# Coco Cloud Project Overview

Aljosa Pasic
Atos Spain

# Mission

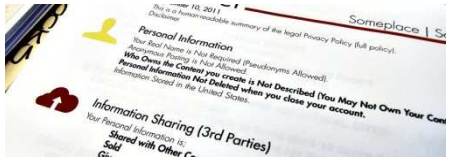
*"Seamless **compliance and confidentiality** for **data** shared in the **cloud** and **mobile** services, aligned to **agreements** considering **legal**, **business**, **organizational regulations** and **user** defined **preferences.**"*

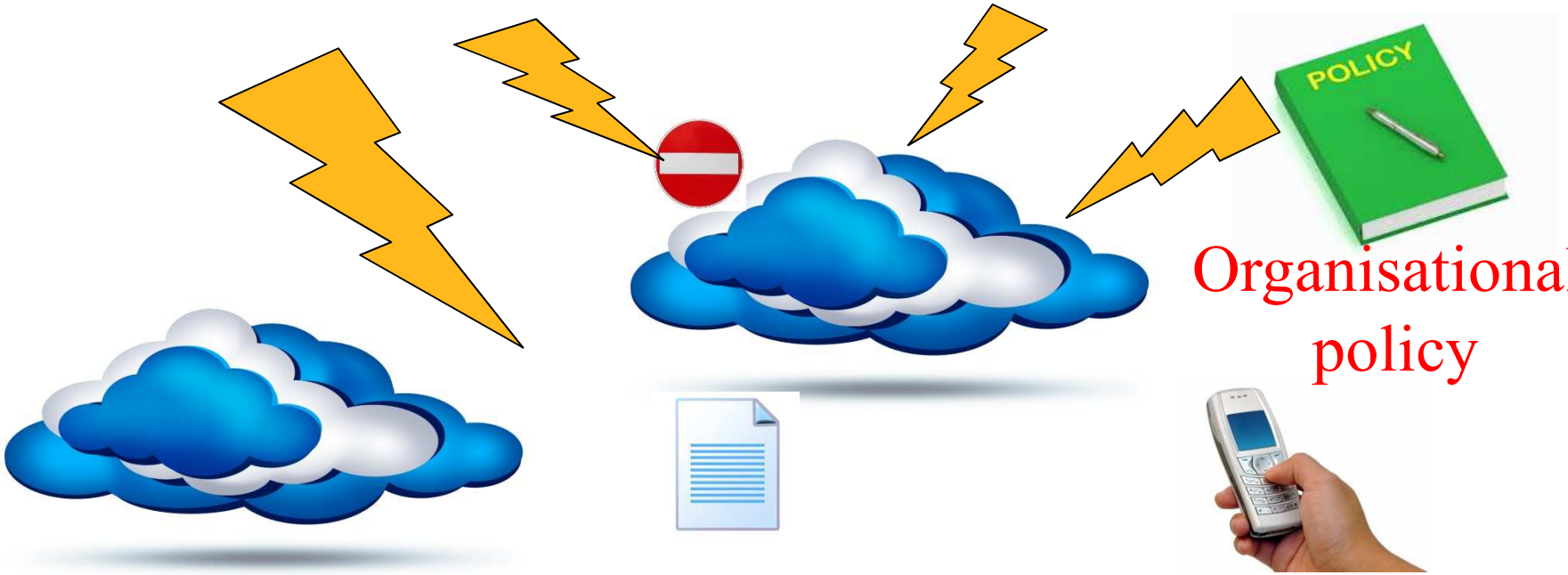
# Scenario without Coco Cloud

Laws

Contracts

User preferences



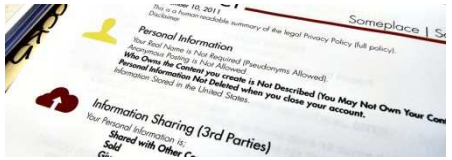

Organisational policy

# Scenario WITH Coco Cloud

Laws

Contracts

User preferences





Organisational policy

# Objectives

- Framework for the creation, analysis, operation and termination of machine readable (MR) e-Data Sharing Agreements (DSA). The objective is achieved though development of tools and components related to :
  - making the writing, understanding, analysis, management and enforcement of DSAs easier through set of tools.
  - transforming high level descriptions (often a form of controlled natural language) to directly enforceable data usage policies;
  - selecting the mostly appropriate enforcement mechanisms depending on the underlying Cloud or mobile infrastructure;

# Consortium

- Corporates:
  - HP (Coordinator (Claudio Caimi), Technology provider)
  - SAP (Technology provider/pilot developer for mobile case)
  - ATOS (Technology provider)
- Research/Academia
  - CNR (Scientific coordinator (Fabio Martinelli), research in data sharing and enforcement of usage control policies/mobile)
  - ICL (research on enforcement policies)
  - UO (Legal aspects with focus on  interconnection with ICT)
- SME:
  - 2B (legal aspects)
- End-User:
  - AGID (E-government pilot owner)
  - GQ (Health pilot)

# Coco Cloud Value proposition

I am always travelling and need my documents with me, but the IT policy of my organization is restricting sharing of data on our private mobile devices.

