Coco Cloud relevant evaluation objectives. In cooperation with the whole Coco Cloud consortium, a number of evaluation objectives will be identified and analysed. Each of the Pilot owners will consider such common evaluation objectives in their pilot's design and development activities, where applicable.

Goals		
ID	Name	Description
WP7-COCO-Gol-1	Compliant consumption of protected resources	Ensure the compliant consumption of protected resources from the point of view of data owner in Coco Cloud pilots
WP7-COCO-Gol-2	Confidentiality of protected resources	Ensure the confidentiality of protected resources from the point of view of data owner in Coco Cloud pilots

Questions		
ID	Name	Description
WP7-COCO-Que-1	Compliant consumption of protected resources	Which compliance regulations can be applicable for each resource type?
WP7-COCO-Que-2	Confidentiality of protected resources	Which types of resources have to be protected?

Metrics

ID	Name	Description
WP7-COCO-Met-1 (WP7-COCO-Que-1)	Which compliance regulations can be applicable for each resource type?	For each resource type: number of compliance conditions enforced / number of compliance conditions applicable
WP7-COCO-Met-2 (WP7-COCO-Que-1, WP7-COCO-Que-2)	Which types of resources have to be protected?	number of resource types to be protected

3. Public Administration Pilot

As described in Coco Cloud Deliverable 7.1, the business case for the Public Administration pilot was built within a specific regulatory scenario, based on the Italian master law for innovation, the “Codice dell'Amministrazione Digitale” (CAD – Digital Administration Code). In particular Article 58 of this law defined that Public Administrations had the duty to contract legal binding conventions (i.e. data sharing agreements), following the recommendations of national technical guidelines released by AGID. AGID was responsible for the monitoring of the implementation of this article.

In this scenario, the Public Administrations could leverage on Coco Cloud system for the definition of the DSAs and AGID could take advantage from Coco Cloud system to carry out automated monitoring of the compliance status of the DSA schema with the technical guidelines. Two principal use cases were identified (Civilian data sharing and Cadastral data sharing) under this regulatory scenario; they differed from the nature of involved data, but both assumed this business process.

Recently, this regulatory scenario has changed: the Italian law 114/2014, issued on August 2014, establishes new urgent measures for the simplification, administrative transparency and efficiency of the Public Administrations: it aims to simplify the relationship between PAs and, among other directives, it amends Article 58 (referred above), eliminating the concept of “conventions” (i.e. the DSA itself) and relaxing the mechanism of agreement between two PAs wishing to exchange data.

According to the new version of the Article 58, governments provide access for free to their databases to other administrations through the application cooperation (referred to in Article 72, paragraph 1, letter e), which is about technical details to ensure the integration of metadata, information and administrative procedures within the administrations. Within the changed framework, some of the assumptions of the business case have been released, because for the areas in which the use cases had been identified, conventions are no longer necessary. Consequently the role of AGID is somewhat reduced, because the law removes the duty of monitoring the agreements between PAs for their conformance to applicable technical guidelines.

So a use case refinement for AGID pilot is needed: the idea is to reshape a relevant business case in order to either provide an alternative use case or update some of the already defined use cases to reflect the occurred changes, if possible. In order to make up for the delay, an approach consists in the research for a business scenario to integrate the Coco Cloud components into the already in place AGID infrastructure.

Meanwhile AGID has been through a change in management, particularly the Chief of the organisation, an action that has caused as usual, a stop of activities for a couple of months, now fully recovered since the summer break. We are investigating with AGID (through scheduling meetings, sharing competences and documentation) in order to identify the most appropriate new use cases, reflecting real needs and in which the Coco Cloud system can be used to speed up and streamline processes in the public administrations. We commit to completely sort out this situation in the next couple of months and fully align it to the status of other pilots by M18.

4. Pilot Health

4.1. Overall Pilot scope

The Healthcare pilot introduces the challenge of bringing medical images and reports from the hospital to the patient, across the Internet by means of a Cloud platform. Patients and doctors will be closer due to the pilot interfaces, intended to reduce timeouts and patients' physical visits to the hospital to collect their reports and images. Further, it sets an additional communication path between patients and doctors via the Internet, by means of a message system between the pilot's users. Such scenario increases the system capabilities to provide healthcare services. Nevertheless, given the sensitive nature of the data managed by the pilot, the access requires the compliance of agreements between the hospital and the patients, as well as between the hospital and the doctors. Thus, the hospital acts as data controller and is responsible for establishing an adequate contract with the Cloud provider that hosts the portal. In order to ensure the compliance with the data protection legal regulations of the country [10], encryption techniques, digital signatures, non-repudiation mechanisms or similar methods must be present. These security requirements and their relation with the legal framework are developed in detail under chapter 8 of the D2.2 deliverable.

The pilot presents up to eleven main goals (fully described in 4.4.2), including:

- **WP7-HE-Gol-1**: Allow the management of medical reports and images.
- **WP7-HE-Gol-2**: Allow the management of disclosure permissions.
- **WP7-HE-Gol-3.1**: Definition of a mechanism for doctors to ask for a second opinion.
- **WP7-HE-Gol-3.2**: Definition of a mechanism to ask patients for access permissions.
- **WP7-HE-Gol-4,5**: Enable a message communication system between users, as well as an alert communication system (the first for health issues, the second for technical incidences).
- **WP7-HE-Gol-6,7,9,10**: Definition of several mechanisms to guarantee data privacy and data protection.
- **WP7-HE-Gol-8**: Permit tracking and auditing of activities.

Several specific use cases have been proposed to achieve such goals, in addition to the requirements arisen from the scenario, which involve issues regarding functionality, privacy, security and performance requirements. As a modification of the D7.1, only doctors explicitly authorised by the patient can access his or her profile through the pilot. Therefore, a new goal (WP7-HE-Gol-3.2) raises, allowing doctors to ask patients for access permissions, especially in those cases where the patient comes to the specialist and is attended by a doctor who is not her or his usual one. Everyone involved in a disclosure operation must be previously registered in the system.

The design preserves the current workflow and proposes the expected workflow as an extension of the current scenario, allowing both scenarios to coexist. The current and the expected scenarios are summarised in Figure 4:

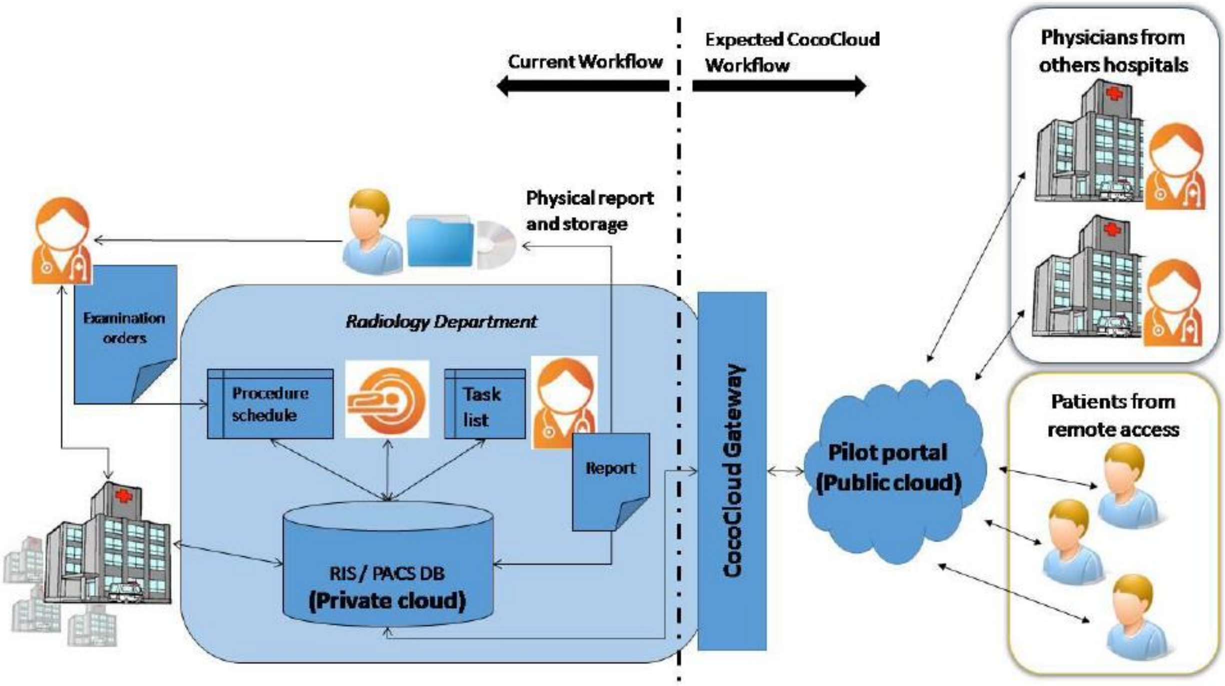

Current Workflow
Expected CocoCloud Workflow
Physicians from others hospitals
Physical report and storage
Examination orders
Radiology Department
Procedure schedule
Task list
Report
RIS / PACS DB (Private cloud)
CocoCloud Gateway
Pilot portal (Public cloud)
Patients from remote access

Figure 4: Expected workflow provided by the health pilot, ensuring coexistence with the current radiological workflow.

