UNIVERSITÀ DEGLI STUDI FIRENZE

DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

www.disit.org

Part 2 on Data Security and Privacy by Paolo Nesi

Data Protection, Privacy and GDPR, IoT Security and Blockchain

University of Florence, DISIT lab, [Https://www.disit.org](https://www.disit.org)

[Https://www.snap4city.org](https://www.snap4city.org)

Paolo.nesi@unifi.it

UNIVERSITÀ DEGLI STUDI FIRENZE

DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

Distributed Data Intelligence and Technologies Lab
Distributed Systems and Internet Technologies Lab

Paolo Nesi

Department of Information Engineering

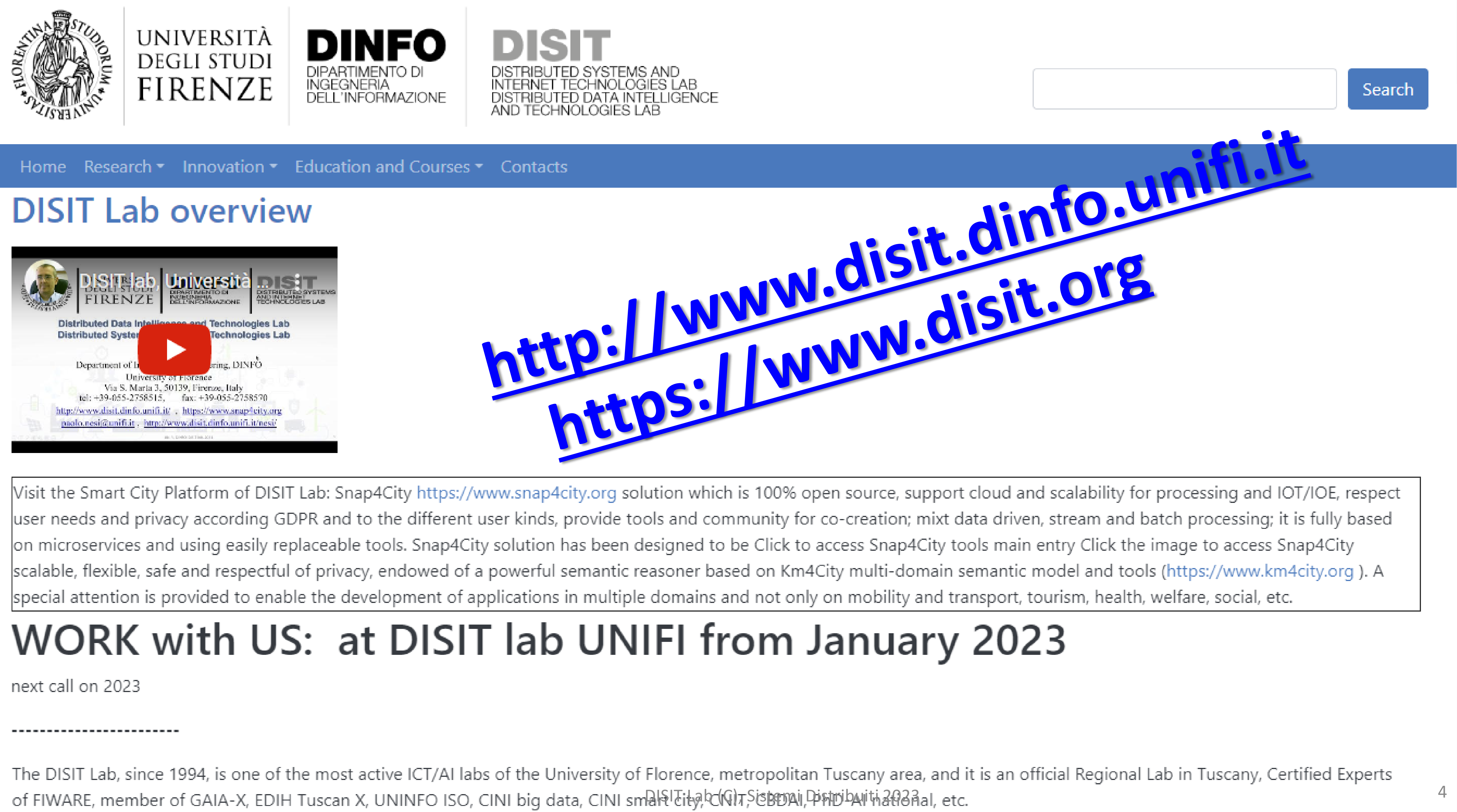
University of Florence
Via S. Marta 3, 50139, Firenze, Italy
tel: +39-055-2758515, fax: +39-055-2758570

http://www.disit.dinfo.unifi.it/

paolo.nesi@unifi.it , http://www.disit.dinfo.unifi.it/nesi/

DISIT Lab

- Researchers: 20
- Current Active Projects: 18
- Project in the last 4 years: 34
- Research Budget (last 2 years): 1.5M€
- Foreseen Research Budget (next 2 years): 2.2M€
- SpinOff: 1


UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE
DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB DISTRIBUTED DATA INTELLIGENCE AND TECHNOLOGIES LAB
Search
Home
Research
Innovation
Education and Courses
Contacts
DISIT lab, Università ...

http://www.disit.dinfo.unifi.it

https://www.disit.org

DISIT Lab overview

Visit the Smart City Platform of DISIT Lab: Snap4City https://www.snap4city.org solution which is 100% open source, support cloud and scalability for processing and IOT/IOE, respect user needs and privacy according GDPR and to the different user kinds, provide tools and community for co-creation; mixt data driven, stream and batch processing; it is fully based on microservices and using easily replaceable tools. Snap4City solution has been designed to be Click to access Snap4City tools main entry Click the image to access Snap4City scalable, flexible, safe and respectful of privacy, endowed of a powerful semantic reasoner based on Km4City multi-domain semantic model and tools (https://www.km4city.org). A special attention is provided to enable the development of applications in multiple domains and not only on mobility and transport, tourism, health, welfare, social, etc.

WORK with US: at DISIT lab UNIFI from January 2023

next call on 2023

The DISIT Lab, since 1994, is one of the most active ICT/AI labs of the University of Florence, metropolitan Tuscany area, and it is an official Regional Lab in Tuscany, Certified Experts of FIWARE, member of GAIA-X, EDIH Tuscan X, UNINFO ISO, CINI big data, CINI smart city, CNIT, CBDAI, PhD AI national, etc.

Con chi lavoriamo

swarco First in Traffic Solutions.

VAR group

THALES

BUSITALIA NORD GRUPPO FERROVIE DELLO STATO ITALIANE

BBC

ALTAIR CHIMICA

TIM

LEONARDO

ECM

COSTRUZIONI NOVICROM

enel x

BMG

europeana think culture

ALSTOM

eutelsat

Hewlett Packard Enterprise

SIAE Società Italiana degli Autori ed Editori

Rai

COMPUTER GROSS

ENGINEERING

PHILIPS

tiscali:

Effective Knowledge s.r.l.

GIUNTI EDITORE

Fondazione per la ricerca e l'innovazione

e-distribuzione

ENTE CASSA DI RISPARMIO DI FIRENZE

CITTÀ METROPOLITANA DI FIRENZE

COMUNE DI FIRENZE

CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

Fraunhofer

Consiglio Nazionale delle Ricerche

cini

cnit consorzio nazionale interuniversitario per le telecomunicazioni

UNIVERSITY OF PITTSBURGH

Camera di Commercio Firenze

ARPAT Agenzia regionale per la protezione ambientale della Toscana

REGIONE TOSCANA

National Technical University of Athens

EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

APRE TOSCANA AGENZIA PER LA PROMOZIONE DELLA RICERCA EUROPEA

ACCADEMIA NAZIONALE DI SANTA CECILIA

CONSORZIO LaMMA

Agenda

- Modello del corso
- Laboratorio DISIT
- Infrastruttura e servizi
- Progetti in corso e attività correlate
- Visione generale del corso

Infrastructure and support

- **Research group since 1994**
- **Cloud and data center** with >700 TByte storage in raid 50/60,
  - >800 CPU cores, 1 Thz Clock
    - >8 Tbyte RAM, >500Tbyte
  - 70.000 GPU cores, Managing several infrastructure
- **IOT center:** reference center
- **Nodo CINI per: Big data, Smart City, AI**
- **Smart City infrastructure**
- **Snap4City Living Lab solution**
  - **Snap4Industry for Industry 4.0 solutions**

Corsi di docenti DISIT

Triennale

Sistemi Distribuiti – Prof. Paolo Nesi

Sistemi Operativi – Prof. Pierfrancesco Bellini

Fondamenti di Informatica – Prof. Gianni Pantaleo

Magistrale: Informatica, Intelligenza Artificiale

Big Data Architectures – Prof. Paolo Nesi (Big Data, Architecture, Cloud, IoT)

Knowledge Engineering – Prof. Pierfrancesco Bellini (Knowledge Engineering, Natural Language Processing)

Security and data privacy -- Prof. P. Nesi, Prof. P. Bellini (Web Security, privacy, GDPR)

Altri corsi:

Data Intelligence – Corso di Intelligence e Sicurezza Nazionale – Prof. Paolo Nesi

Master in Big Data-MABIDA: architetture, Big Data, Knowledge engineering, Natural Language Processing, cloud, etc.

Dottorato: DINFO, nazionale in AI

Agenda

- Modello del corso
- Laboratorio DISIT
- Infrastruttura e servizi
- Progetti in corso e attività correlate
- Visione generale del corso

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

Some DISIT Projects

Herit Data: Tourism and Mng. https://herit-data.interreg-med.eu/
Snap4City: IOT/IOE smart city www.snap4city.org
Trafair: CEF project with several Cities http://trafair.eu/
Mosaic: Mobility and transport model
Km4City: http://www.km4city.org
REPLICATE H2020, SCC1, EC flagship
    http://replicate-project.eu/
Sii-Mobility SCN MIUR: http://www.sii-mobility.org
Feedback: retail and GDO Big Data analytics
5G with 3G-Wind, Open Fiber, Estra
Coll@bora Social Innovation, MIUR:
    http://www.disit.org/5479
RESOLUTE H2020, EC:
    http://www.resolute-eu.org
TRACE-IT, RAISSS, TESYSRAIL, ...
Mobile Emergency:
    http://www.disit.org/5404

Trace-IT

RAISSS

Altri progetti

- AMPERE: industry 4.0
- Smart Ambulance: industry 4.0, smart heath, smart vehicles
- Cyprus: smart city strategy
- PC4City: landslides predictions
- ISPRA: smart city
- ….

SNAP4CITY KM4CITY

SMART SOLUTIONS AND DECISION SUPPORT SYSTEMS

100% OPEN SOURCE

Powered by FIWARE

FREE TRIAL

PEN Test Passed

EU GDPR COMPLIANT

SNAP4 Appliances and Dockers Installations

EUROPEAN OPEN SCIENCE CLOUD

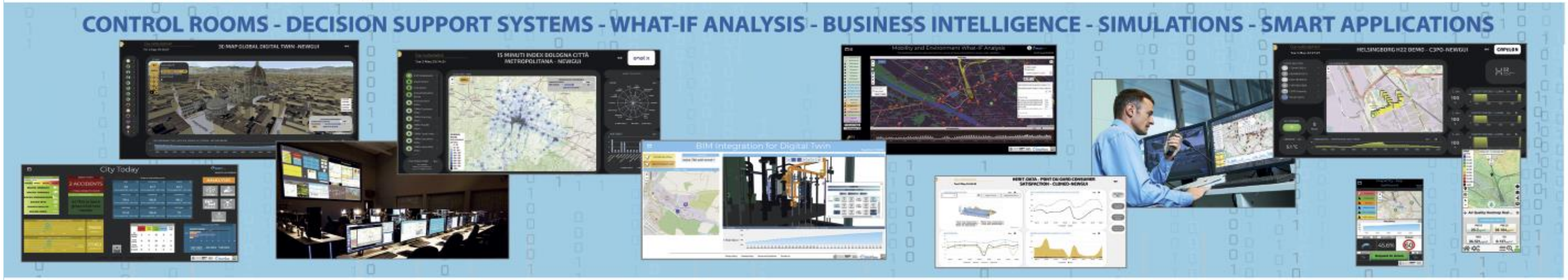
Node-RED

JS Foundation

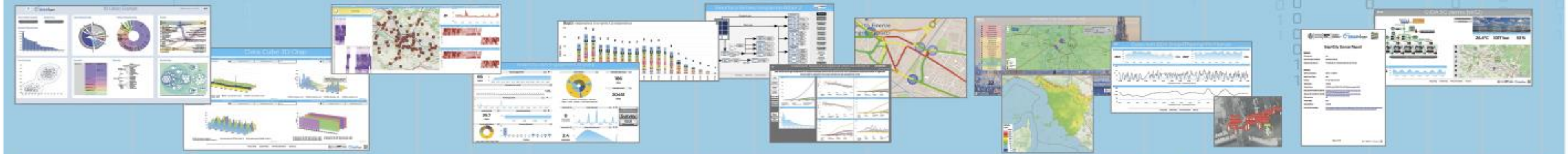
E015 digital ecosystem

NVIDIA

CONTROL ROOMS - DECISION SUPPORT SYSTEMS - WHAT-IF ANALYSIS - BUSINESS INTELLIGENCE - SIMULATIONS - SMART APPLICATIONS



DASHBOARDS - VISUAL ANALYTICS - SYNOPTICS - DIGITAL TWIN - GRAPHICAL WIDGETS - ANALYTICS - GUI CUSTOM STYLES - VISUAL PROGRAMMING

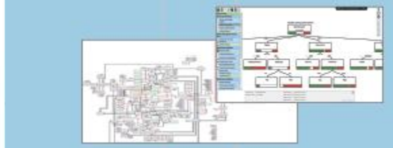


DASHBOARDS, WIDGETS TEMPLATES

PREDICTION - ANOMALY DETECTION - CLUSTERING - ROUTING - SENTIMENT NLP - TRAFFIC FLOW PEOPLE FLOWS - SDG - 15 MIN CITY INDEX - KPI - HEATMAPS - ORIGIN DESTINATION - ETC...