We are sharing citizen data with the other public administrations though cloud based solution but we are afraid that this data can be used for other purposes.

We need to share radiological studies with the other medical professionals, but once generated these studies should not be modified.

## Elevator Pitch

Many organisation use today cloud based services, as well as mobile devices, which offer excellent end user experiences, agility and flexibility. However if used for data sharing, it means losing control and sight of these.

Coco Cloud allows cloud or mobile device data sharing with colleagues or customers, while retaining full control over data sharing policy management and enforcement.

# Use cases and the main challenges

- A Test Bed infrastructure with OpenStack cloud solution
- Three Pilot products for:
  - Data Sharing for e-government
  - Data Sharing focused on mobile devices (BYOD)
  - Data Sharing in e-health scenarios

- Data Usage Control uniformly applied in Cloud and Mobile
- Management and enforcement of DSA
- From **human** understandable **data sharing agreements** to machine **enforceable policies**

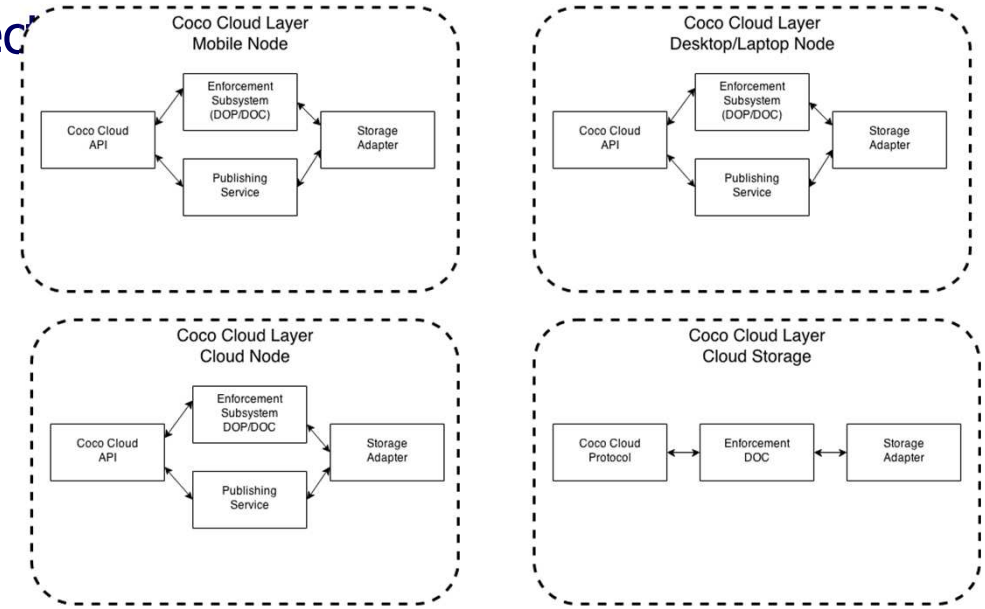
# Deployment modes

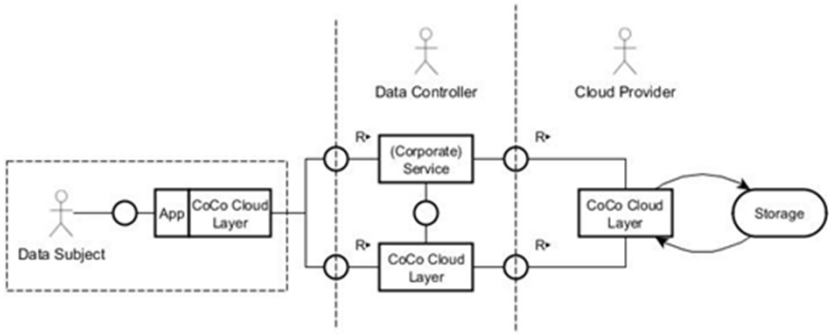
Coco Cloud ENGINE is the main projec
result, marketing  will depend on the
deployment mode e.g.

a) deployed at the third party :
gateway, broker

b) deployed at CSP SaaS: extended
SaaS service

c) deployed at the client: packaged
through aPaaS



# Mapping Coco Cloud to PaaS market segment

| | Computation | Communication | Storage |
|---|---|---|---|
| SaaS | | | |
| SaaS extensions/customisation | Orchestration? | Data encryption | Data leakage protection |
| Domain expert PaaS | bpmPaaS | | Business analytics PaaS or dataPaaS |
| Code-driven PaaS | aPaaS | iPaaS (ESBaaS) | dbPaaS |
| Foundational PaaS | Application containers, web servers | Messaging queue | Object storage |
| IaaS | VM | SDN | SDS |