Notice that it is mandatory to preserve the current scenario to ensure standardised health assistance. Patients coming to the hospital expecting to receive healthcare personally, or elderly, who are not familiar with the Internet and ICTs, are examples of people who are not ready to assume a full change towards the Cloud-based health information systems. Therefore, despite the advantages of the future scenario, the whole workflow of the current scenario must be kept.

The main beneficiaries of the project are, on one hand, patients and doctors from Quirón Hospital as individuals, and on the other hand, Quirón Hospital Group as a healthcare provider organisation. Each stakeholder has its own specific benefits. In case of the patients, they gain autonomy, as well as a faster, more secure and ubiquitous access to the radiological reports and images, avoiding unnecessary timeouts and visits to the hospital. For the doctors, the portal allows them easily disclosing a patient’s case to other doctors, in order to get a second opinion. In case of the hospital, the pilot will reduce costs by avoiding hardcopies of the reports and the images, as well as increasing its efficiency by dedicating administrative resources to other tasks, instead of handing reports. In addition, the portal allows the hospital to reduce queues and brings to the patient the chance of participating more actively in the healthcare cycle – putting the patient at the centre of the healthcare loop – thus increasing patient trust and fidelity. As a long-term benefit, the hospital will become more competitive in offering healthcare services.

4.2. Requirement Analysis Overview

Up to now, the Health pilot raises several requirements arranged in the following categories: functional, privacy, security and performance, depending on the goal of each requirement. The current architecture intends to satisfy all these requirements and for the moment, all requirements are considered by the current design. This is a list with the most important ones (priority 1), extracted from D7.1 [1]:

Functional requirements

- **WP7-HE-Fun-1**: Each system user must have a username and password to authenticate to the system. Further, a digital certificate is recommended to guarantee the authenticity of the user access according to the DSA compliance.
  - Goal addressed: WP7-HE-Gol-7
- **WP7-HE-Fun-2**: Establishment of a communication mechanism between the different actors of the system. This mechanism has two types of information flow, the Alert Messages and the Information Messages. To interact through the messages mechanism, the patient must have previously granted permission to the user with whom s/he wants to communicate. Such user must be a doctor, given that the communication must occur between a doctor and a patient.
  - Goals addressed: WP7-HE-Gol-4 and WP7-HE-Gol-5
- **WP7-HE-Fun-3**: Users can view detailed reports directly from the “Patient and doctor portal” interface.
  - Goal addressed: WP7-HE-Gol-1
- **WP7-HE-Fun-5:** Users can edit the visibility of any report from their profiles.
  - Goal addressed: WP7-HE-Gol-6
- **WP7-HE-Fun-6.1:** A doctor can invite another doctor to view/analyse a given case in order to have a second opinion.
  - Goal addressed: WP7-HE-Gol-3.1
- **WP7-HE-Fun-6.2:** A doctor can ask patient permission to access her or his profile.
  - Goal addressed: WP7-HE-Gol-3.2
- **WP7-HE-Fun-7:** Allow users to edit and modify their personal data stored in their individual profile. Only the data subject, or the legal representative failing him, has enough permissions to edit and modify their personal information.
  - Goals addressed: WP7-HE-Gol-6 and WP7-HE-Gol-7
- **WP7-HE-Fun-8:** Allow users to reset their password, if they have forgotten it.
  - Goal addressed: WP7-HE-Gol-7
- **WP7-HE-Fun-9:** Patients can grant permissions to other patients (like caregivers or family members), if required.
  - Goal addressed: WP7-HE-Gol-2
- **WP7-HE-Fun-10:** The doctor user enters the search criteria into a search form and performs the search operation over those patients, who previously have granted access permission to the doctor.
  - Goal addressed: WP7-HE-Gol-1
- **WP7-HE-Fun-11:** The administrator user can manage patient and doctor user’s accounts in order to add, edit or remove users.
  - Goal addressed: WP7-HE-Gol-7
- **WP7-HE-Fun-12:** Configure or edit the connection parameters between hospital PACS/RIS and the “Patient and doctor portal”.

- Goal addressed: WP7-HE-Gol-9

- **WP7-HE-Fun-15:** Doctors can include comments appended to a given report during the diagnostic process.
    - Goals addressed: WP7-HE-Gol-1 and WP7-HE-Gol-3

Privacy requirements

- **WP7-HE-Pri-1:** Personal data must only be viewed by doctors or other users, for the purpose of providing healthcare services to the patient, being previously authorised by the patient.
    - Goals addressed: WP7-HE-Gol-7, WP7-HE-Gol-9 and WP7-HE-Gol-10
- **WP7-HE-Pri-2:** Patients can exercise their rights of access, modification, deletion or opposition about their personal data.
    - Goal addressed: **WP7-HE-Gol-6**

Security requirements

- **WP7-HE-Sec-1**: Access control must employ user and password (mandatory), digital certificate (highly recommended) or, failing this, a second check through email account validation.
    - Goal addressed: WP7-HE-Gol-7
- **WP7-HE-Sec-2**: The application must monitor and register all relevant accesses and operations.
    - Goal addressed: WP7-HE-Gol-8
- **WP7-HE-Sec-3**: Session timeout must be enforced.
    - Goal addressed: WP7-HE-Gol-7
- **WP7-HE-Sec-4**: All connections need to be done via an encrypted link (e.g., HTTPS).
    - Goal addressed: WP7-HE-Gol-9
- **WP7-HE-Sec-5**: All actions performed within the system must be DSA compliant.
    - Goal addressed: **WP7-HE-Gol-6, WP7-HE-Gol-10**

Data usage control requirements

- **WP7-HE-Dus-1**: Data stored in a public Cloud must be protected by encryption mechanisms.
    - Goal addressed: WP7-HE-Gol-10
- **WP7-HE-Dus-2**: In case the user owns a digital signature, all sensitive data (those data established as sensitive data by the privacy law) must be signed by the current user with her or his personal digital signature, before any transaction.
    - Goal addressed: **WP7-HE-Gol-6, WP7-HE-Gol-10**
- **WP7-HE-Dus-3**: All data must be available any time through the “Patient and doctor portal” with the proper security measures.

- Goal addressed: **WP7-HE-Gol-5, WP7-HE-Gol-8**

Performance requirements

- **WP7-HE-Per-2:** If a report needs to be visualised, then significant memory space must be reserved.
    - Goal addressed: **WP7-HE-Gol-5, WP7-HE-Gol-8**
- **WP7-HE-Per-3:** The "Patient and doctor portal" must support several requests at once.
    - Goal addressed: **WP7-HE-Gol-5, WP7-HE-Gol-8**
- **WP7-HE-Per-4:** The "Patient and doctor portal" must be available any time.
    - Goal addressed: **WP7-HE-Gol-5, WP7-HE-Gol-8**

4.3. Pilot Specific Architecture

4.3.1. General Pilot Architecture

Figure 5 shows the overall pilot architecture, where two Clouds can be distinguished. On the one hand, the public Cloud that supports the Health pilot infrastructure and those components that are not present in the current radiological workflow. On the other hand, the private Cloud that holds the usual components of the radiology department, which the Health pilot system also requires. Specifically, the PACS provides storage for DICOM objects, which can contain reports and medical images as well, including different modalities. To interact with the PACS there is a query/retrieve protocol, defined in the DICOM [11] standard from the NEMA [12] organisation. The protocol allows carrying out queries, storages and retrieves of images, reports, and patients' related data. Usually the interaction with the PACS (to evaluate and to diagnose clinical images) is supported by a client application running under http protocols.

The pilot architecture includes a "dcm4chee archive" PACS on the private Cloud, which internally persists the DICOM objects in the file system and the user data in a relational "MySQL" database.

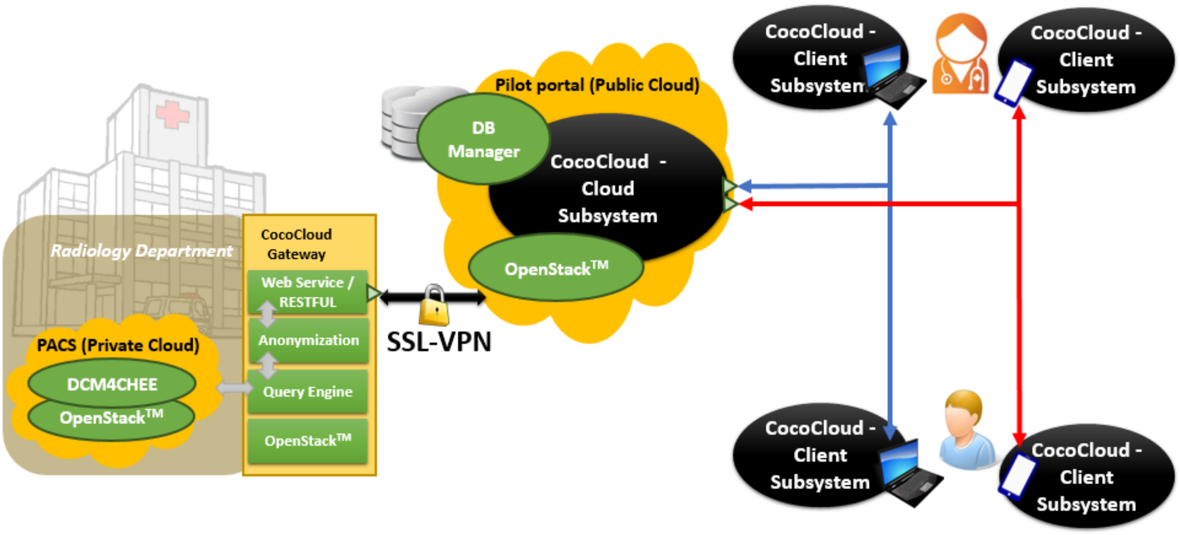

Radiology Department
PACS (Private Cloud)
DCM4CHEE
OpenStack™
CocoCloud Gateway
Web Service / RESTFUL
Anonymization
Query Engine
OpenStack™
SSL-VPN
Pilot portal (Public Cloud)
DB Manager
CocoCloud - Cloud Subsystem
OpenStack™
CocoCloud - Client Subsystem
CocoCloud - Client Subsystem
CocoCloud - Client Subsystem
CocoCloud - Client Subsystem