API - MICROSERVICES - GIS - BPM VIDEO - REPORTS - MAPS - 3D ...

ANY: DATA, BROKER, NETWORK AND VERTICAL



EXPERT SYSTEM, KNOWLEDGE BASE
SEMANTIC REASONING
SMART DATA MODEL
IOT DEVICE MODELS, STORAGE

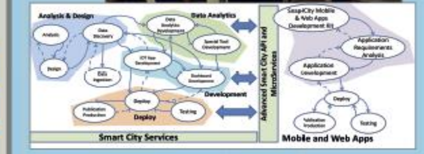
BIG DATA ANALYTICS, ARTIFICIAL INTELLIGENCE
EXPLAINABLE AI, MACHINE LEARNING
OPERATIVE RESEARCH, STATISTICS

VISUAL PROGRAMMING, ADAPTERS
DATA FLOWS, WORKFLOWS
PARALLEL DISTRIBUTED PROCESSING
DATA DRIVEN

Native and External Applications

- Smart Parking
- Smart Light
- Smart Waste
- Smart Energy
- Social Media Analysis

...



METHODOLOGIES
LIVING LABS
COURSES AND COMMUNITY
DEVELOPMENT TOOLS

Standards and Interoperability (9/2022)

SNAP4CITY

KM4CITY

Compliant with:

- **IoT:** NGSI V2/LD, LoRa, LoRaWan, MQTT, AMQP, COAP, OneM2M, TheThingsNetwork, SigFOX, Libelium, IBIMET/IBE, Enocean, Zigbee, DALI, ISEMC, Alexa, Sonoff, HUE Philips, Tplink, BACnet, TALQ, Protocol Buffer, KNX, OBD2, Proximus, ..
- **IoT model:** FIWARE Smart Data Model, Snap4City IoT Device Models
- **General**: HTTP, HTTPS, TLS, Rest Call, SMTP, TCP, UDP, SOAP, WSDL, FTP, FTPS, WebSocket, WebSocket Secure, GML, WFS, WMS, RTSP, ONVIF, AXIS TVCam, CISCO Meraki, OSM, Copernicus, The Weather Channel, Open Weather, OLAP, ….
- **Formats**: JSON, GeoJSON, XML, CSV, GeoTIFF, OWL, WKT, KML, SHP, db, XLS, XLSX, TXT, HTML, CSS, SVG, IFC, XPDL, OSM, Enfuser FMI, Lidar, glTF, GLB, DTM, GDAL, Satellite, D3 JSON, …
- **Database**: Open Search, MySQL, Mongo, HBASE, SOLR, SPARQL, ODBC, JDBC, Elastic Search, Phoenix, PostGres, MS Azure, ..
- **Industry**: OPC/OPC-UA, OLAP, ModBUS, RS485, RS232,..
- **Mobility**: DATEX, GTFS, Transmodel, ETSI, ..
- **Social**:Twitter, FaceBook, Telegram, ..
- **Events**: SMS, EMAIL, CAP, RSS Feed, ..
- **OS**: Linux, Windows, Android, Raspberry Pi, Local File System, AXIS, ESP32, etc.

https://www.snap4city.org/65

Node-RED

JS Foundation

FIWARE
Open APIs for Open Minds

gaia-x

E015
digital ecosystem

bee smart city

sigfox
partner network

ckan

GJL

LABGEO

esri Italia
THE SCIENCE OF WHERE

EUROPEAN OPEN
SCIENCE CLOUD
MARKETPLACE

https://www.Snap4City.org

- 8 running installations in Europe
  - Toscana, Pisa, Sweden, ISPRA, Snap4.eu,
  - Altair, Italmatic, Denmark, ….
- 13 projects, 12 pilots on 10 Countries
  - >40 cities/area
- **Wide MULTI-tenant deploy, e.g.,**
  - 18 Organizations / tenant
  - > 7400 users on
  - > 1400 Dashboards
  - > 16 mobile Apps
  - **> 2 Million of structured data per day**
  - > 520 IoT Applications/node-RED
  - > 700 web pages with training
  - > 60 videos, training videos

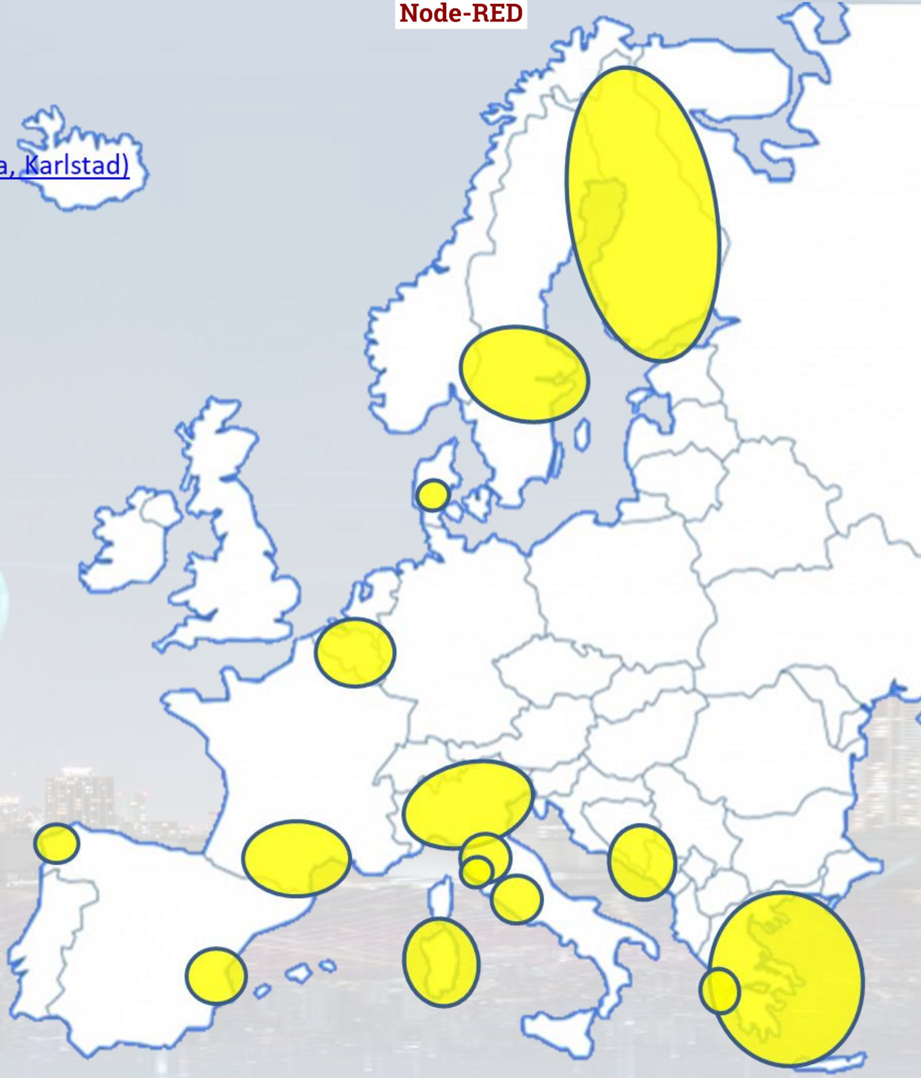
100% OPEN SOURCE

PEN Test Passed

EU GDPR COMPLIANT

Main Organizations/areas

- Antwerp area (Be)
- Bologna (I)
- Capelon (Sweden: Västerås, Eskilstuna, Karlstad)
- DISIT demo (multiple)
- Dubrovnik, Croatia
- Firenze area (I)
- Garda Lake area (I)
- Greece (Gr)
- Helsinki area (Fin)
- Livorno area (I)
- Lonato del Garda (I)
- Modena (I)
- Mostar, Bosnia-Herzegovina
- Oslo & Padova (Impetus)
- Pisa area (I)
- Pistoia (I)
- Pont du Gard, Occitanie (Fr)
- Prato (I)
- Roma (I)
- Santiago de Compostela (S)
- Sardegna Region (I)
- Siena (I)
- SmartBed (multiple)
- Toscana Region (I), SM
- Valencia (S)
- Venezia area (I)
- WestGreece area (Gr)



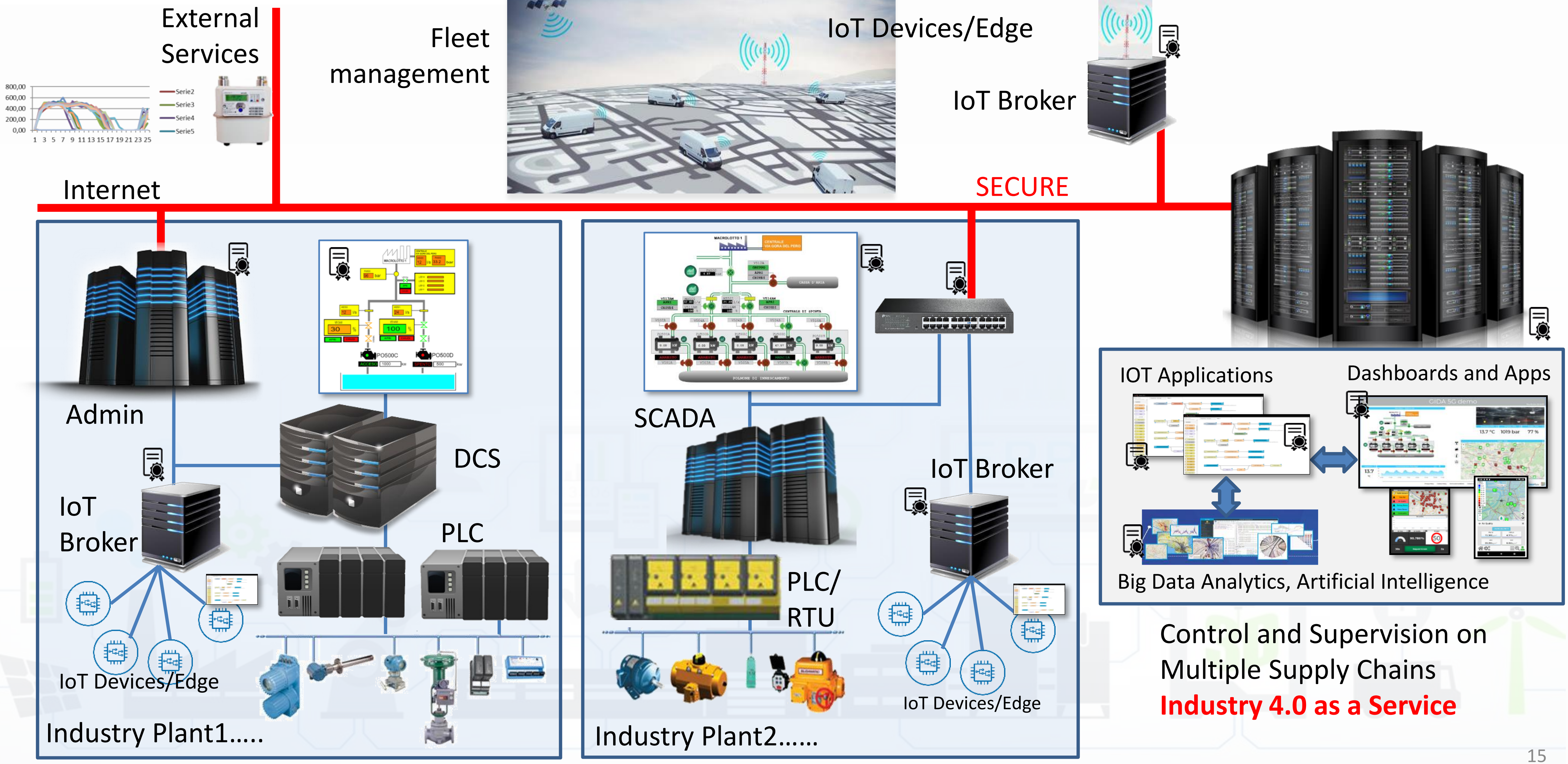
- **Trials in Israel, Colombia, Brasile, Australia, India, Romania, etc.**

EUROPEAN OPEN SCIENCE CLOUD

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

https://www.snap4city.org/369

SNAP4INDUSTRY



External Services

Fleet management

IoT Devices/Edge

IoT Broker

Internet

SECURE

Admin

DCS

IoT Broker

PLC

IoT Devices/Edge

Industry Plant1.....