# Market watch: aPaaS, CASB, CSG…

**Figure 1.** Magic Quadrant for Enterprise Application Platform as a Service, Worldwide

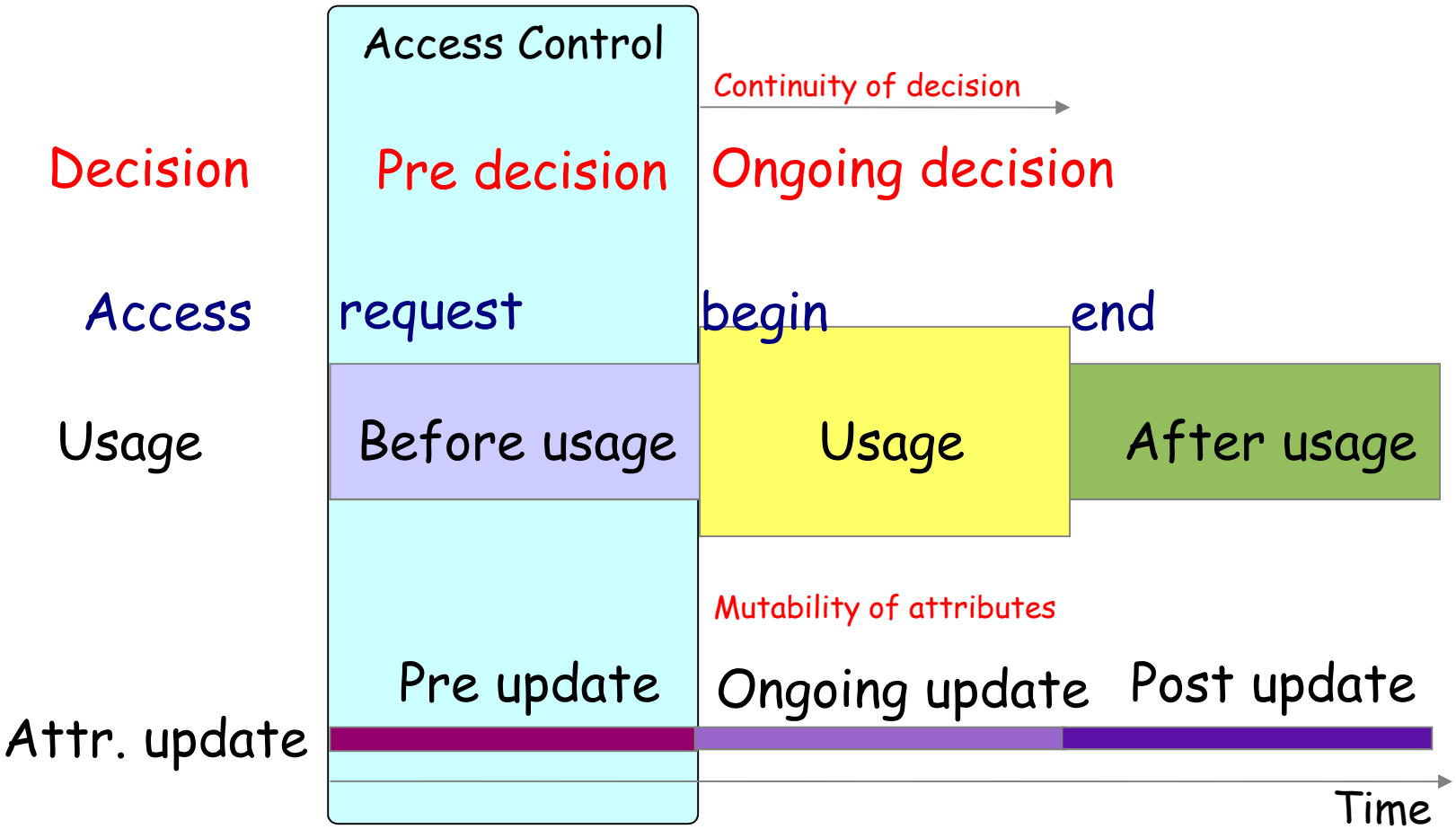

Source: Gartner (March 2015)