Figure 5: Coco Cloud Health pilot architecture

The pilot is intended to keep the most realistic approach as possible. Due to the big amount of highly sensitive information stored in the PACS, it cannot be exposed directly to the Internet under no circumstances in a production environment. In addition, the PACS must be inside the hospital's private network as an essential piece of the radiological workflow. Therefore, it is necessary to have the production environment (current radiological workflow) separated from the Coco Cloud pilot, at least during the early stages of the project.

The Coco Cloud gateway component is placed between both Clouds, and it aims to provide a secure way to access the hospital private network from the Internet. The pilot connects directly to the Coco Cloud gateway through a SSL-VPN connection, ensuring that only the pilot portal can reach the entry point to the private hospital network (i.e. the gateway). In addition, the gateway is responsible for carrying out a pseudo-anonymisation process with backward traceability, interacting with the PACS to gather those images and reports requested by the pilot and bringing them in an anonymised way.

The pilot on the public Cloud has the Coco Cloud cloud subsystem, and therefore is able to perform DSA enforcement. In that scenario, users from client applications request the pilot for images and reports and, provided that the corresponding DSAs allow it, the pilot must derive the requests to the aforementioned gateway. Moreover, the database of the pilot portal (public Cloud) stores all the user information other than images and reports in an encrypted bundle with its DSA, whereas the gateway acts as a data provider for the pilot, providing images and reports on demand. Last, the pilot is responsible of wrapping the DICOM objects within their DSAs, converting them into an encrypted object (a bundle of raw data) and sending them to the client.

Regarding the client side, users can access to the radiological portal through a Coco Cloud compliant application that implements the Coco Cloud client subsystem. The hospital systems administrator must previously register patients as users. In order to enable reports' disclosure to other patients, the involved patients must be previously included within the DSA agreement, by means of an optional clause, so that report's owner is able to allow or disallow other patients to access her or his report, whenever they are present in the DSA agreement as trusted patients for disclosure.

In order to guarantee DSA enforcement anytime, the pilot functionalities from the client side will be only available when it is online. In addition, for export purposes, the user must specify her or his intentions about the report that s/he is trying to export, being necessary to indicate the reason of its exportation, either to provide healthcare services or to perform research activities. Once the pilot receives an export request, the DSA enforcement subsystem will check the related agreements and, if DSA compliant, it will allow the user to export the report (i.e. the agreement explicitly establishes that the owner allows export for specific purposes, such as providing healthcare, doing research activities or extracting statistical data).

4.3.2. Coco Cloud Platform services to be used in the Pilot

The main Coco Cloud platform services required by the Health pilot are those related to the DSA enforcement, which must apply to different stages along the pilot workflow. When the users interact with the Health pilot, the DSA enforcement subsystem must check the user permissions according to the signed agreement. Figure 6 illustrates this workflow.

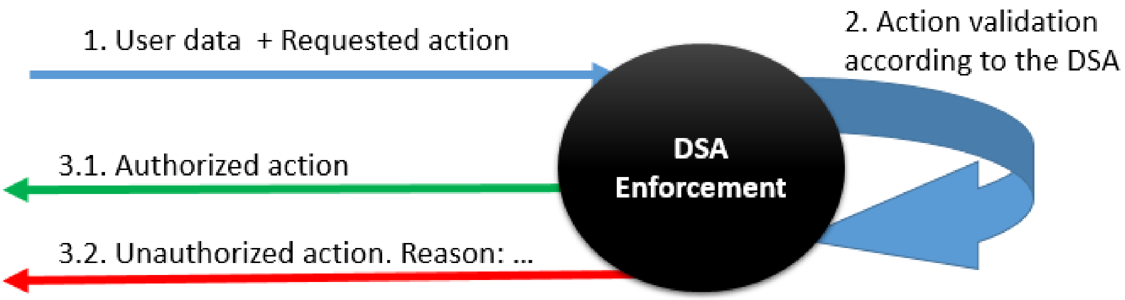

1. User data + Requested action
2. Action validation according to the DSA
DSA Enforcement
3.1. Authorized action
3.2. Unauthorized action. Reason: ...

Figure 6: **DSA Enforcement lifecycle: An incoming petition reaches the DSA Enforcement subsystem with information about the user and her or his requested action (1). The subsystem checks the action and validates it according to the petitioner's permissions specified on the DSA clauses (2). Finally, the DSA Enforcement responds either allowing the user to continue with her or his action (3.1) or avoiding it due to incompatible DSA clauses, in whose case it must return an explanation message (3.2)**.

As Figure 5 shows, each public entry point of the system (the pilot on the public Cloud and the client devices) must be Coco Cloud compliant and therefore able to perform DSA enforcements. Specifically, the public Cloud requires a Coco Cloud cloud subsystem and every client must be a Coco Cloud-enabled application, meaning that such clients must include the Coco Cloud client library.

4.3.3. Software Components for the pilot

This section will define all the necessary components and subcomponents to be developed (or re-used) for the implementation of the Health pilot. The aim is to establish a final definition of all the pilot components and its relations. Initially, the following components are proposed:

Component (Location)	Description	Available technologies	Lead developer
PACS (Private Cloud)	A PACS is necessary to provide a standardised source of DICOM objects (DICOM images and reports). For the proof of concept, a PACS including only dummy images and reports (non-personal data) will be used. Further deployment stages of the pilot will be based on images of real patients.	DCM4CHEE[1] (Java), running on a JBoss[2] server with a MySQL database OpenStack™ Dedicated DSL and server/s	GHQ
Coco Cloud gateway (Hospital gateway)	This component will connect the portal application located in the public Cloud to the PACS private Cloud, keeping separated the current radiological workflow of the pilot project, and ensuring all security and privacy enforcements. Functionalities: • Secure connection • Authorised access control • Anonymisation process • Query/retrieve on the PACS to provide images to the portal • Data encryption • Data transfer	SSL-VPN connection Java: • Web Service / RESTful entry point (to attend incoming petition) • Query engine (Generates the PACS query from the requested action) OpenStack™	GHQ ATOS
Portal administration database (Public Cloud)	Database, including the portal data: • User profile data: ID, name, surname, address, e-mail • Report annotations • Messages • Alerts • System logs	A suitable database for the OpenStack™ Framework (SQL Server, Oracle, MySQL, PostgreSQL, DB2, Non-relational, …) OpenStack™	ATOS GHQ Other partners (*DSA Enforcement, if the database requires a special treatment to store data as Coco Cloud objects*)
Radiological Portal	The pilot application itself placed on the public Cloud.	Java:	ATOS

[1] http://www.dcm4che.org/

[2] http://www.jboss.org/

Component (Location)	Description	Available technologies	Lead developer
(Public Cloud)	Functionalities: • User authentication • DSA enforcement • Information management (messages, alerts and annotations over images or reports) • DICOM object provider (View and export) • Edition of optional clauses in the DSA (to allow Disclose/"Un-disclose" reports) • User and system management • Statistics • Audit management	• Web Service / RESTful entry point (to attend incoming petition) • Client interfaces (mobile device app and web app) DSA Enforcement OpenStack™	GHQ Other partners (*DSA Enforcement*)
Client Coco-Cloud-enabled application	The client application that allows users to access the radiological portal. Functionalities: • User authentication • Profile management • View reports • Disclose/"Undisclose" reports • Export report to local device • Message management • Alert management	Java Applet for web browsers Android application for mobile devices Coco Cloud client	ATOS Other partners (*Coco Cloud client*)
System audit (All locations)	Software tools to audit all the system components	Java (log4j, slf4j, ...) Secondary database for audit information	ATOS

4.4. *Evaluation Framework and Success Criteria*

4.4.1. Pilot Participants

4.4.1.1. Target Groups

Target group	Target group members
Core target (audience to be reached in priority)	Patients and doctors as individuals, Cloud providers and GHQ itself as organisations.
Primary stakeholders (stakeholders that could be interested in the pilot)	Hospitals not belonging to GHQ as organisations and doctors who do not work at GHQ, as well as patients who potentially could go to any hospital, belonging to GHQ or not, as individuals.
Secondary stakeholders (prescribers and opinion leaders)	Specialised or general public press, scientific divulgation journals, lawyers specialised in data protection and in particular in sensitive data, in a digital context, as well as more generally lawyers specialised in ICT (TMT).