SCADA

IoT Broker

PLC/ RTU

IoT Devices/Edge

Industry Plant2......

IOT Applications

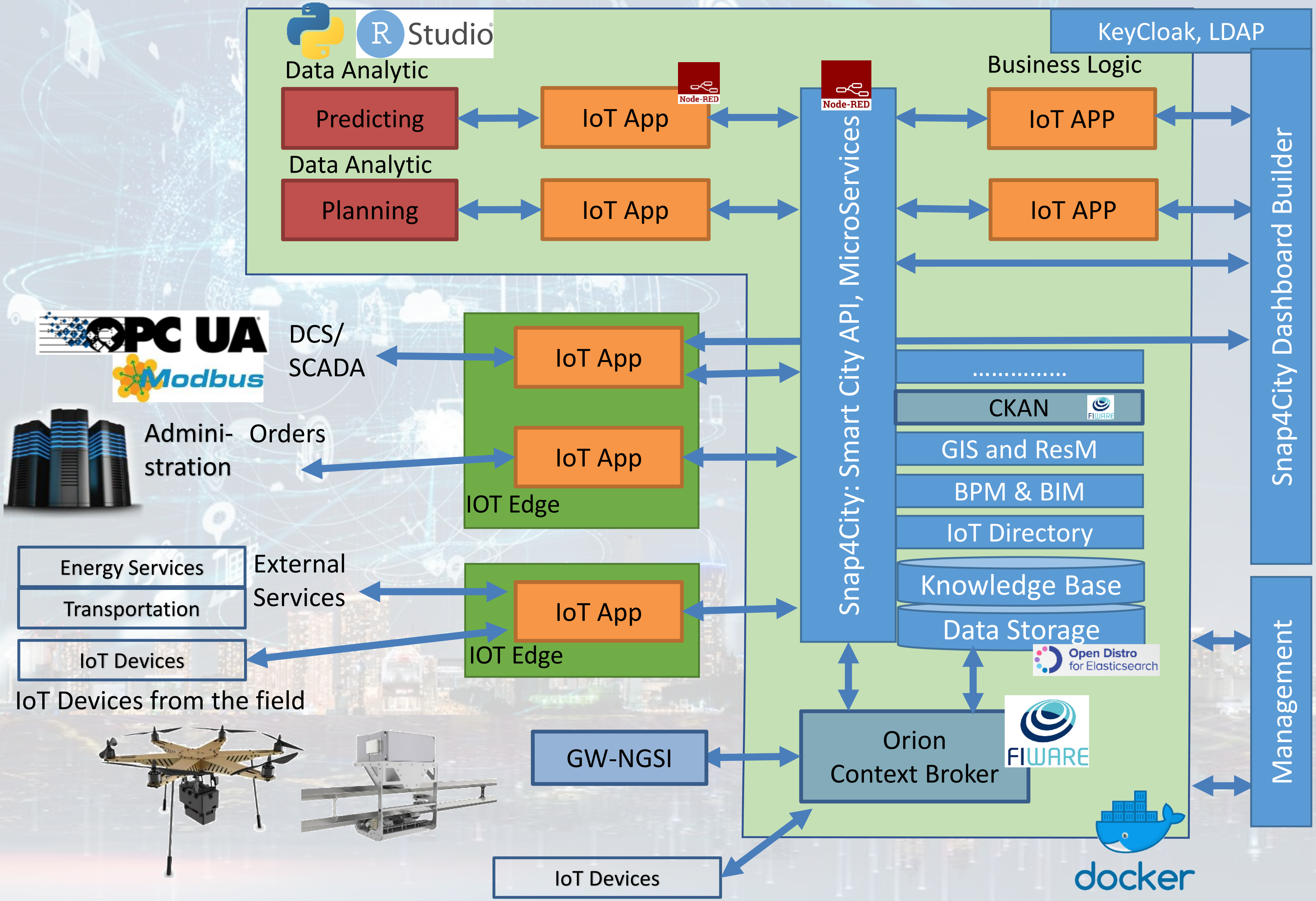
Dashboards and Apps

Big Data Analytics, Artificial Intelligence

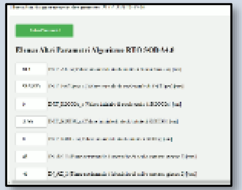
Control and Supervision on Multiple Supply Chains

Industry 4.0 as a Service

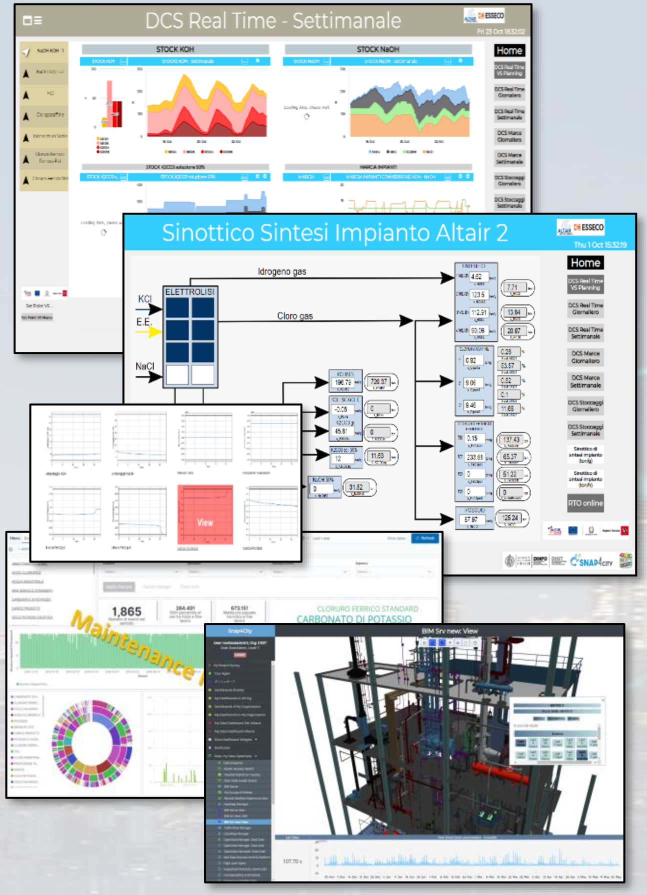
Snap4Industry Detailed Architecture



Production Parameters



Dashboards, Visual Analytics, Synoptics, 3D, Maps



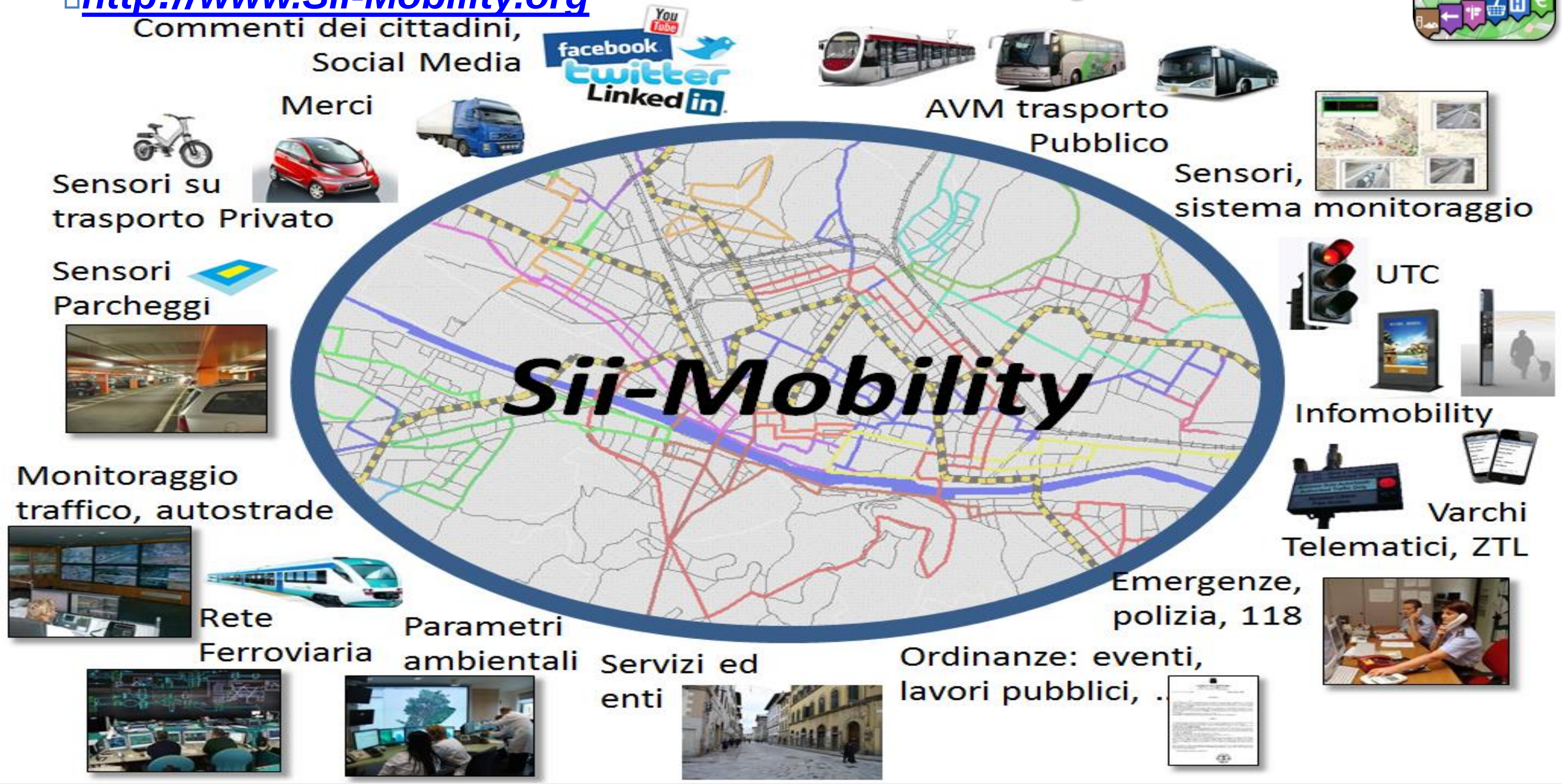
UNIVERSITÀ DEGLI STUDI FIRENZE

DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB http://www.disit.org

Sii-Mobility

http://www.Sii-Mobility.org



Commenti dei cittadini, Social Media

Merci

Sensori su trasporto Privato

Sensori Parcheggi

Monitoraggio traffico, autostrade

Rete Ferroviaria

Parametri ambientali

Servizi ed enti

Ordinanze: eventi, lavori pubblici, ..