| | Criteria | Adallom | Bitglass | CipherCloud | NetSkope | Perspecsys | SkyHigh | Zscalar |
|---|---|---|---|---|---|---|---|---|
| | Maturity in Market | Established 2011 | Established 2013 | Established 2008 | Established 2011 | Established 2011 | Established 2011 | Established 2008 |
| Visibility | | | | | | | | |
| | Deployment Options | | | | | | | |
| | Out-of-band log analysis | YES | YES | YES | YES | YES | YES | YES |
| | Out-of-band API connectors | YES | YES | YES | YES | YES | YES | NO |
| | Agentless | YES | YES | NO | YES | NO | YES | YES |
| | Thin agent | YES | NO | NO | YES | NO | NO | YES |
| | Reverse proxy | YES | YES | YES | YES | YES | YES | NO |
| | On-premise | YES | YES | YES | YES | NO | YES | YES |
| | Cloud Based | YES | YES | YES | YES | YES | YES | YES |
| | Hybrid | YES | YES | YES | YES | NO | YES | YES |
| | Activity Aware | YES | YES | YES | YES | YES | YES | YES |
| | Context Aware | | | | | | | |
| | User | YES | YES | YES | YES | YES | YES | YES |
| | Device | YES | YES | YES | YES | YES | YES | YES |
| | Location | YES | YES | NO | YES | YES | YES | YES |
| | Inspect SSL | YES | YES | YES | YES | YES | YES | YES |
| Compliance | | | | | | | | |
| | Compliance | | | | | | | |
| | SOC-1 | YES | YES | YES | YES | YES | NO | YES |
| | SOC-2 Type II | YES | YES | YES | YES | YES | NO | YES |
| | FIPS 140-2 | YES | YES | YES | YES | YES | NO | NO |
| | ISO 27001 certified | YES | YES | YES | | YES | YES | YES |
| | Encrypt by default | YES | NO | NO | NO | NO | YES | YES |
| | Structured Data Encryption | NO | NO | YES | NO | NO | YES | NO |
| | Tokenization? | NO | NO | YES | NO | YES | NO | NO |
| Policy Control | | | | | | | | |
| | Single Sign On for Cloud Apps | | | | | | | |
| | SAML | YES | YES | YES | YES | YES | YES | YES |
| | OTHER | Centrify | OneLogin/EasySSO | Simplified | PING/OneLogon/Okta | ---- | PING/OneLogin/Okta | Ping |
| | Active Directory Integration | YES | YES | YES | YES | YES | YES | YES |
| | Mobile Enforcement | YES | YES | YES | YES | YES | YES | YES |
| | Can enforce policies based on corporate vs. personal credentials? | YES | NO | NO | YES | NO | YES | YES |
| | Policy Methods | | | | | | | |
| | Global | YES | NO | NO | YES | NO | YES | YES |
| | Per App | YES | YES | YES | YES | YES | YES | YES |
| | Per User | YES | YES | YES | YES | YES | YES | YES |
| | Per Group | YES | YES | YES | YES | YES | YES | YES |
| | DLP | | | | | | | |
| | Proprietary | YES | YES | YES | YES | YES | YES | YES |
| | Integrate with Commercial DLP providers | YES | NO | NO | NO | NO | YES | YES |
| | Enforce DLP in context of location, Device, AD group, activity.. | YES | NO | YES | YES | YES | YES | YES |
| | MDM Integration | | | | | | | |
| | MobileIron | YES | NO | NO | YES | NO | NO | YES |
| | Airwatch | YES | NO | NO | YES | NO | NO | YES |
| | Other | MDM Agnostic | *** | *** | *** | *** | Native | MDM Agnostic |
| | SIEM Integration | | | | | | | |
| | Arcsight | YES | YES | YES | YES | YES | YES | YES |
| | Q-Radar | YES | YES | NO | YES | NO | YES | YES |
| | Splunk | YES | YES | YES | YES | YES | YES | YES |
| | Other | LogRythm / Various | LogRythm | LogRythm | LogRythm, RSA, CA, Sumologic | LogRythm | LogRythm | LogRythm, RSA, CA, Sumologic |
| Threat Protection | | | | | | | | |
| | Anomaly detection | | | | | | | |
| | Sanctioned Apps | YES | YES | YES | YES | YES | YES | YES |
| | Shadow IT | YES | YES | NO | YES | YES | YES | YES |
| | AntiMalware | YES | NO | YES | NO | NO | NO | YES |
| | Execute/Detonate content in sandbox for malware review? | YES | NO | NO | NO | NO | NO | YES |

# Problems common to other DPSP projects

- Regulate sharing of data between organization and end-user, or between organization and organization
- Written in natural language: complex, difficult to parse, prone to ambiguity
- In the digital world, constraints in such contracts are still inaccessible from the software architecture supporting data sharing!
  - need to translate traditional contracts into technical policies
  - ensure degrees of enforcement and auditing
- What often happens is that
  - the end-user simply clicks the button "Accept the terms and conditions"…
- Moreover: terms and conditions are often obscure and confusing: how could ``common people" express their own preferences?