Table 1: Target group definitions for user engagement strategy

4.4.1.2. Benefits for stakeholders and users

Target group	Target group members
Core target (audience to be reached in priority)	The benefits for the patient are: • The patient is more autonomous, as s/he becomes more responsible and gets more involved in her or his healthcare, by having a more important role in the clinical workflows; • The patient can access her or his radiological reports and images in a fast, secure and ubiquitous way, by using the Cloud and the Internet infrastructures;

	• The patient will avoid unnecessary timeouts and visits to the hospital to collect the results. The benefits for the doctor are: • The portal allows doctors to easily disclose a patient’s case to other doctors, in order to get a second opinion, as well as to have an easier access to the patients’ reports through the Internet (i.e. remote access). The benefits for the hospital are: • The hospital will reduce costs by avoiding hardcopies of the reports and the images; • The hospital can dedicate the administrative resources to other tasks instead of handing reports, such as better patient attention in the reception section; • Queues are reduced at the hospital, meaning less timeouts for the radiology department; • The hospital will get the patient to participate more actively in his healthcare cycle, thus increasing patient trust and fidelity; • The hospital will become more competitive in offering healthcare services. And other common benefits are: • A bi-directional communication system is available to the patient, so that he/she can send and receive messages either from the portal administrator or the doctors; • The system allows the disclosure of information to third-parties, including other doctors and non-doctor users, such as family members or caregivers. The benefits for the Cloud provider are: • Offer hosting services and infrastructures to the hospital.
Primary stakeholders (stakeholders that could be interested in the pilot)	The benefits for the patient who goes to any hospital are: • The patient has available his/her medical images and reports anywhere, avoiding repetition of studies. The benefits for the doctor who does not work in GHQ are: • As immediate benefit, the doctor can access the most recent medical images and reports of the patient, if such patient comes from a GHQ hospital. Furthermore, the doctor can have the same advantages as a doctor from GHQ, if his/her reference hospital adopts the pilot product.

	The benefits for a hospital not belonging to GHQ are: • It can be interested in having the same benefits as a hospital belonging to GHQ. To achieve this, the hospital can buy the pilot product and then configure it with its infrastructure.
Secondary stakeholders (prescribers and opinion leaders)	Scientific journals: As a novel system able to share sensitive information across the Internet and improve the care quality of the patient, it can be an interesting challenge for the scientific scope. Specifically, a quantitative and qualitative study showing how the pilot improves the care quality of the patient could be highly interesting for the scientific community. Lawyers specialised in data protection and in particular in sensitive data, in a digital context, as well as more generally lawyers specialised in ICT (TMT): Due to the ability of the system to share highly sensitive data across the Internet and to store them on Cloud systems, ubiquitous and delocalized, being at the same time compliant with the current legislation, the pilot has a strong interest for lawyers specialized in digital offenses and sensitive data protection. Press notes: As a novel system intended to improve the care quality of the patient, specialised or general press can be interested in publishing about the pilot working in its production environment.

Table 2: Benefits per target group

4.4.2. GQM for Health Pilot

Goals		
ID	Name	Description
WP7-HE-Gol-1	View reports.	Medical information exchange between doctors and patients, in particular in the radiologic specialty. The “Patient and doctor portal” will enable a straightforward connection to the Hospital Cloud infrastructure by offering itself as a new service of medical imaging diagnosis and follow-up.
WP7-HE-Gol-2	Disclose patient profile to another patient user.	There are some situations when a patient needs to grant permissions to another non-doctor user (like a family member or a caregiver) to allow him/her access his/her profile and manage his/her alerts and healthcare messages, either because of surgery rehabilitation or because of a disability, for example. There are three available access permission levels: access denied (default), read-only, and read/write permissions. Thus,

		by default any patient cannot access another patient's profile, and patients with others types of permissions must be specifically declared by the profile owner.
WP7-HE-Gol-3.1	Invite another doctor to view a given profile and get a second opinion.	When a doctor has doubts about the diagnosis of a report/image acquisition, he/she can invite another doctor through the "Patient and doctor portal" to ask for a second opinion. Nevertheless, the second doctor must be authorised by the patient to access his/her profile, thus if the patient never has authorised that doctor previously, a request for access is sent to the patient in order to authorise the second doctor to access that patient profile.
WP7-HE-Gol-3.2	Ask patient for access permission.	When a doctor has to treat a patient for the first time, usually the patient will have this doctor as unauthorized to access his/her profile by default. Therefore, that doctor can send a request for access to the patient asking him/her for authorization to access his/her profile.
WP7-HE-Gol-4	Message management.	When a patient has any question about the information in a report, he/she can contact the doctor via a messaging system, built into the app. On the other hand, a doctor can contact a patient in order to ask any relevant information involved in the diagnosis discussion.
WP7-HE-Gol-5	Alert management.	When a user (patient or doctor) experiments any technical incident within the "Patient and doctor portal", he/she can contact the administrator via an alert messaging system, built into the app. Further, the administrator can notify users when a given technical incident has been corrected.
WP7-HE-Gol-6	Patient privacy protection.	Patients can choose to hide some reports and conversation threads of alerts or messages, meaning that no one else can access such study thereafter (either authorized or/and unauthorized persons).
WP7-HE-Gol-7	User authentication.	The user (patient or doctor) is unequivocally identified in the portal by means of control access policies (credentials and digital certificates, if possible).
WP7-HE-Gol-8	Audit.	Audit accesses and operations.
WP7-HE-Gol-9	Communication channel protection.	All electronic communications involving sensitive data must be protected.
WP7-HE-Gol-10	Data protection at-rest.	Personal data, including sensitive data, at-rest in the public Cloud must remain encrypted.

Questions		
ID	Name	Description
WP7-HE-Que-1 (WP7-HE-Gol-1)	View reports.	Can users access medical images and reports across the Internet, if they have enough permission?
WP7-HE-Que-2 (WP7-HE-Gol-2)	Disclose patient profile to another patient user.	Can users choose with whom they want to share their profile?
WP7-HE-Que-3.1 (WP7-HE-Gol-3.1)	Grant doctor to view a given patient profile.	Can doctors grant temporal access to users' data to other doctors?
WP7-HE-Que-3.2 (WP7-HE-Gol-3.2)	Ask patient for access permission.	Can doctors ask patients to get access permission?
WP7-HE-Que-4 (WP7-HE-Gol-4)	Message management.	Can users send and receive messages between them?
WP7-HE-Que-5 (WP7-HE-Gol-5)	Alert management.	Can users send alerts about incidents to the technical staff?
WP7-HE-Que-6 (WP7-HE-Gol-6)	Patient privacy protection.	Are cautions taken to protect patient privacy?
WP7-HE-Que-7 (WP7-HE-Gol-7)	User authentication.	Is the user authentication secure enough to protect the patient profile?
WP7-HE-Que-8 (WP7-HE-Gol-8)	Monitoring.	Is there enough information in the audit track to reproduce any use case previously executed?
WP7-HE-Que-9 (WP7-HE-Gol-9)	Communication channel protection.	About the encryption to protect the channel, is it considered strong enough to transport highly sensitive data (i.e. assessed by an expert)?
WP7-HE-Que-10 (WP7-HE-Gol-10)	Data protection at-rest.	Are the data at-rest protected?

Metrics		
ID	Name	Description
WP7-HE-Met-1 (WP7-HE-Que-1)	View reports – successful rate	Number of users who can access medical images and reports / Number of users who try to access medical images and reports.
WP7-HE-Met-2 (WP7-HE-Que-2)	Disclose patient profile to another patient user – successful rate	Number of users who can choose with whom they want to share their profile / Number of users who try to choose with whom they want to share their profile.
WP7-HE-Met-3.1 (WP7-HE-Que-3.1)	Doctor grants access permissions to user' data – successful rate	Number of doctors who can invite other doctors to get a second opinion / Number of doctors who try to invite other doctors to get a second opinion.
WP7-HE-Met-3.2 (WP7-HE-Que-3.2)	Ask patient for access permission	Number of doctors who can ask patient for access permission / Number of doctors who try to ask patient for access permission.
WP7-HE-Met-4 (WP7-HE-Que-4)	Message management – successful rate	Number of messages successfully sent / Number of tries.
WP7-HE-Met-5 (WP7-HE-Que-5)	Alert management – successful rate	Number of alerts successfully sent / Number of tries.
WP7-HE-Met-6 (WP7-HE-Que-6)	Patient privacy protection – vulnerability rate	A security expert will assess if there are any potential vulnerabilities.
WP7-HE-Met-7 (WP7-HE-Que-7)	User authentication – security rate	A security expert will assess if there are any potential vulnerabilities in the authentication process.
WP7-HE-Met-8 (WP7-HE-Que-8)	Audit – replicability rate	Simulate different use cases in order to check if all of them have been monitored properly. Assess the ability of the monitoring system according to: Number of use cases that can be identically replicated starting from the monitored log information / Number of attempts of use case replication.
WP7-HE-Met-9 (WP7-HE-Que-9)	Communication channel protection – strength rate	A security expert will assess if there are any potential vulnerabilities in the encrypted channel.
WP7-HE-Met-10 (WP7-HE-Que-10)	Data protection at-rest – Cloud security rate	A Cloud expert will assess several Cloud provider alternatives according to the available security offers.