Emergenze, polizia, 118

Varchi Telematici, ZTL

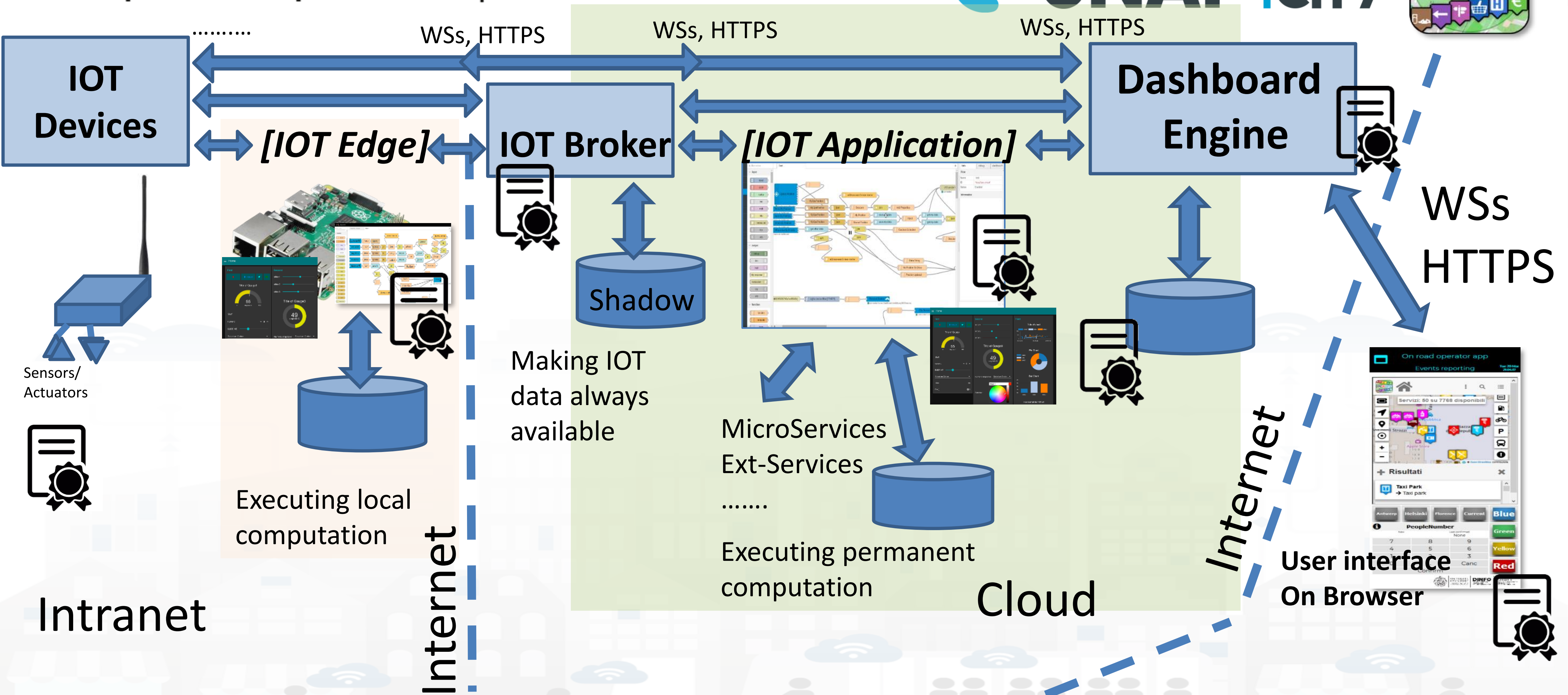
Infomobility

UTC

Sensori, sistema monitoraggio

AVM trasporto Pubblico

Sii-Mobility



....

WSs, HTTPS

WSs, HTTPS

WSs, HTTPS

IOT Devices

[IOT Edge]

IOT Broker

[IOT Application]

Dashboard Engine

WSs HTTPS

Sensors/ Actuators

Shadow

Making IOT data always available

MicroServices Ext-Services ....

Executing local computation

Executing permanent computation

User interface On Browser

Intranet

Internet

Internet

Cloud

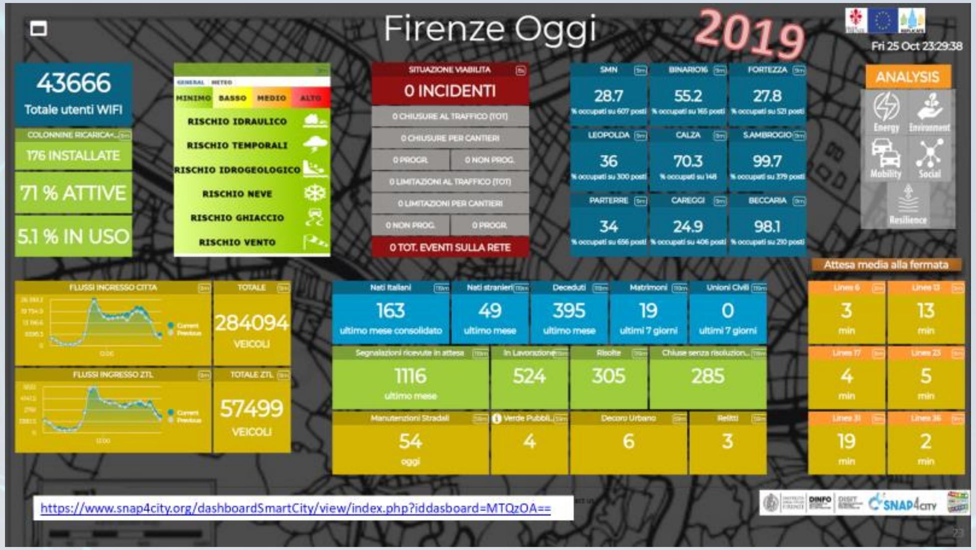
End 2 end security

Smart City Control Room
Florence Metropolitan City

COMUNE DI FIRENZE

reference

- **Multiple Domain Data**
  - mobility and transport, accidents, public transport, parking, traffic flow, Traffic Reconstruction, …
  - civil protection, gov data, covid-19, social & social media, people flow, tourism, energy, …
- **Multiple dash/tool Levels & Decision Makers**
- **Historical and Real Time data**
  - Billions of Data
  - Predictions, what-if analysis
- **Services Exploited on:**
  - Multiple Levels, Mobile Apps, API
- **Since 2017**



Firenze Oggi 2019

Fri 25 Oct 23:29:38

43666 Totale utenti WIFI

COLONNINE RICARICA

176 INSTALLATE

71 % ATTIVE

5.1 % IN USO

GENERAL METEO

MINIMO BASSO MEDIO ALTO

RISCHIO IDRAULICO

RISCHIO TEMPORALI

RISCHIO IDROGEOLOGICO

RISCHIO NEVE

RISCHIO GHIACCIO

RISCHIO VENTO

SITUAZIONE VIABILITA

0 INCIDENTI

0 CHIUSURE AL TRAFFICO (TOT)

0 CHIUSURE PER CANTIERI

0 PROGR. 0 NON PROG.

0 LIMITAZIONI AL TRAFFICO (TOT)

0 LIMITAZIONI PER CANTIERI

0 NON PROG. 0 PROGR.

0 TOT. EVENTI SULLA RETE

SMN	BINARIO16	FORTEZZA
28.7 % occupati su 607 posti	55.2 % occupati su 165 posti	27.8 % occupati su 521 posti
LEOPOLDA	CALZA	S.AMBROGIO
36 % occupati su 300 posti	70.3 % occupati su 148	99.7 % occupati su 379 posti
PARTERRE	CAREGGI	BECCARIA
34 % occupati su 656 posti	24.9 % occupati su 406 posti	98.1 % occupati su 210 posti

ANALYSIS

Energy Environment Mobility Social Resilience

Attesa media alla fermata

Linea 6	Linea 13
3 min	13 min
Linea 17	Linea 23
4 min	5 min
Linea 31	Linea 36
19 min	2 min

FLUSSI INGRESSO CITTA — TOTALE 284094 VEICOLI

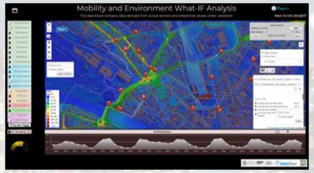
FLUSSI INGRESSO ZTL — TOTALE ZTL 57499 VEICOLI

Nati Italiani	Nati stranieri	Deceduti	Matrimoni	Unioni Civili
163 ultimo mese consolidato	49 ultimo mese	395 ultimo mese	19 ultimi 7 giorni	0 ultimi 7 giorni

Segnalazioni ricevute in attesa	In Lavorazione	Risolte	Chiuse senza risoluzion...
1116 ultimo mese	524	305	285

Manutenzioni Stradali	Verde Pubbli...	Decoro Urbano	Relitti
54 oggi	4	6	3

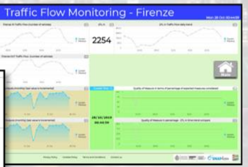
https://www.snap4city.org/dashboardSmartCity/view/index.php?iddasboard=MTQzOA==


Mobility and Environment What-IF Analysis

Smart Bench

Energy

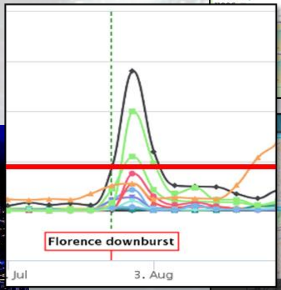
Environment


Traffic Flow Monitoring - Firenze

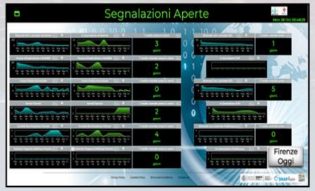
FIRENZE - Real Time

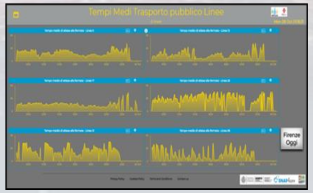
Mobility

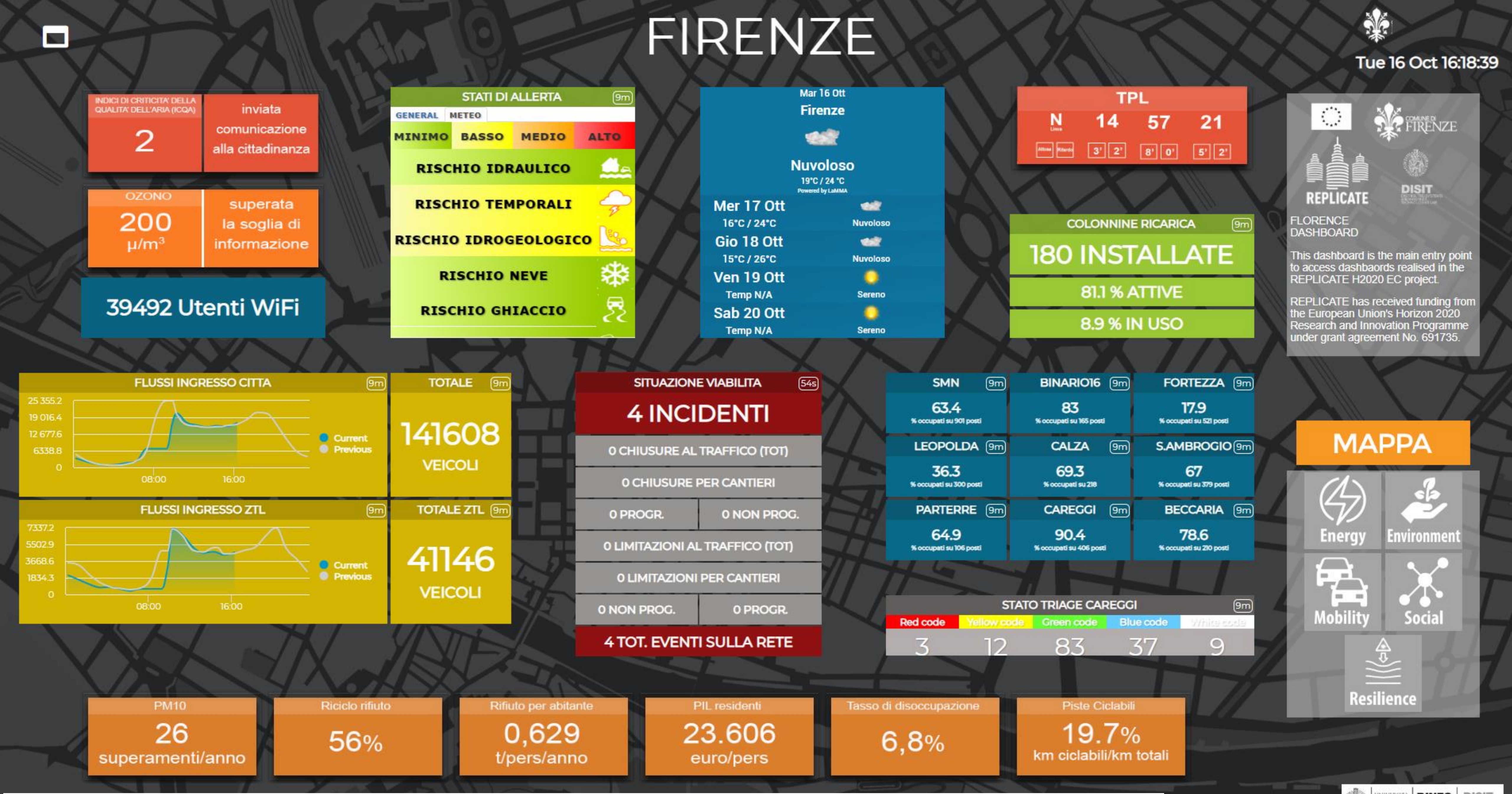
Citizens Engagement



Parking Monitoring Firenze


Segnalazioni Aperte


Tempi Medi Trasporto pubblico Linee



FIRENZE

Tue 16 Oct 16:18:39

INDICI DI CRITICITA' DELLA QUALITA' DELL'ARIA (ICQA)
2
inviata comunicazione alla cittadinanza

OZONO
200 μ/m³
superata la soglia di informazione

39492 Utenti WiFi

STATI DI ALLERTA 9m
GENERAL | METEO
MINIMO | BASSO | MEDIO | ALTO
RISCHIO IDRAULICO
RISCHIO TEMPORALI
RISCHIO IDROGEOLOGICO
RISCHIO NEVE
RISCHIO GHIACCIO

Mar 16 Ott
Firenze
Nuvoloso
19°C / 24 °C
Powered by LaMMA

Mer 17 Ott 16°C / 24°C	Nuvoloso
Gio 18 Ott 15°C / 26°C	Nuvoloso
Ven 19 Ott Temp N/A	Sereno
Sab 20 Ott Temp N/A	Sereno

TPL

N Linea	14	57	21
Attesa Ritardo	3' 2'	8' 0'	5' 2'

COLONNINE RICARICA 9m
180 INSTALLATE
81.1 % ATTIVE
8.9 % IN USO

REPLICATE
DISIT
FLORENCE DASHBOARD

This dashboard is the main entry point to access dashbaords realised in the REPLICATE H2020 EC project.