# Usage Control Model

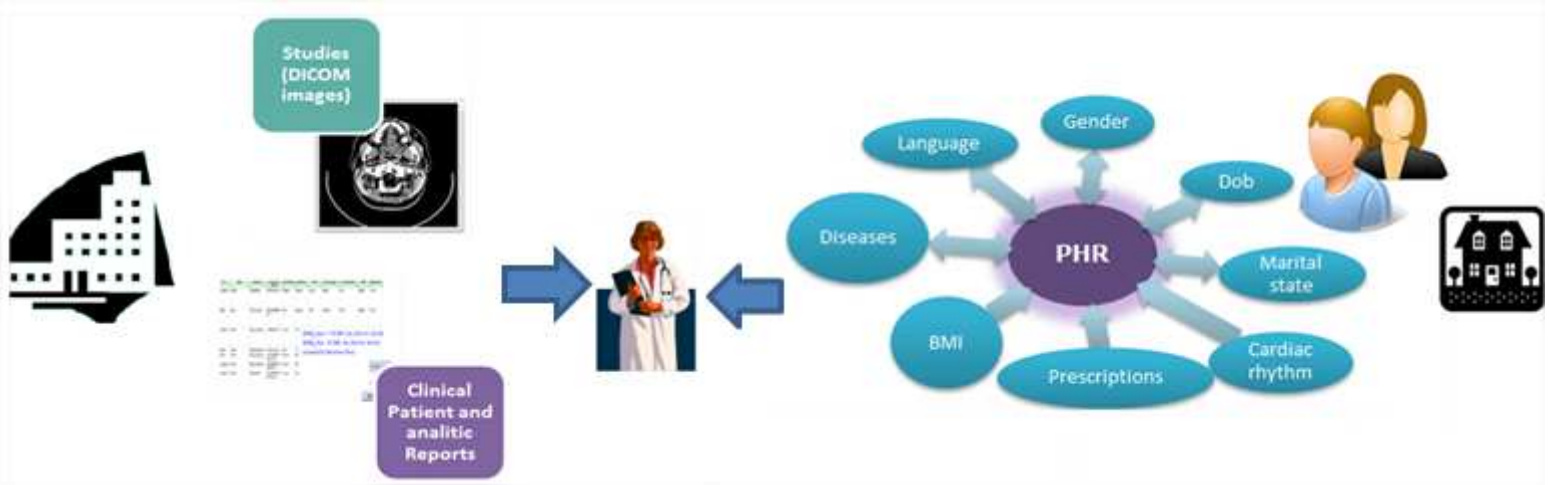


# e-Health pilot

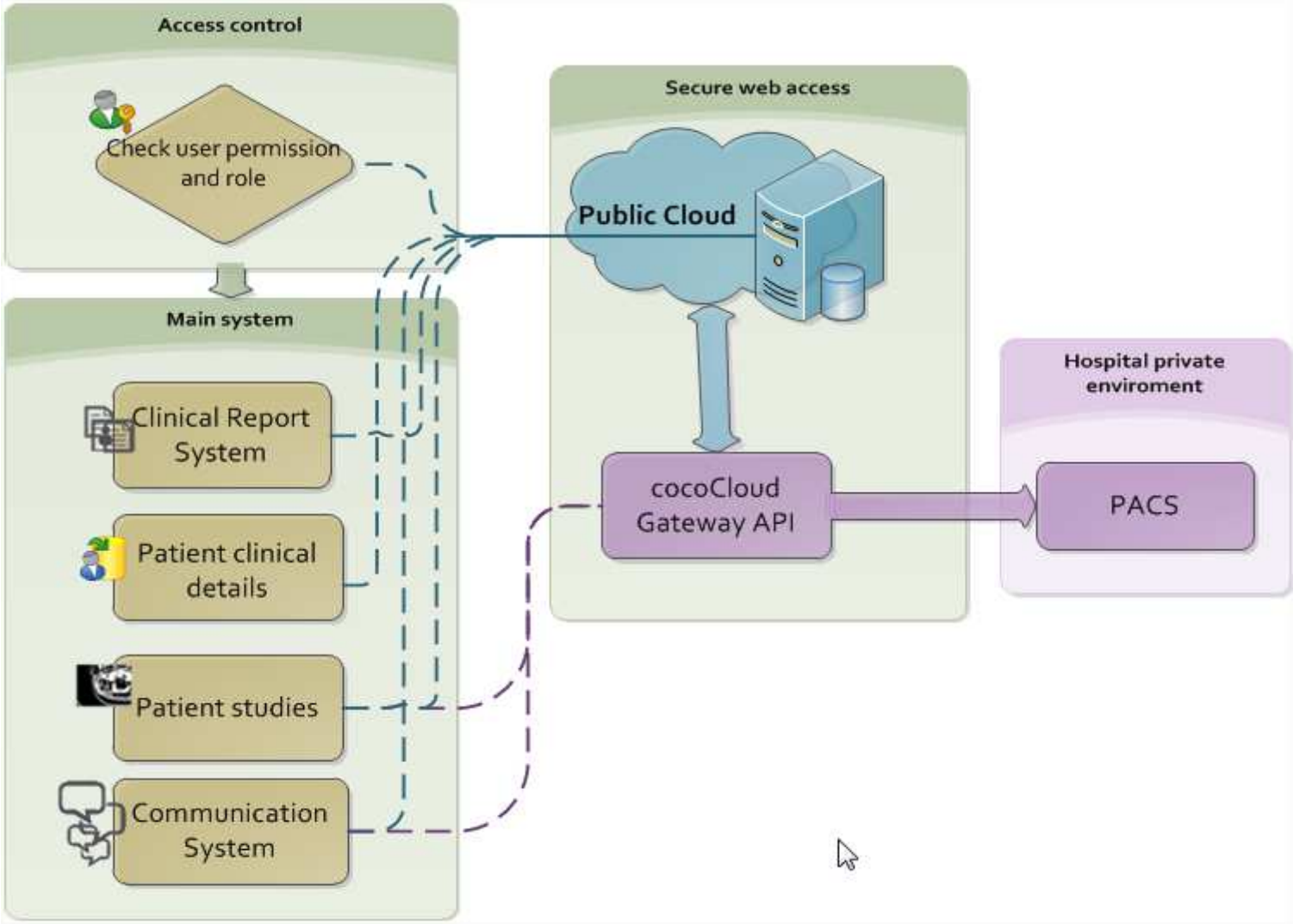
This pilot is addressing the daily situation of medical information exchange between doctors and patients.

The system will enable a straightforward connection with the Hospital Cloud infrastructure of Quiron hospital in Valencia and a new service of medical imaging follow-up.