Mapping among Goals, Question, Metrics		
Goal	Question	Metric
WP7-HE-Gol-1	WP7-HE-Que-1	WP7-HE-Met-1
WP7-HE-Gol-2	WP7-HE-Que-2	WP7-HE-Met-2
WP7-HE-Gol-3.1	WP7-HE-Que-3.1	WP7-HE-Met-3.1
WP7-HE-Gol-3.2	WP7-HE-Que-3.2	WP7-HE-Met-3.2
WP7-HE-Gol-4	WP7-HE-Que-4	WP7-HE-Met-4
WP7-HE-Gol-5	WP7-HE-Que-5	WP7-HE-Met-5
WP7-HE-Gol-6	WP7-HE-Que-6	WP7-HE-Met-6
WP7-HE-Gol-7	WP7-HE-Que-7	WP7-HE-Met-7
WP7-HE-Gol-8	WP7-HE-Que-8	WP7-HE-Met-8
WP7-HE-Gol-9	WP7-HE-Que-9	WP7-HE-Met-9
WP7-HE-Gol-10	WP7-HE-Que-10	WP7-HE-Met-10

4.4.3. Common Technical Criteria

In order to establish a set of quality values for each metric, a threshold is defined for each one. The rates above the threshold are considered appropriate and indicate a successful result of the metric. Note that each threshold is a ratio between the number of metrics performed successfully and the total number of metrics that have been attempted (successfully or unsuccessfully), as described in the metrics table.

Common Technical Criteria		
ID	Name	Threshold
WP7-HE-Met-1	View reports – successful rate	0.9
WP7-HE-Met-2	Disclose patient profile to another patient user – successful rate	0.9
WP7-HE-Met-3.1	Doctor grants access permissions to user' data – successful rate	0.9
WP7-HE-Met-3.2	Ask patient for access permission – successful rate	0.9
WP7-HE-Met-4	Message management – successful rate	0.9
WP7-HE-Met-5	Alert management – successful rate	0.9
WP7-HE-Met-6	Patient privacy protection – vulnerability rate	N/A
WP7-HE-Met-7	User authentication – security rate	N/A
WP7-HE-Met-8	Audit – replicability rate	1
WP7-HE-Met-9	Communication channel protection – strength rate	N/A
WP7-HE-Met-10	Data protection at-rest – Cloud security rate	N/A

4.4.4. Measurement and Analysis of Results

In this section the score of each metric related to the rating system is established, as well as the minimum number of attempts that must be executed in order to assume a given use case as enough tested.

The measurement and interpretation of those metrics will result in the calculation of percentages values. As established on the previous table, higher values than 0.9 are desirable for each metric. The number of attempts will be defined according to the variability of the metrics. As an indicative minimum number, 10 attempts or replications are suggested.

In case of qualitative metrics (those metrics based on expert assessments, i.e. WP7-HE-Met-6, WP7-HE-Met-7, WP7-HE-Met-9, WP7-HE-Met-10), the experts analysis will be used as bases for the interpretation of the results.

4.5. *Schedule of activities and provisional time plan*

The following table shows the relation between milestones, deliverables and the scheduled activities so far.

Scheduled activities		
Milestone	Deliverable	Activities
MS5 First version of the overall Coco Cloud architecture, DSA and Enforcement Infrastructure [month 12]	D7.2) Design of the Pilot Products – First Release: [month 12]	• Finalise the architecture design as well as the analysis of goals, functionalities and requirements. • Ensure that the requirements are aligned with the proposed architecture design. • Establishment of the metrics to evaluate the pilot results.
MS9 First Version of integrated Coco Cloud + Test-bed and Pilots [month 24]	D7.4) Pilot Product for Health: [month 24]	• Development stage. Preliminary versions of all components defined in the pilot specifications must be ready.
MS13 First Validation of the Pilots [month 26]	D7.6) First Test Plan & Evaluation of Pilot Products: [month 26]	• Development stage ongoing. Refinement of the pilot components. • Issue the first test plan and preliminary evaluations of the pilots in the development environment.
MS14 Final Version of integrated infrastructure +Test-bed and Pilot [month 34]	D7.7) Final Pilot Products [month 36]	• Development stage ongoing. Refinement of the pilot components. • Integration of the pilot products with the test-bed. • First test and validations of the pilot within the test environment.
MS15 Final Validation of the Pilots [month 36]	D7.8) Revised Test Plan & Evaluation of Pilot Products [month 36]	• Finalisation of the development stage. • Final evaluation and validation of the pilots in production environment.

5. Mobile Pilot

5.1. Overall Pilot scope

Digital contents are at the heart of the majority of business transactions and operations nowadays. They have become a crucial asset that companies need to protect, but meeting at the same time operational and security needs. If we also consider that many information flows are global and in real time, we may understand the reason of the popularity of Cloud file sharing tools (public or private) and associated mobile apps.

In fact, sensitive corporate data stored in private or even public Clouds are more and more consumed by corporate employees through their mobile devices. Such data comprises working documents, mails, etc., up to analytics on-demand software and live reports from business data generated remotely on-the-fly (e.g. SAP BO analytics applications for mobile and tablets).

In order to protect the confidential documents, companies usually resort to using specific security policies, to which the employees have to adhere. These policies are written in natural language, and as such, they are not suitable for being automatically enforced. Beside the mandatory access control and authorisation checks that must be performed by an application before giving access to confidential data, there are several other security constraints that must be fulfilled.

The objective of the mobile pilot is to focus on an additional functionality that targets many existing and currently adopted business workflows and applications: the compliant consumption of sensitive and confidential digital contents. In this way, the Coco Cloud contributions can be demonstrated in a business-relevant use case that is also close to existing solutions; thus easing the demonstration of their advantages and maximising their potential uptake. To this end, this pilot demonstrates the interaction Cloud-mobile as notable information flow, using an architecture pattern easily applicable to other contexts and solutions.

In particular, the definition of the main goals of the pilot follows these objectives:

- **WP7-MO-Gol-1**: Allow compliant (corporate) information consumption on mobile devices.
- **WP7-MO-Gol-2**: Permit information sharing operations on the Cloud.
- **WP7-MO-Gol-3**: Definition of machine-understandable confidentiality policies.

Many software products available on the market include requirements similar to WP7-MO-Gol-1 and WP7-MO-Gol-2. This consideration leads to the identification of a twofold strategy for the development of the pilot: demonstrating important Coco Cloud functionalities, as well as supporting dissemination and exploitation actions through the availability of a concrete and validated usage scenario.

WP7-MO-Gol-3 is functional to supporting the enforcement of resource policies, as well as their visualisation to end-users. This will permit to pilot applications to design a pleasant user experience by explaining the contents of data policies during their enforcement, thus easing their acceptance by end-users, and the legal compliance of key legal principles, such as transparency, consent and common will of parties in a contractual relationship.

5.2. Requirement Analysis Overview

The requirements elicited for this pilot identify concretely a minimal set of characteristics for the functionalities in the pilot scope. With this respect, the functional, privacy, security and data usage requirements are addressed by the pilot architecture, detailed in the next section. With respect to the performance requirements, they have mostly to be addressed during the implementation phase with finer-grained analysis thus they will be addressed later on in the pilot development phase.

Functional requirements

- **WP7-MO-Fun-1:** The scenario must have Cloud file sharing service functionalities.
    - Goal addressed: WP7-MO-Gol-2
- **WP7-MO-Fun-2:** The scenario must have download of Cloud-stored files functionalities.
    - Goal addressed: WP7-MO-Gol-1
- **WP7-MO-Fun-3:** The scenario must have a support for data access on mobile devices (and in disconnected scenarios).
    - Goal addressed: WP7-MO-Gol-1
- **WP7-MO-Fun-4:** The scenario must have a support for compliant data usage on mobile devices (and in disconnected scenarios).
    - Goal addressed: WP7-MO-Gol-1

Privacy requirements

- **WP7-MO-Pri-1:** The scenario must have personal data protection.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Pri-2:** The scenario must have the possibility to express data sharing conditions and obligations.
    - Goals addressed: WP7-MO-Gol-1. WP7-MO-Gol-2, WP7-MO-Gol-3
- **WP7-MO-Pri-3**: The scenario must have corporate data protection.
    - Goal addressed: WP7-MO-Gol-3

Security requirements

- **WP7-MO-Sec-1:** The scenario must have Access Control capabilities.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Sec-2:** The scenario should have Accountability & Compliance capabilities.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Sec-3:** The scenario must have Authentication capabilities.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Sec-4:** The scenario must have Data Confidentiality in-transit.
    - WP7-MO-Gol-1, WP7-MO-Gol-2

- **WP7-MO-Sec-5:** The scenario must have Data Confidentiality at-rest.
    - WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Sec-6:** The scenario should have Availability for resources and their policies.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2, WP7-MO-Gol-3
- **WP7-MO-Sec-7:** The scenario must have Integrity for resources and their policies.
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2, WP7-MO-Gol-3