REPLICATE has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 691735.

FLUSSI INGRESSO CITTA 9m

TOTALE 9m
141608
VEICOLI

FLUSSI INGRESSO ZTL 9m

TOTALE ZTL 9m
41146
VEICOLI

SITUAZIONE VIABILITA 54s
4 INCIDENTI
0 CHIUSURE AL TRAFFICO (TOT)
0 CHIUSURE PER CANTIERI
0 PROGR. | 0 NON PROG.
0 LIMITAZIONI AL TRAFFICO (TOT)
0 LIMITAZIONI PER CANTIERI
0 NON PROG. | 0 PROGR.
4 TOT. EVENTI SULLA RETE

SMN 9m	BINARIO16 9m	FORTEZZA 9m
63.4 % occupati su 901 posti	83 % occupati su 165 posti	17.9 % occupati su 521 posti
LEOPOLDA 9m	CALZA 9m	S.AMBROGIO 9m
36.3 % occupati su 300 posti	69.3 % occupati su 218	67 % occupati su 379 posti
PARTERRE 9m	CAREGGI 9m	BECCARIA 9m
64.9 % occupati su 106 posti	90.4 % occupati su 406 posti	78.6 % occupati su 210 posti

STATO TRIAGE CAREGGI 9m

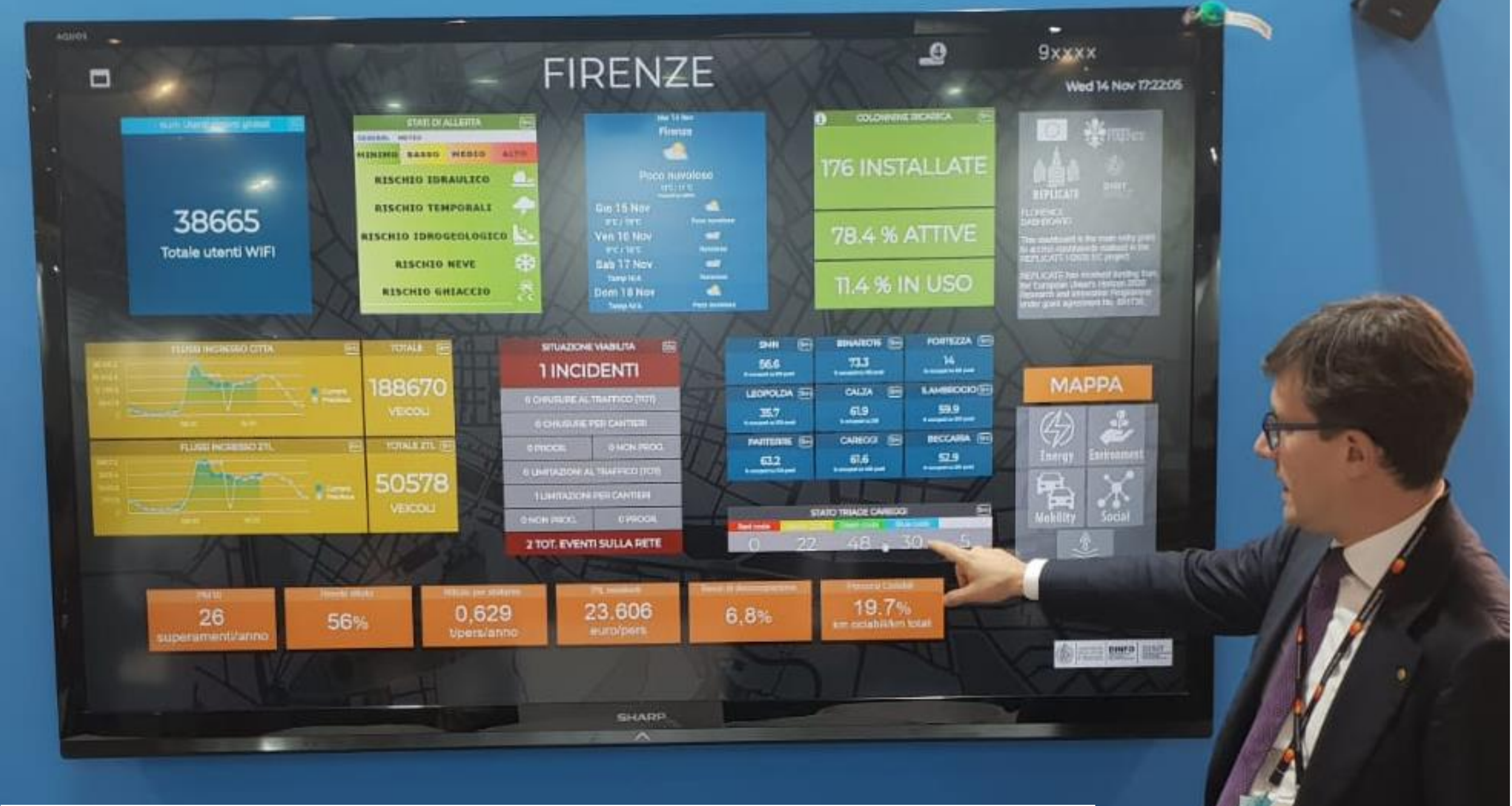
Red code	Yellow code	Green code	Blue code	White code
3	12	83	37	9

MAPPA
Energy
Environment
Mobility
Social
Resilience

PM10	Riciclo rifiuto	Rifiuto per abitante	PIL residenti	Tasso di disoccupazione	Piste Ciclabili
26 superamenti/anno	56%	0,629 t/pers/anno	23.606 euro/pers	6,8%	19.7% km ciclabili/km totali

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO | DISIT

https://main.snap4city.org/view/index.php?iddasboard=MTAwMw==



http://www.darionardella.it/il-sindaco-dario-nardella-in-missione-a-madrid-e-barcellona/

UNIVERSITÀ DEGLI STUDI FIRENZE

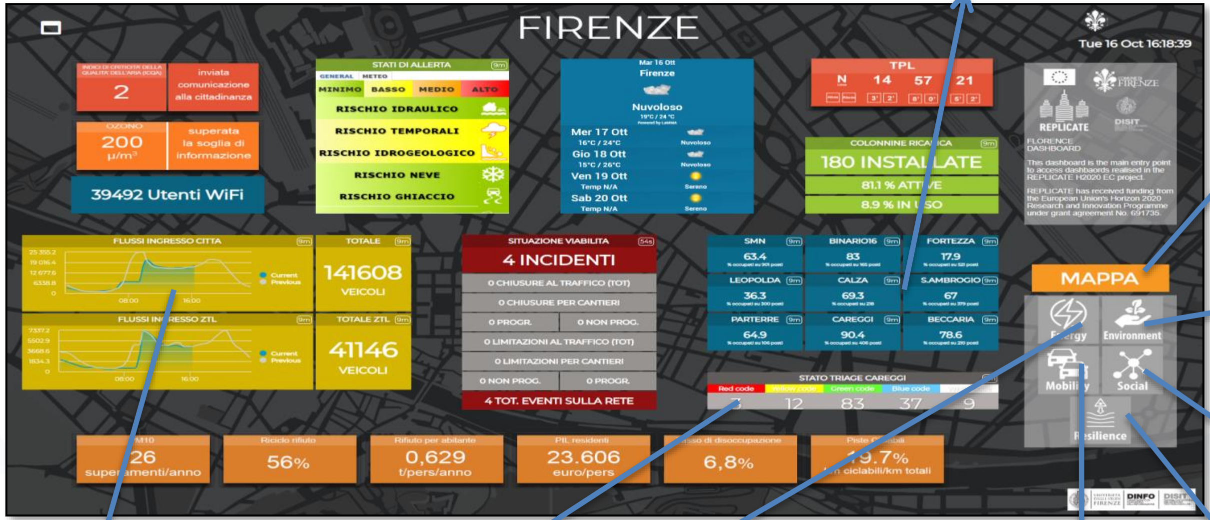
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

REPLICATE

Parcheggi Firenze App

MAIN


FIRENZE

Tue 16 Oct 16:18:39

INDICI DI CRITICITA' DELLA QUALITA' DELL'ARIA (ICQA) 2 — inviata comunicazione alla cittadinanza

OZONO 200 μ/m³ — superata la soglia di informazione

39492 Utenti WiFi

STATI DI ALLERTA (9m)

GENERAL METEO

MINIMO BASSO MEDIO ALTO

RISCHIO IDRAULICO

RISCHIO TEMPORALI

RISCHIO IDROGEOLOGICO

RISCHIO NEVE

RISCHIO GHIACCIO

Mar 16 Ott
Firenze
Nuvoloso
19°C / 24 °C
Powered by LaMMA

Mer 17 Ott 16°C / 24°C	Nuvoloso
Gio 18 Ott 15°C / 26°C	Nuvoloso
Ven 19 Ott Temp N/A	Sereno
Sab 20 Ott Temp N/A	Sereno

TPL

N	14	57	21
	3' 2'	8' 0'	5' 2'

COLONNINE RICARICA (9m)
180 INSTALLATE
81.1 % ATTIVE
8.9 % IN USO

REPLICATE

DISIT

FLORENCE DASHBOARD

This dashboard is the main entry point to access dashbaords realised in the REPLICATE H2020 EC project.

REPLICATE has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No. 691735.