PACS (private cloud), CocoCloud gateway (private cloud), Portal administration database (public cloud), Radiological portal (public cloud), CocoCloud-enabled client application

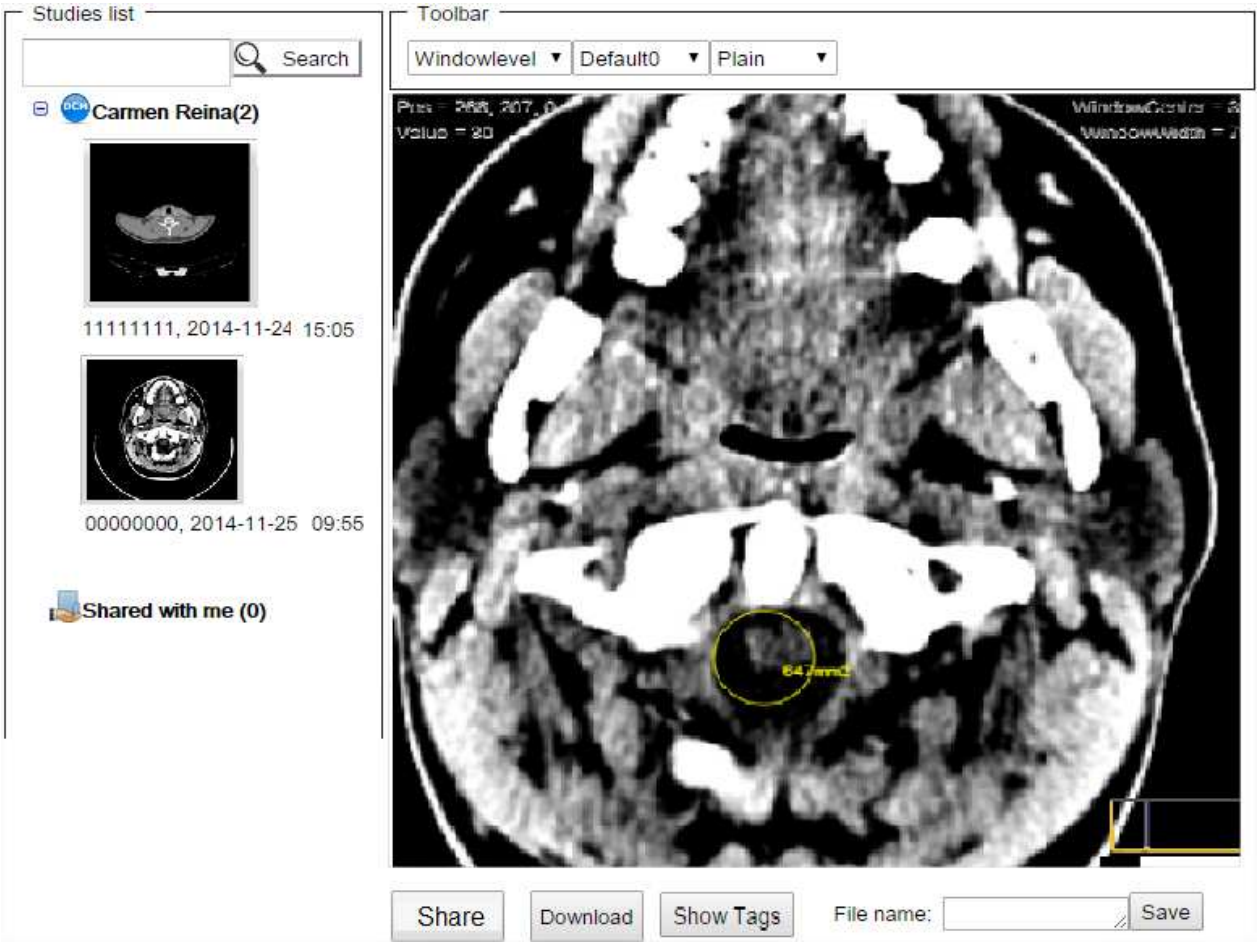


# Architecture



# Graphical user interface (GUI): Doctor Main interface

# Graphical user interface (GUI): Patient Radiological studies




- It is interesting to display a preview of its series before download a full study.
- Dicom toolbar; This tool bar controls various functions, filters, zoom, draw circles or lines,...
- It can be made a png image with the displayed study on the right.
- The selected study can be downloaded and/or shared with another professional.

# Patient clinical report

It displays the radiological report of the patient, including clinical data and radiological findings.