Data usage requirements

- **WP7-MO-Dus-1:** The scenario must have Usage Control enforcement capabilities on mobile devices.
    - Goals addressed WP7-MO-Gol-1, WP7-MO-Gol-2
- **WP7-MO-Dus-2:** The scenario must have context-aware usage control directives (e.g. conditions and obligations).
    - Goals addressed: WP7-MO-Gol-1, WP7-MO-Gol-2

Performance requirements

- **WP7-MO-Per-1:** The scenario should have effective mobile policy enforcement performances.
    - Goals affected: WP7-MO-Gol-1
- **WP7-MO-Per-2:** The scenario should have effective energy consumption performances.
    - Goals affected: WP7-MO-Gol-1
- **WP7-MO-Per-3:** The scenario should have encryption algorithms optimised for their usage in mobility.
    - Goals affected: WP7-MO-Gol-1

5.3. *Pilot Specific Architecture*

5.3.1. General Pilot Architecture

The Mobile Pilot architecture can be depicted as in the following figure:

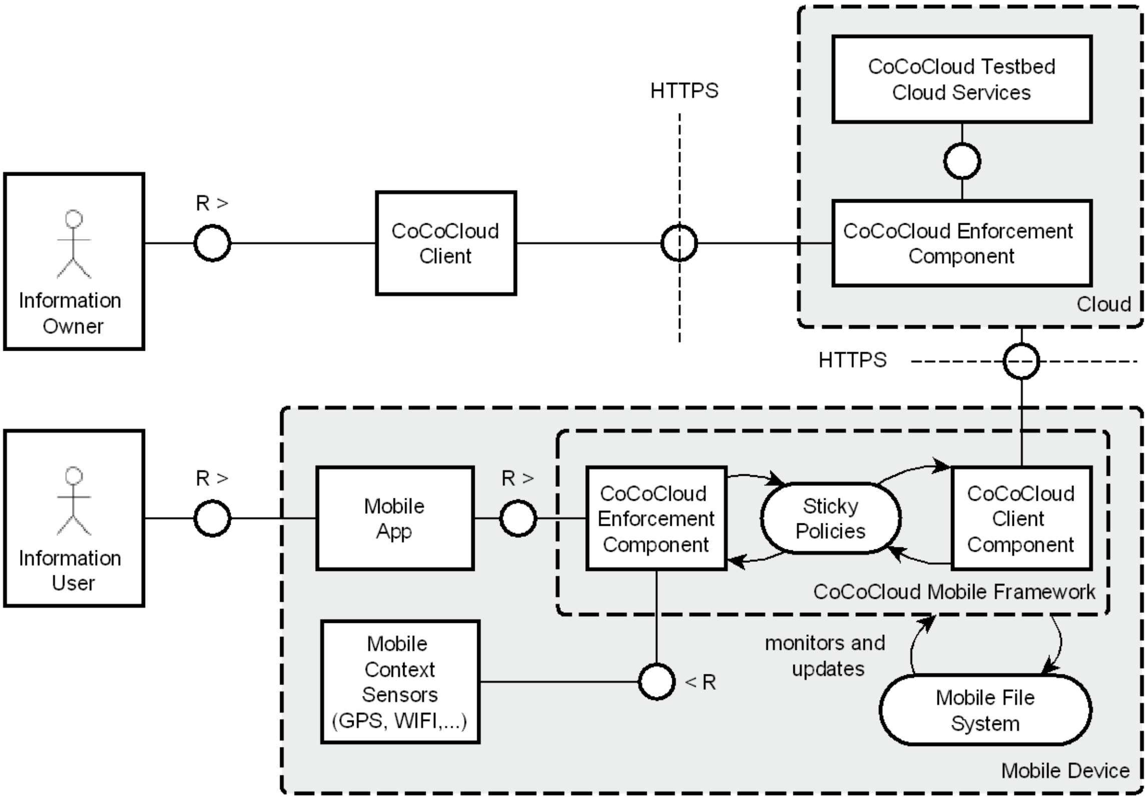

CoCoCloud Testbed Cloud Services
HTTPS
R >
CoCoCloud Client
CoCoCloud Enforcement Component
Information Owner
Cloud
HTTPS
R >
Mobile App
R >
CoCoCloud Enforcement Component
Sticky Policies
CoCoCloud Client Component
Information User
CoCoCloud Mobile Framework
Mobile Context Sensors (GPS, WIFI,...)
< R
monitors and updates
Mobile File System
Mobile Device

Figure 7: Mobile Pilot General Architecture

The Information Owner can create and distribute new pieces of information for corporate Information Users, using Coco Cloud components, in particular the file sharing facilities. The Test-bed facilities can be used for implementing the Mobile pilot requirements. This operation necessarily requires the specification of which Corporate DSA/Sticky Policy[3] must be associated to each new piece of information. The components responsible for the creation of the various Corporate DSAs are not shown in Figure 2, but in principle, they would not deviate from the standard DSA tools offered by Coco Cloud.

Information Users can consume corporate pieces of information through their mobile phones. Specific Coco Cloud-enabled apps (like for instance a file manager, a PDF viewer and so on) can interact with the Coco Cloud mobile components for accessing and consuming Coco Cloud-protected resources.

The Coco Cloud mobile components are responsible for verifying access conditions and usage control prescriptions, along the utilisation of protected contents. They will make use of physical position detection systems (GPS, Wi-Fi, Bluetooth) and any other means to enforce and fulfil prescriptions and obligations stated by the Sticky Policy associated to each protected content.

[3] Sticky Policy concept is detailed in deliverable D5.1

The described high-level architecture could be complemented by mobile-specific identity management services, if available.

The mobile pilot and its usage of Coco Cloud contributions can be divided in two main parts:

- Information Creation.
- Information Consumption.

Figure 8 depicts an activity diagram associated to the Information Creation part.

The Corporate Policy Officer is entitled to the definition of corporate-wide information classification levels and associated DSAs. To perform this activity, standard DSA authoring tools will be used.

The Information Owner can make use of DSAs and associated Sticky Policies at the creation of new contents. In particular, such contents will be uploaded on a Cloud infrastructure protected by Coco Cloud contributions, together with their DSA/Sticky Policy following the information classification guidelines.

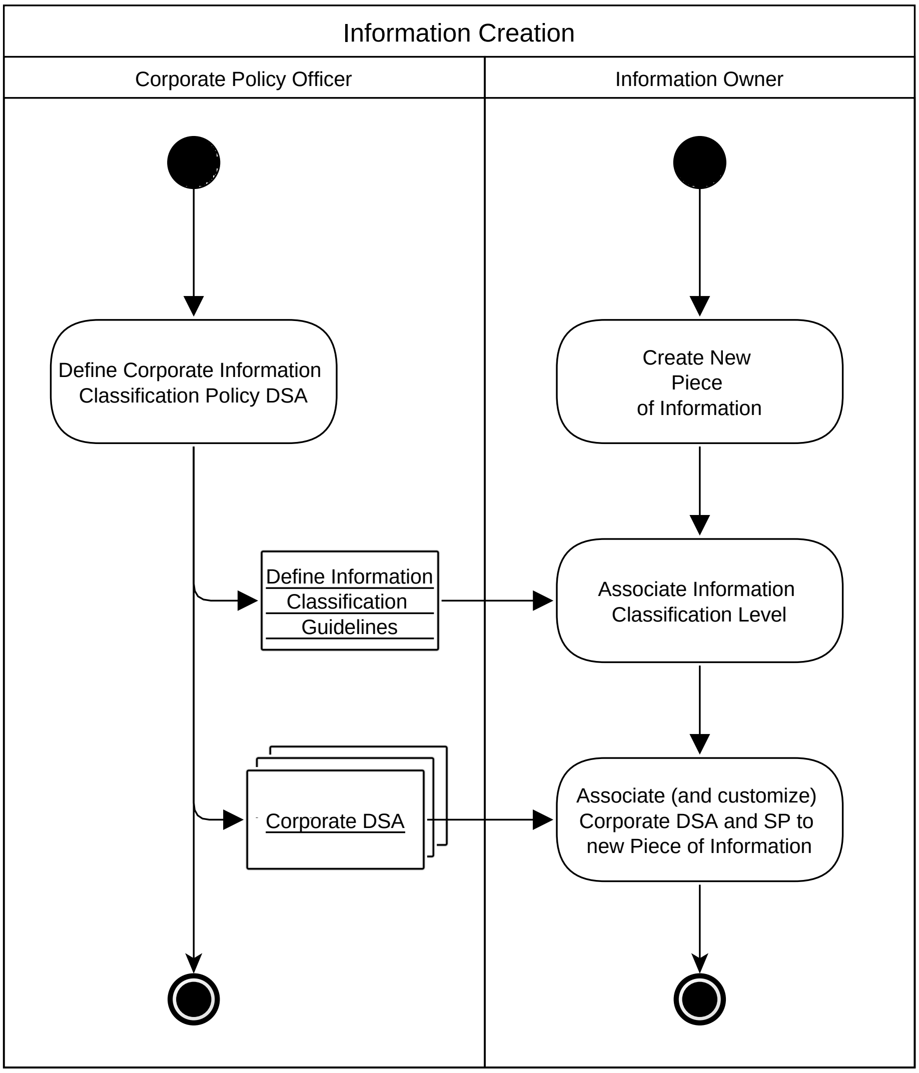

Information Creation
Corporate Policy Officer
Information Owner
Define Corporate Information Classification Policy DSA
Create New Piece of Information
Define Information Classification Guidelines
Associate Information Classification Level
Corporate DSA
Associate (and customize) Corporate DSA and SP to new Piece of Information

Figure 8: A UML activity diagram for information creation (comprising the association with security policy)

The Information Consumption is illustrated in the following Figure 9.