FLUSSI INGRESSO CITTA (9m) — Current, Previous

TOTALE (9m) 141608 VEICOLI

FLUSSI INGRESSO ZTL (9m) — Current, Previous

TOTALE ZTL (9m) 41146 VEICOLI

SITUAZIONE VIABILITA (54s)
4 INCIDENTI
0 CHIUSURE AL TRAFFICO (TOT)
0 CHIUSURE PER CANTIERI
0 PROGR. | 0 NON PROG.
0 LIMITAZIONI AL TRAFFICO (TOT)
0 LIMITAZIONI PER CANTIERI
0 NON PROG. | 0 PROGR.
4 TOT. EVENTI SULLA RETE

SMN (9m)	BINARIO16 (9m)	FORTEZZA (9m)
63.4 % occupati su 901 posti	83 % occupati su 165 posti	17.9 % occupati su 521 posti
LEOPOLDA (9m)	CALZA (9m)	S.AMBROGIO (9m)
36.3 % occupati su 300 posti	69.3 % occupati su 218	67 % occupati su 379 posti
PARTERRE (9m)	CAREGGI (9m)	BECCARIA (9m)
64.9 % occupati su 106 posti	90.4 % occupati su 406 posti	78.6 % occupati su 210 posti

STATO TRIAGE CAREGGI

Red code	Yellow code	Green code	Blue code	White code
3	12	83	37	9

MAPPA

Energy Environment Mobility Social Resilience

PM10	Riciclo rifiuto	Rifiuto per abitante	PIL residenti	Tasso di disoccupazione	Piste Ciclabili
26 superamenti/anno	56%	0,629 t/pers/anno	23.606 euro/pers	6,8%	19.7% km ciclabili/km totali

UNIVERSITÀ DEGLI STUDI FIRENZE DINFO DISIT

MAPPA FIRENZE

Tue 16 Oct 16:40:17

4CITY

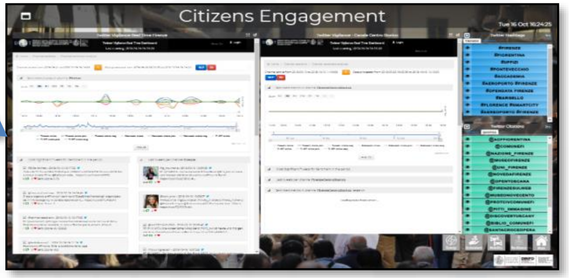
Environment

Tue 16 Oct 16:21:59

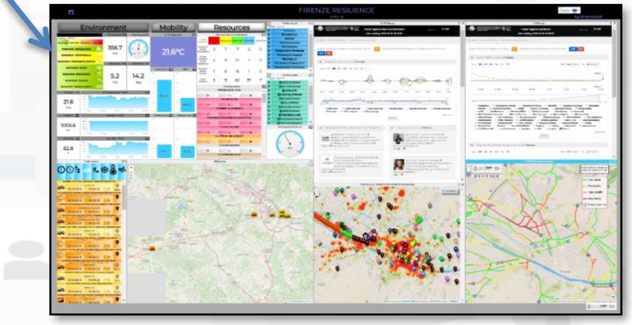
Air quality | Weather sensors | Pollen monitoring