**Personal details**

**Name:** XXXXXXXX
**Sex:** XXXXX
**Dob:** XXXXXXX
**Marital state:** XXXXX

**ical data**

**Echography:** Bad
**Cardiac rhythm abnormality:** No
**SBP:** Bad

**iseases**

**Diabetes:** Yes

**it Patterns**

**Alcohol:** High
**Smoker:** High
**Diet:** Low
**BMI:** 19.2 Kg/cm

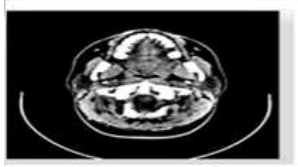
Fake data

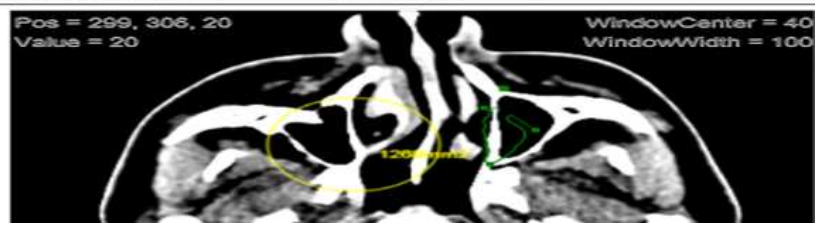
**Demographic data**

Address details: XXXXX
Language Preferences: XXXXX
Contact details: XXXXXX
Contact person:

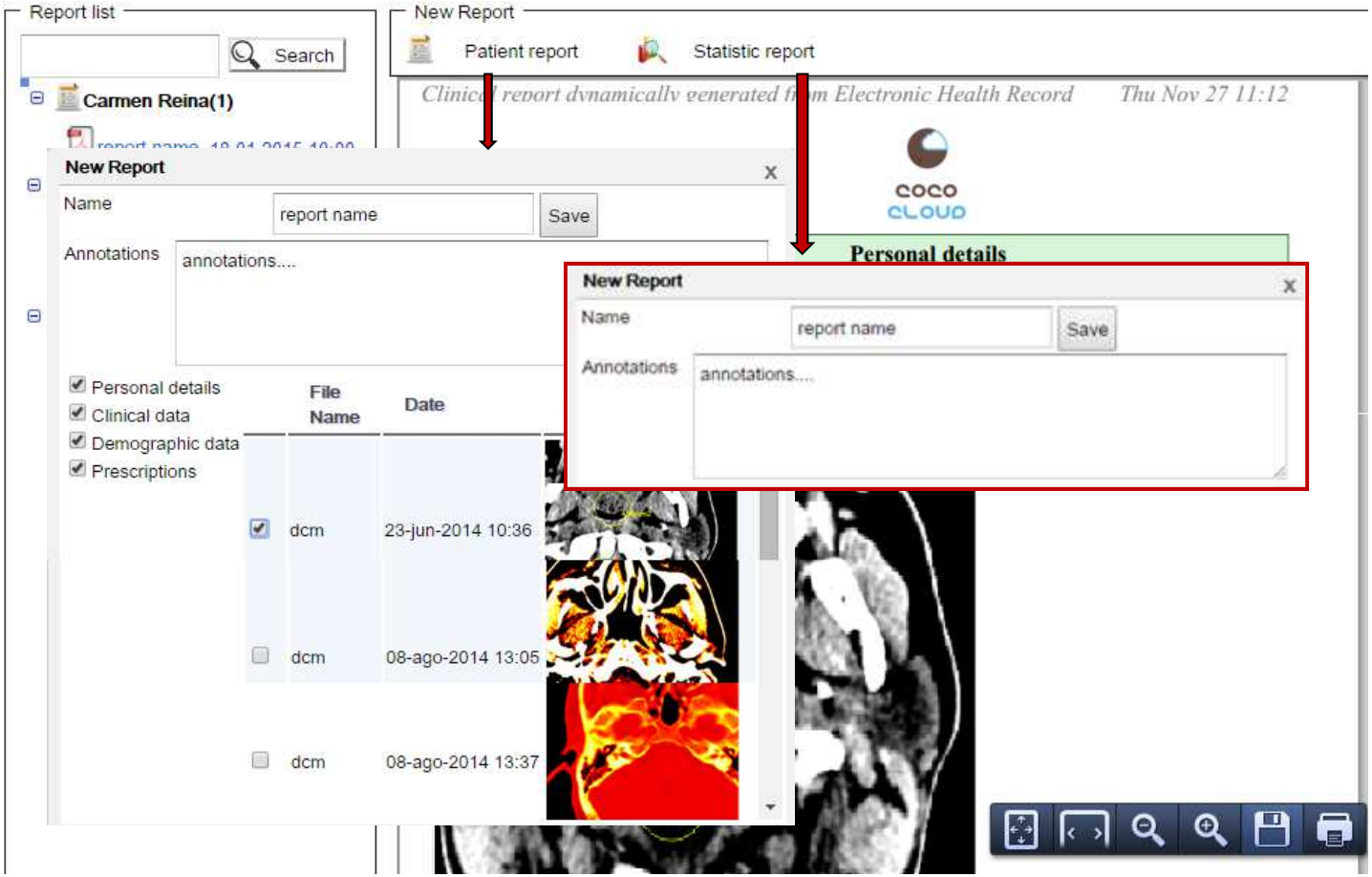
**Prescription**

| Drug | From | To | Frequen | Dose | Units | Dose Taken |
|---|---|---|---|---|---|---|
| name | 21-sep-2014 | 28-sep-2014 | 24 | 1.0 | units | -- |
| name | 14-sep-2014 | 21-sep-2014 | 24 | 1.0 | unit | -- |





# Graphical user interface (GUI): Create an annotation ("add to report")




- All available reports are shown in the same format; report name and date of creation and each of them is a clickable link to its PDF file
- To generate a patient clinical report, a dialog box is displayed in order to allow the physician to set report name, notes and patient's details.
- We emphasize the possibility to add previously saved images.