An Information User requests access to a piece of information through a mobile app that integrates with the Coco Cloud framework. The app (a file manager or a PDF viewer) can also possibly create a request for a Cloud-hosted resource, mediated by the Coco Cloud mobile components. In this latter case, the Coco Cloud cloud component receives a resource request on behalf of the Information User.

On the Cloud side, the Coco Cloud components (and in particular the Cloud enforcement engine) verify the resource-specific access and usage control conditions, and grants to the Coco Cloud mobile components the access to the resource.

At that point, the mobile Coco Cloud components (and in particular the mobile enforcement engine) verifies once again the mobile-specific context attributes that are part of the Sticky Policy before granting to the app the access to the requested resource. While the app consumes the resource, the mobile Coco Cloud components monitor the usage conditions and implement the obligations prescribed in the sticky policy.

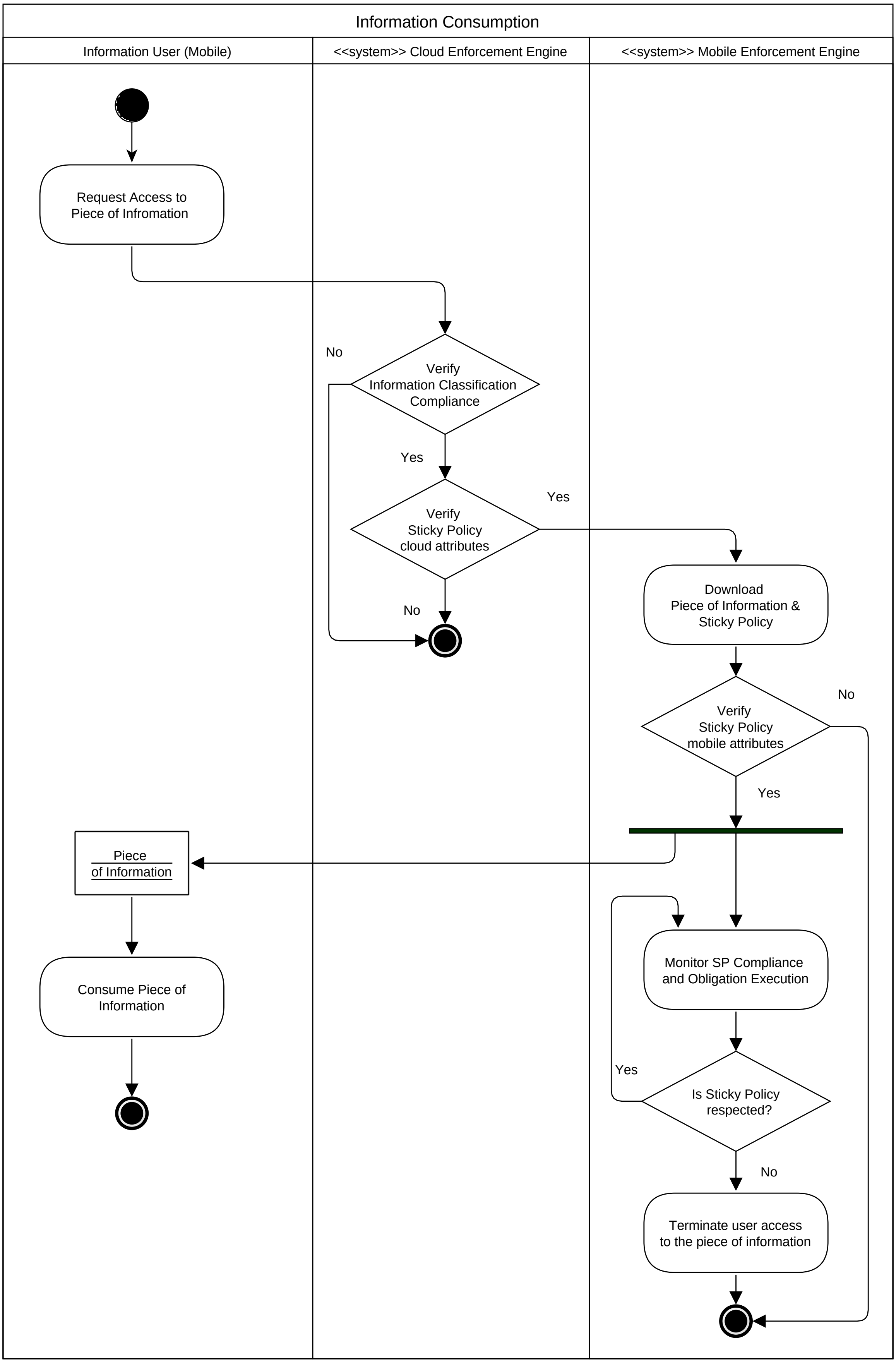

Information Consumption
Information User (Mobile)
<<system>> Cloud Enforcement Engine
<<system>> Mobile Enforcement Engine
Request Access to Piece of Infromation
No
Verify Information Classification Compliance
Yes
Yes
Verify Sticky Policy cloud attributes
No
Download Piece of Information & Sticky Policy
No
Verify Sticky Policy mobile attributes
Yes
Piece of Information
Monitor SP Compliance and Obligation Execution
Consume Piece of Information
Yes
Is Sticky Policy respected?
No
Terminate user access to the piece of information

Figure 9: A UML activity diagram for information consumption on mobile devices

5.3.2. Coco Cloud Platform services to be used in the Pilot

As illustrated in Figure 8 and Figure 9, the Mobile Pilot will make use of the following Coco Cloud services:

- Coco Cloud DSA authoring tool(s).
- Coco Cloud cloud enforcement infrastructure.
- Coco Cloud-enhanced Cloud storage.
- Coco Cloud mobile enforcement infrastructure.

5.3.3. Software Components for the pilot

The following software components (on top of Coco Cloud contributions mentioned in section 3.3.2) are foreseen, as part of the pilot architecture:

- Coco Cloud-enabled file manager mobile app.
- Coco Cloud-enabled PDF document viewer mobile app.

This minimal list of apps aims at demonstrating concretely a number of Coco Cloud functionalities, by means of software that is generally used in many business processes. Additional apps may be part of the pilot, if necessary for demonstrating the project's objectives.

5.4. Evaluation Framework and Success Criteria

5.4.1. Pilot Participants

5.4.1.1. Target Groups

Target group	Target group members
Core target (audience to be reached in priority)	A selection of SAP employees (identified as Information Users) will be involved in the pilot; they will be enabled to use specific app(s) for information distribution and compliant consumption.
Primary stakeholders (stakeholders that could be interested in the pilot)	Information owners of resources distributed to SAP employees, governance stakeholders (for example, roles similar to Corporate Policy Officer).
Secondary stakeholders (prescribers and opinion leaders)	Specialised press, business analysts, scientific divulgation journals.

Table 3: Target group definitions for user engagement strategy

5.4.1.2. Benefits for stakeholders and users

Target group	Target group members
Core target (audience to be reached in priority)	Information Users can access and consume information in a compliant way, thus relieving them from the possibility of causing data leaks or other forms of policy violations.
Primary stakeholders (stakeholders that could be interested in the pilot)	Information Owners can share their information in a simpler and more secure way: simpler, because Cloud file sharing services permit an easier access to pieces of information if compared to emails or traditional file shares on corporate servers; more secure, as access and usage control conditions can define and enforce more strictly how information is accessed and used. Corporate Policy Officers would benefit from a tighter control on pieces of information, which can be accessed and consumed through protective and accountable measures, thus preventing unintentional information leakage and supporting investigations in case of deliberate actions.
Secondary stakeholders (prescribers and opinion leaders)	Specialised press can be interested in novel methods for easing confidential and compliant information consumption of employees, as extending the technical means for enforcing confidentiality policies can have positive impact with respect to work organisation both for employees and at company scale. For similar reasons, business analysts can consider such new capabilities as a business-effective means to sustain and easing either top-down or bottom-up business information flows and collaboration also in internal social communities. Scientific journals can be interested in obtaining experience reports conducted in business environment (in vivo), to make comparison with theoretical results and controlled experiments (in vitro) existing in the literature.

Table 4: Benefits per target group

5.4.2. GQM for Mobile Pilot

Goals		
ID	Name	Description
WP7-MO-Gol-1	Allow compliant (corporate) information consumption on mobile devices from the point of view of information users.	Corporate employees need to be enabled to act as Information Users on pieces of information in accordance to data-specific corporate confidentiality policies.