Firenze

47m

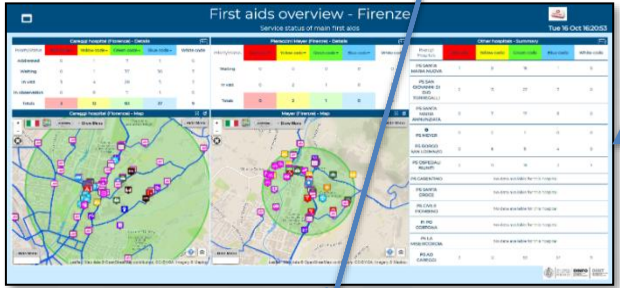

Citizens Engagement

Tue 16 Oct 16:24:26


FIRENZE RESILIENCE

Environment | Mobility | Resources

21.6°C


First aids overview - Firenze

Service status of main first aids

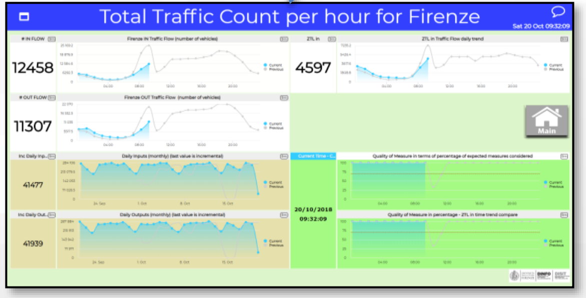
Tue 16 Oct 16:20:53

Energy

Tue 16 Oct 16:21:39

82.3% | 36.4% | 38.8%

45 users | 196177 kWh


Total Traffic Count per hour for Firenze

Sat 20 Oct 09:32:09

IN FLOW	12458	ZTL in	4597
OUT FLOW	11307		
	41477		
	41939		

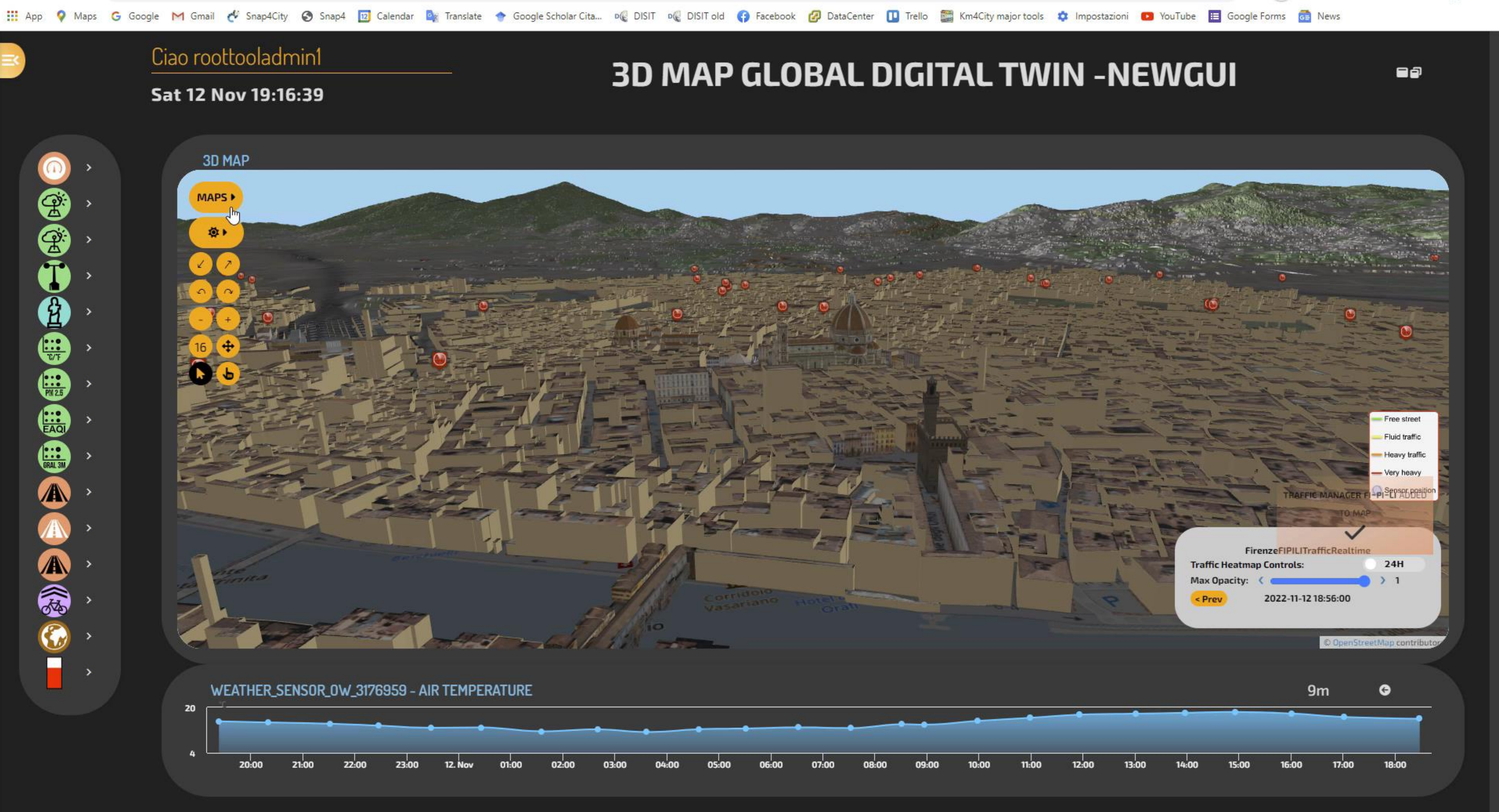
20/10/2018 09:32:09

Main

Mobility

Sat 20 Oct 09:30:45

479 Free | 431 Free | 298



Ciao roottooladmin1

Sat 12 Nov 19:16:39

3D MAP GLOBAL DIGITAL TWIN -NEWGUI

3D MAP

TRAFFIC MANAGER FI-PI-LI ADDED TO MAP

FirenzeFIPILITrafficRealtime

Traffic Heatmap Controls: 24H

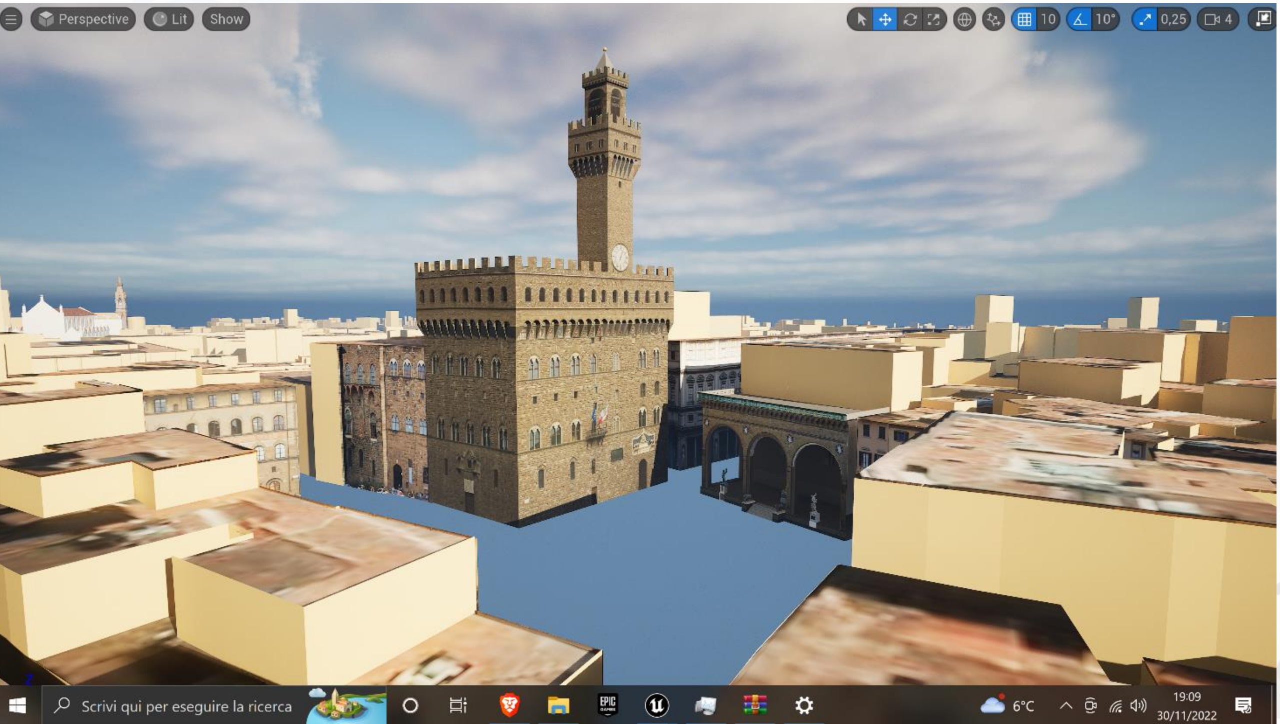
Max Opacity: 1

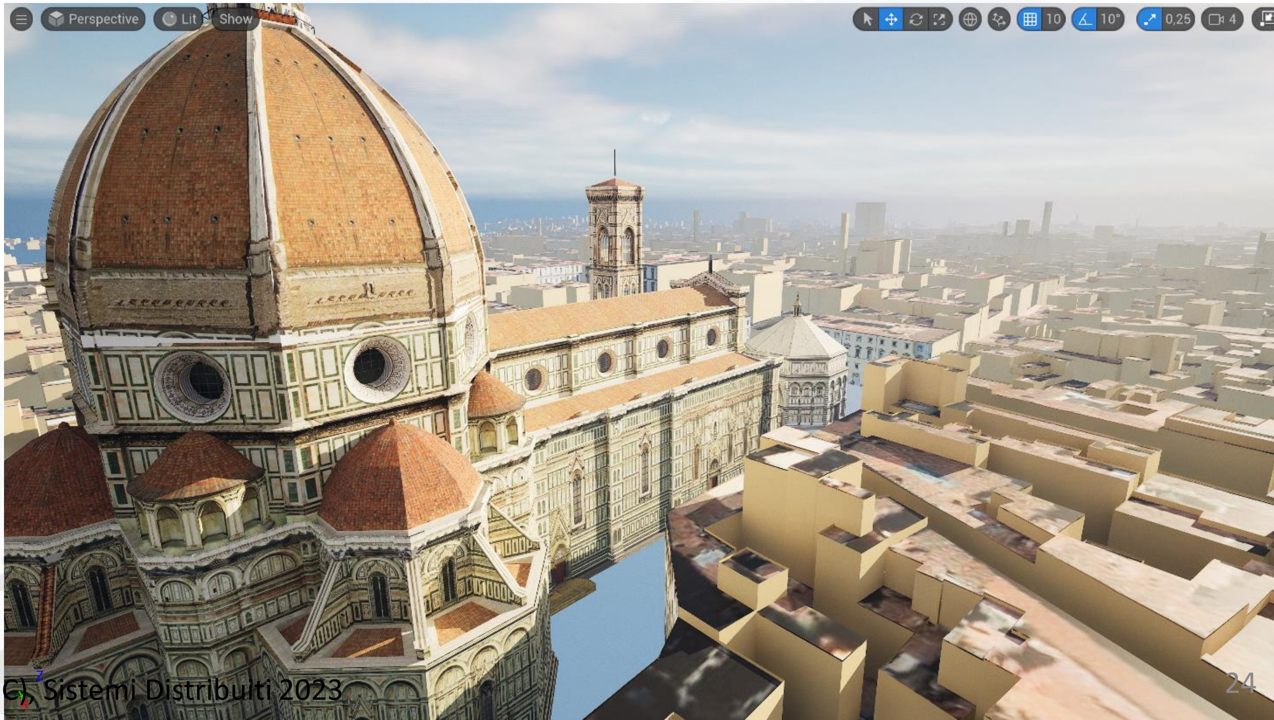
< Prev 2022-11-12 18:56:00

WEATHER_SENSOR_OW_3176959 - AIR TEMPERATURE 9m

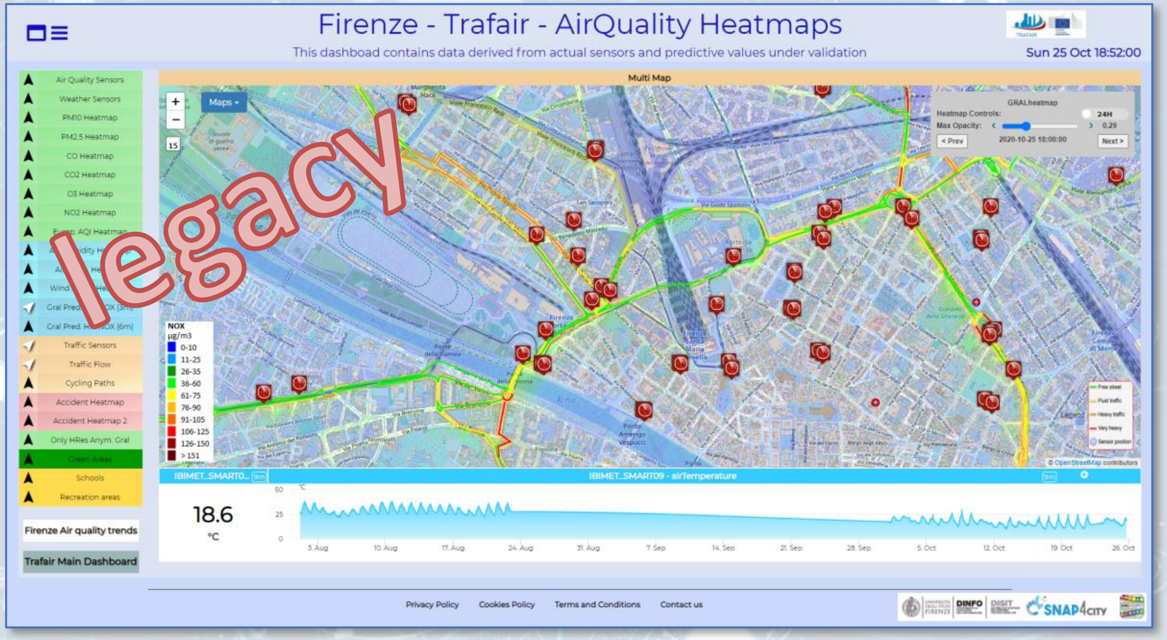
OCULUS

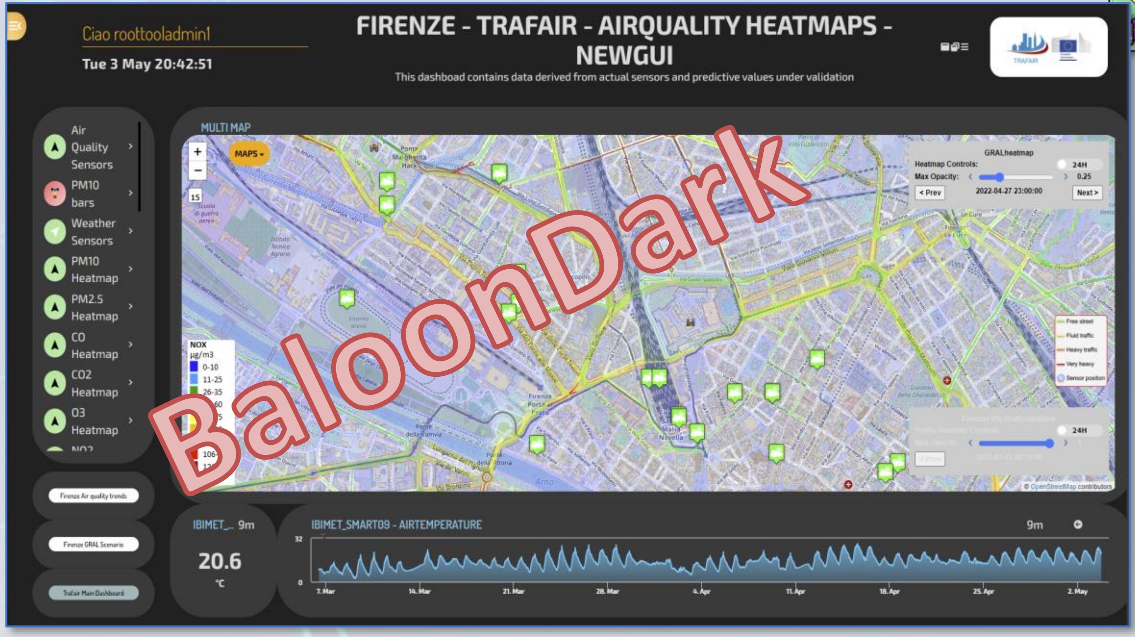
oculus

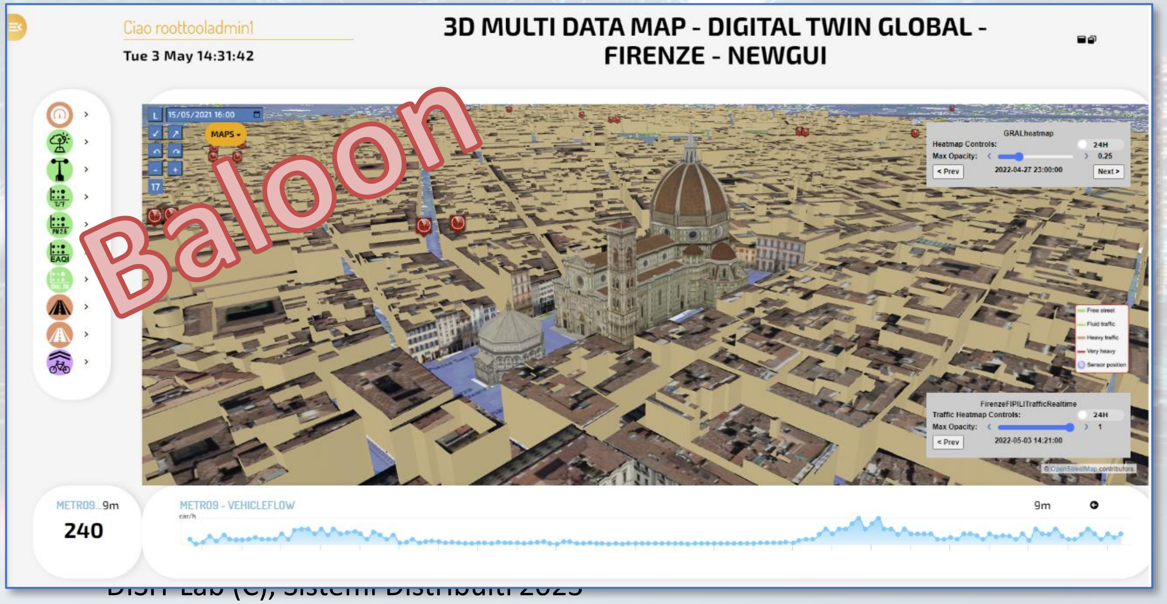

Perspective
Lit
Show
10
10°
0,25
4
Scrivi qui per eseguire la ricerca
6°C
19:09
30/11/2022