# Tools

## Front-End

**Eclipse IDE:** Eclipse is an integrated development environment (IDE) and it is used to develop the software application in Java.

**GWT framework:** Google Web Toolkit or GWT is an open sourc… web devel… tain co… ic…

Share clinical reports

Share user profile

Create preview Radiological Study (png image)

**HTML5 DICOM Viewer:** In order to display clinical images,

List alerts

Apply filter to Radiological Study

Apply Draw to Radiological Study

Apply zoom to Radiological Study

View detailed alert

View Patient Report

**e-Accessibility:** It has been identified … an important issue to be solved, especially from patient point of view, m… Health Information (PHI), as simple as possible… circumstan…

View detailed messages

List messages

## Back-end

**Eclipse IDE**

Create a new alert

Invalidate alert

Invalidate message

**WAD…** …jects. The WADO standard specifies a Web-based service for accessing and presenting DICOM persistent objects, such as images and medical imaging reports. It will be used in studies use case in order to access to a patient study using the DICOM Unique Identifier (UID).

**cocoCloud gatewayAPI:**

Create a new message

Add Patient Radiological Studies

View Radiological Studies

**Java open source PDF libraries:** It is necessary to generate a PDF doc… …reporting AdCoS.

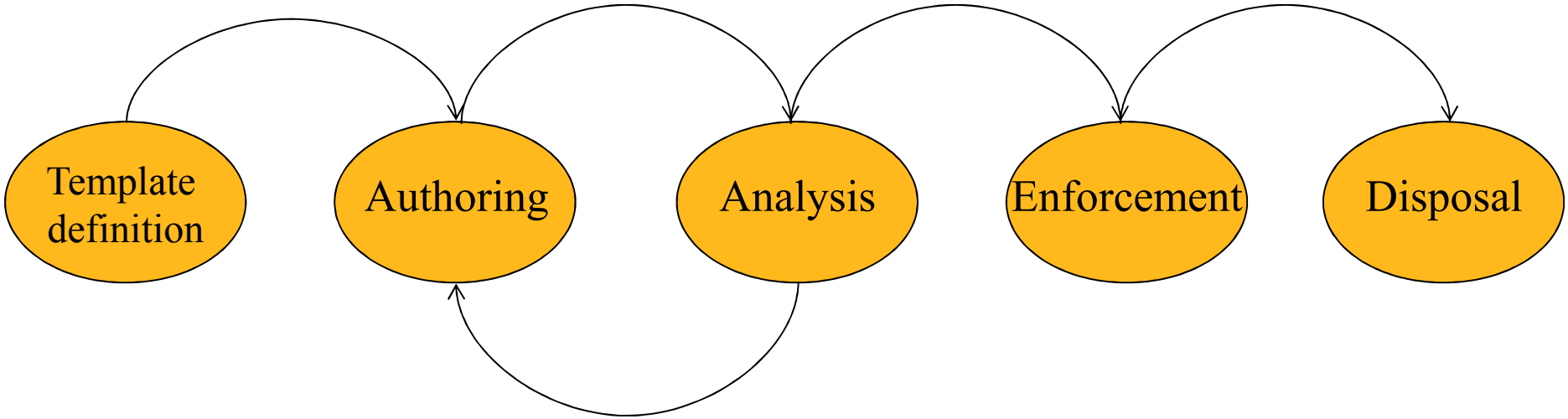
Create Patient Report

**Java open source machine learning libraries:** It is necessary to generate a model from our collated data and apply it in order to generate our Analytic report in Analysis and reporting AdCoS. This report is generated by applying the model (previously) obtained with data mining techniques.

# electronic Data Sharing Agreements (e-DSA)

- e-DSA is an electronic, human-readable & machine-readable contract, consisting of
  - Predefined legal information
  - Dynamically defined information, including:
    - Validity period
    - Entities participating in the agreement
    - Data covered
    - Intended use of data
    - The policies regulating the data sharing
    - Methods to assure data confidentiality/security when transferring data
    - Signatures of parties

# e-DSA lifecycle: main phases



# e-DSA: a matter of standardization

- e-DSA as a whole: a XML document
- containing several fields, each of them specified with different languages. Roughly:
  - a natural language for, e.g., validity period, parties, data covered, purpose of use…
  - a Controlled Natural Language for editing rules constraining data sharing. CNL must be quite user-friendly and readable, could be used even by non policy experts
  - a process algebra-like language encoding the above rules in a format amenable for automated analysis – a formal, technical language, should be used by expert analysts
  - an enforceable language (a la XACML) -- it will be the input for enforcement – a very technical language, for policy experts

# Another view on Coco Cloud benefits

https://www.powtoon.com/online-presentation/c6CWMuS1992/cococloud-short-presentation-0615/

# Conclusion

- e-DSA issues similar to MR SecLA, PLA, SLA…
- Usage control prototype ready
- Enforcement ENGINE poses different challenges
- From market perspective, intrusiveness (need for app to be Coco aware) might be an important obstacle