		Data transfers to mobile devices must be secured due to the confidentiality of the exchanged information. Data-specific policies have to be transmitted in a secure way (thus preserving confidentiality, integrity and availability for offline usage).
WP7-MO-Gol-2	Permit information sharing operations on the Cloud from the point of view of information creators.	Confidential or non-public pieces of information have to be shared among corporate employees for pursuing company's business objectives. This means to have services that: - Accept and store pieces of information (for instance captured as files) sent by an Information Owner; - Permit Information Owners to assign confidentiality policies, access and usage control restrictions for their pieces of information. Such operations need to take place according to confidentiality policies that prescribe terms, guidelines and conditions for information consumption. It is necessary to have technical means to simplify information sharing operations compliant with confidentiality policies. Integrity and confidentiality have to be preserved, as well as the availability of both data and policies.
WP7-MO-Gol-3	Definition of machine-understandable confidentiality policies from the point of view of Corporate Policy Officer.	Corporate Policy Officer establishes the official confidentiality policies for a corporation. Such operation involves the consideration of legal requirements, in accordance with the contractual provisions in

		place and with the legal framework composed by the laws of countries where the corporation operates. Enabling a Corporate Policy Officer with the possibility to express confidentiality policies in natural language and to transform them in machine-understandable form allows for data sharing and consumption operations, whose policy compliance is machine-regulated and -verified.

Questions		
ID	Name	Description
WP7-MO-Que-1 (WP7-MO-Gol-1)	Resource type in final system.	Which resources can be consumed through the system, among those normally consumed?
WP7-MO-Que-2 (WP7-MO-Gol-1, WP7-MO-Gol-3)	Policy terms that are enforceable by Coco Cloud components on the mobile platform.	Which terms of corporate policies can be enforced automatically on mobile devices when using Coco Cloud?
WP7-MO-Que-3 (WP7-MO-Gol-1, WP7-MO-Gol-2, WP7-MO-Gol-3)	Pilot architecture modularity.	How modular is the final pilot architecture with respect to its adoption in existing products and solutions?
WP7-MO-Que-4 (WP7-MO-Gol-2)	Permit information sharing operations on the Cloud.	Which resources can be shared with colleagues using the system?
WP7-MO-Que-5 (WP7-MO-Gol-2, WP7-MO-Gol-3)	Policy terms that are enforceable by Coco Cloud components on the Cloud platform.	Which terms of corporate policy can be enforced automatically on the Cloud when using Coco Cloud?
WP7-MO-Que-6 (WP7-MO-Gol-3)	Definition of machine-understandable confidentiality policies.	Which terms of corporate policies can be described?
WP7-MO-Que-7 (WP7-MO-Gol-1, WP7-MO-Gol-2)	Adherence to requirements.	What is the adherence of the pilot implementation with respect to the elicited requirements (functional, security, data usage,

		performance)?

Metrics		
ID	Name	Description
WP7-MO-Met-1 (WP7-MO-Que-1)	Resource types	For all users: survey on most common resource types consumed on mobile.
WP7-MO-Met-2 (WP7-MO-Que-1)	Resource types more consumed in mobility	For each user: # resource types consumed through pilot / # resource types generally consumed on mobile.
WP7-MO-Met-3 (WP7-MO-Que-2)	Mobile-enforceable policy terms	For each policy: # mobile enforceable terms / # terms.
WP7-MO-Met-4 (WP7-MO-Que3)	Architecture modularity	Expert assessment from a sample of primary stakeholders.
WP7-MO-Met-5 (WP7-MO-Que-4)	Resource types stored on the Cloud	For all users: survey on most common resource sharing solutions (to the Cloud).
WP7-MO-Met-6 (WP7-MO-Que-4)	Support for the needed resource types	For each users: number of resource types shared through pilot / number of resource types generally shared.
WP7-MO-Met-7 (WP7-MO-Que-5)	Cloud-enforceable policy terms	For each policy: number of Cloud enforceable terms / number of terms.
WP7-MO-Met-8 (WP7-MO-Que-6)	Support for corporate policy terms	For each policy: number of terms digitally representable / number of terms.
WP7-MO-Met-9 (WP7-MO-Que-7)	Adherence of pilot to requirements	Expert assessment from a sample of primary stakeholders.

Mapping among Goals, Question, Metrics		
Goal	Question	Metric
WP7-MO-Gol-1	WP7-MO-Que-1	WP7-MO-Met-1
WP7-MO-Gol-1	WP7-MO-Que-1	WP7-MO-Met-2
WP7-MO-Gol-1, WP7-MO-Gol-3	WP7-MO-Que-2	WP7-MO-Met-3
WP7-MO-Gol-1, WP7-MO-Gol-2, WP7-MO-Gol-3	WP7-MO-Que3	WP7-MO-Met-4
WP7-MO-Gol-2	WP7-MO-Que-4	WP7-MO-Met-5
WP7-MO-Gol-2	WP7-MO-Que-4	WP7-MO-Met-6
WP7-MO-Gol-2, WP7-MO-Gol-3	WP7-MO-Que-5	WP7-MO-Met-7
WP7-MO-Gol-3	WP7-MO-Que-6	WP7-MO-Met-8
WP7-MO-Gol-1, WP7-MO-Gol-2	WP7-MO-Que-7	WP7-MO-Met-9

5.4.3. Common Technical Criteria

The majority of the metrics previously defined deals with objective characteristics, generally expressed as percentages: for instance, WP7-MO-Met-7 has to be computed for each policy, evaluating the number of terms digitally representable divided by the number of terms.

There are two other forms of metrics being considered: surveys and expert assessment.

Surveys will involve pilot's users, essentially to evaluate objectively whether there are business operations on common resource types that are not supported by the pilot infrastructure.

Expert assessments will involve senior software architects or management with a good knowledge of market products and solutions, in order to receive also valuable feedback in the light of easing exploitation activities of pilot results.

5.4.4. Measurement and Analysis of Results

The measurement and interpretation of all the previous metrics will be developed as follows.

A majority of metrics result in the calculation of percentage values. Indicatively, higher values (>=75%) are desirable for each metric. However, there are cases where a quantitative assessment could not be sufficient to provide exhaustive answers to the associated question(s): for example, considering WP7-MO-Met-7, there could be just few terms that are not digitally representable, but their importance can be crucial for the pilot development. Therefore, during the analysis phase all metrics will be evaluated in-context, thus to provide also a qualitative perspective to their interpretation.

With respect to surveys (WP7-MO-Met-1 and WP7-MO-Met-5), their results will be used in order to provide an interpretation context to other metrics and to qualitative considerations.

Considering expert assessments, they will be gathered in the form of statements and used in the interpretation of the associated questions.

5.5. *Schedule of activities and provisional time plan*

Scheduled activities		
Milestone	**Deliverable**	**Activities**
MS5 First version of the overall Coco Cloud architecture, DSA and Enforcement Infrastructure [month 12]	D7.2) Design of the Pilot Products – First Release: [month 12]	• Finalise the architecture design as well as the analysis of goals, functionalities and requirements. • Ensure that the requirements are aligned with the proposed architecture design. • Establishment of the metrics to evaluate the pilot results.
MS9 First Version of integrated Coco Cloud + Test-bed and Pilots [month 24]	D7.5) Pilot Product for Mobile: [month 24]	• Development stage. Preliminary versions of all components defined in the pilot specifications must be ready.
MS13 First Validation of the Pilots [month 26]	D7.6) First Test Plan & Evaluation of Pilot Products: [month 26]	• Development stage ongoing. Refinement of the pilot components. • Preliminary evaluations of the pilots in the development environment.
MS14 Final Version of integrated infrastructure +Test-bed and Pilot [month 34]	D7.7) Final Pilot Products [month 36]	• Development stage ongoing. Refinement of the pilot components. • Integration of the pilot products with the test-bed. • First test and validations of the pilot within the test environment.
MS15 Final Validation of the Pilots [month 36]	D7.8) Revised Test Plan & Evaluation of Pilot Products [month 36]	• Finalisation of the development stage. • Final evaluation and validation of the pilots in production environment.

6. References

1 Coco Cloud D7.1 – Definition of Pilot Requirements

2 Coco Cloud D3.2 – First Version of Coco Cloud Architecture

3 Coco Cloud D4.1 – DSA specifications, methodologies and techniques

4 J. Heide and M.V. Pedersen and F.H.P. Fitzek and T. Larsen. Chapter in *Network Coding in the Real World* (p. 87-114).Academic Press, 2011.

5 V. Basili, G. Caldera, and H.D. Rombach. *The Goal Question Metric Approach.* Encyclopaedia of Software Engineering – Volume 2, John Wiley & Sons, Inc., 1994.

6 V. Basili and D. Weiss. *A Methodology for Collecting Valid Software Engineering Data.* IEEE Trans. Software Eng., 1984.

7 V. Basili and H.D. Rombach. *The TAME Project: Towards Improvement-Oriented Software Environments.* IEEE Trans. Software Eng., 1988.

8 F. Latum, R. Solingen, M. Oivo, B. Hoisl, H.D. Rombach, and G. Ruhe. *Adopting GQM-Based Measurement in an Industrial Environment.* IEEE Trans. Software Eng., 1998.

9 L. Briand, C. Differding, and H.D. Rombach. *Practical Guidelines for Measurement-Based Process Improvement.* Software Process Improvement and Practice Journal, 1997.

10 Spanish ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data, implemented by the ROYAL DECREE 1720/2007 of 21 December.

11 DICOM Standard: Digital Imaging and Communications in Medicine. http://dicom.nema.org/ - Accessed on October 29, 2014.

12 NEMA: National Electrical Manufacturers Association. http://www.nema.org/ - Accessed on October 29, 2014.