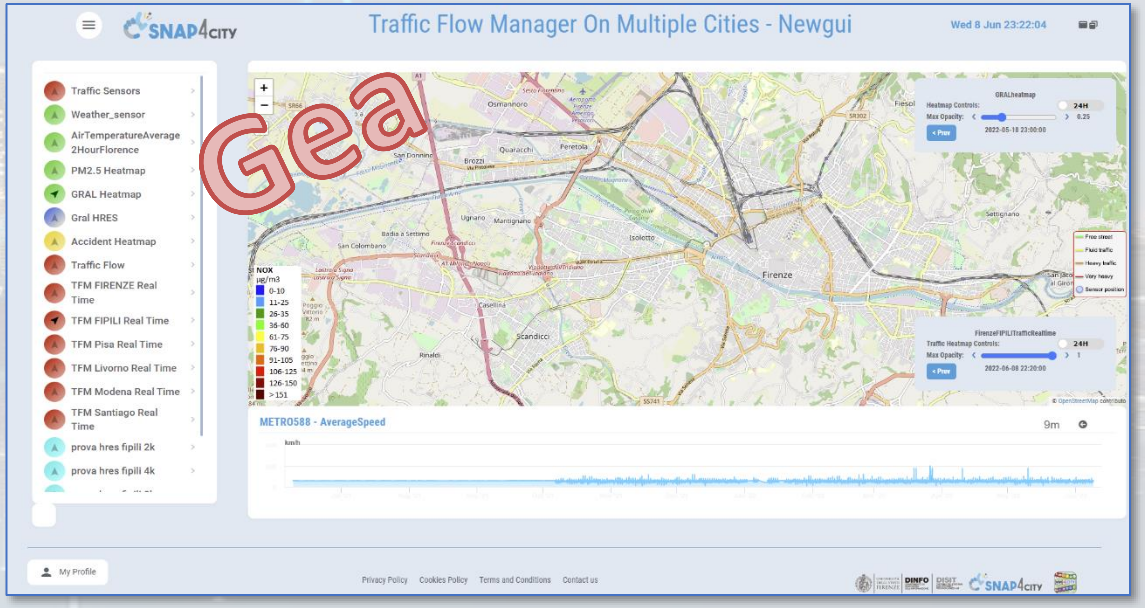

Perspective
Lit
Show
10
10°
0,25
4

Different Themes

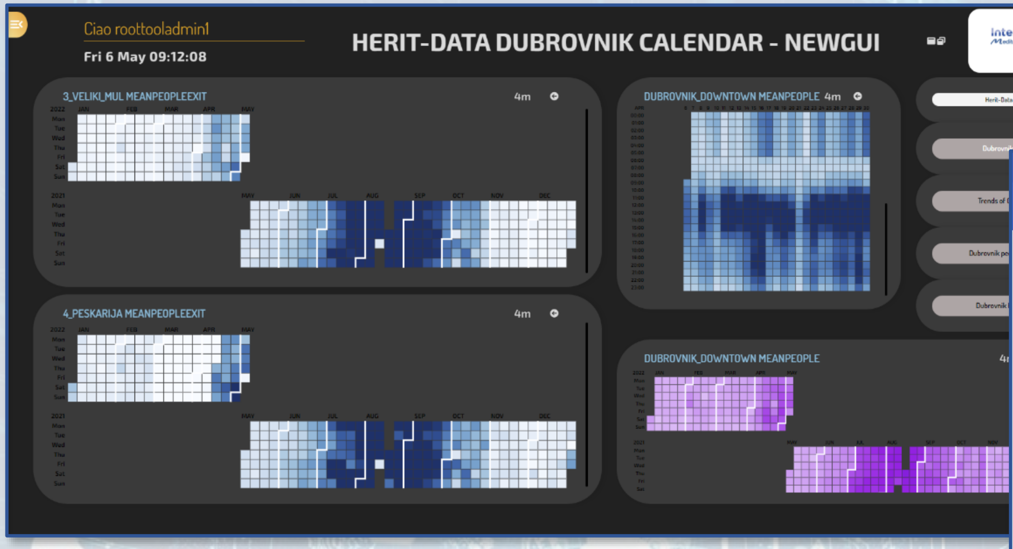


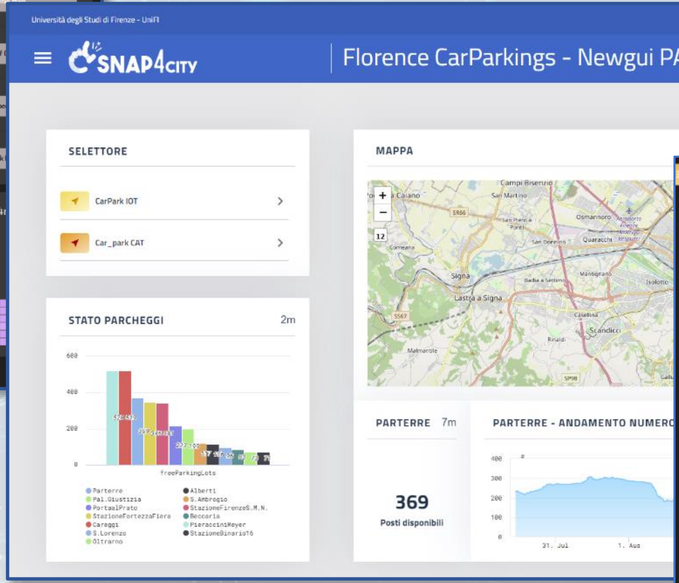


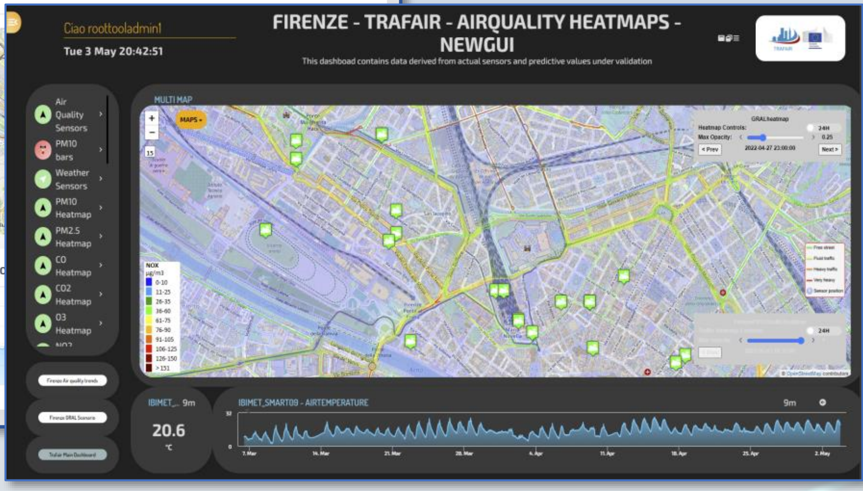


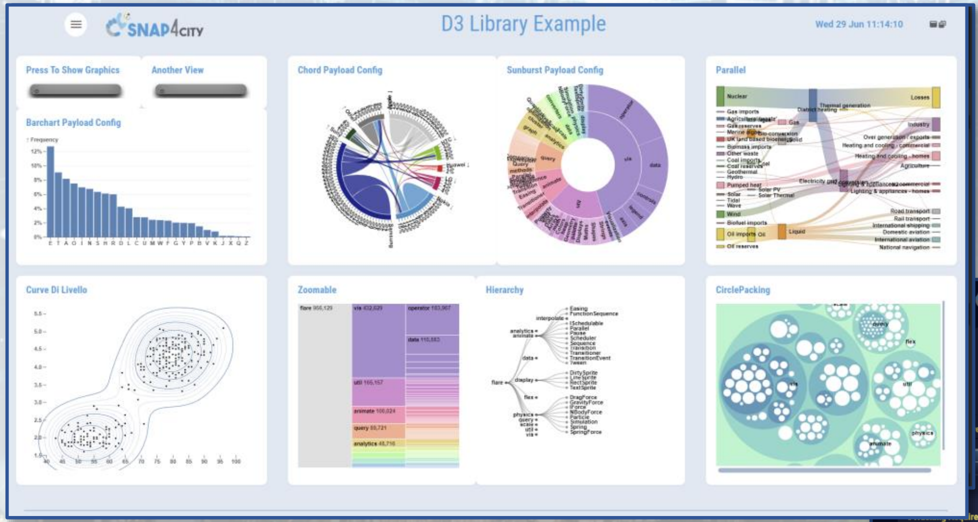


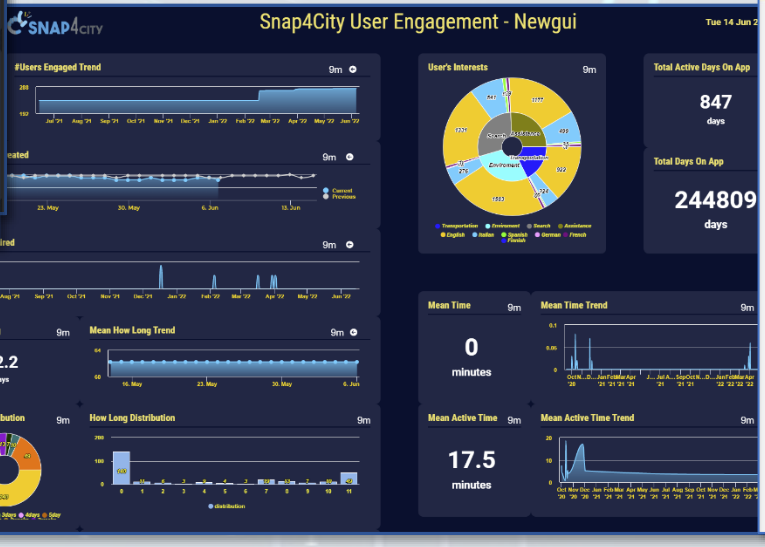
Different Themes

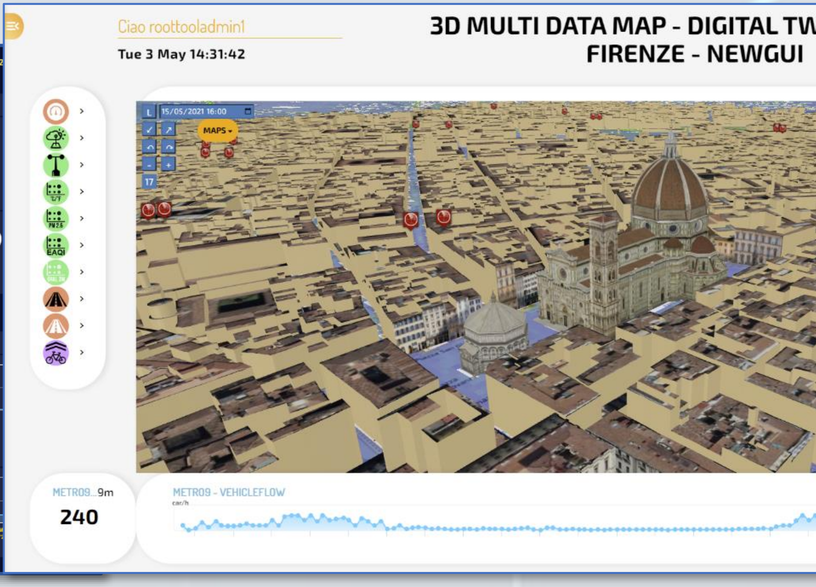

Ciao roottooladmin1
Fri 6 May 09:12:08
HERIT-DATA DUBROVNIK CALENDAR - NEWGUI
Interreg Mediterranean HERIT-DATA
3_VELIKI_MUL MEANPEOPLEEXIT
4m
DUBROVNIK_DOWNTOWN MEANPEOPLE
4_PESKARIJA MEANPEOPLEEXIT
Herit-Data Main
Dubrovnik Main
Trends of
Dubrovnik




Ciao roottooladmin1
Tue 3 May 20:42:51
FIRENZE - TRAFAIR - AIRQUALITY HEATMAPS - NEWGUI
This dashboard contains data derived from actual sensors and predictive values under validation
Air Quality Sensors
PM10 bars
Weather Sensors
PM10 Heatmap
PM2.5 Heatmap
CO Heatmap
CO2 Heatmap
O3 Heatmap
MULTI MAP
MAPS
IBIMET_... 9m
20.6
°C
IBIMET_SMART09 - AIRTEMPERATURE







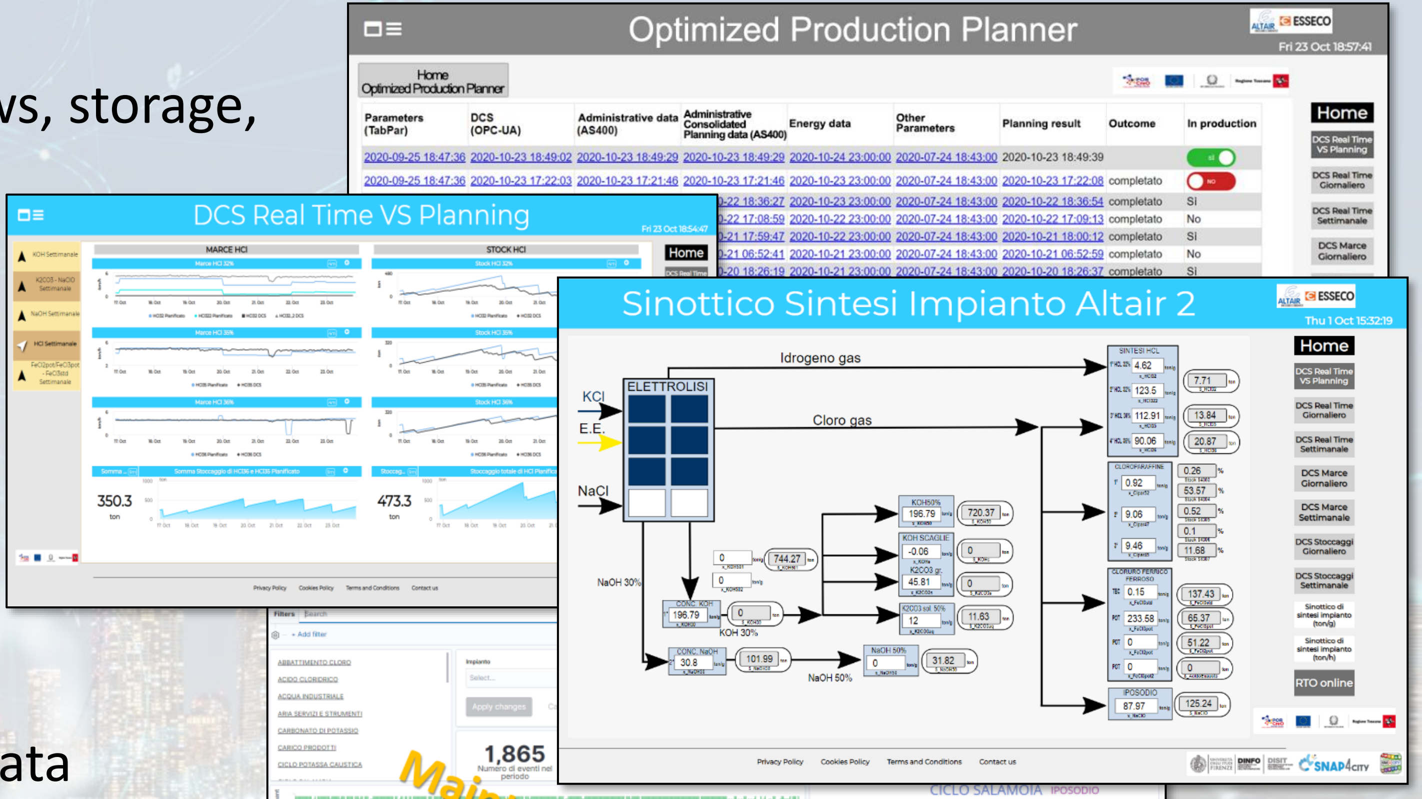
New styles/themes can be developed by specializing a few files from open source

https://www.snap4city.org/793

Snap4Altair Decision Support supervision and control, Industry 4.0

reference

- **Multiple Domain Data**
  - Distributed Control System: energy, flows, storage, chemical data, settings, ..
  - Cost of energy
  - Orders
  - Production Parameters
  - Maintenance data
- **Multiple Levels & Decision Makers**
- **Historical and Real Time data**
  - Billions of Data
  - Optimized planning on chemical model
  - Business Intelligence on Maintenance data
- **Services Exploited on:**
  - Multiple Levels, Mobile Apps, API
- **Since 2020**



Optimized Production Planner

Fri 23 Oct 18:57:41

Home
Optimized Production Planner

Parameters (TabPar)	DCS (OPC-UA)	Administrative data (AS400)	Administrative Consolidated Planning data (AS400)	Energy data	Other Parameters	Planning result	Outcome	In production
2020-09-25 18:47:36	2020-10-23 18:49:02	2020-10-23 18:49:29	2020-10-23 18:49:29	2020-10-24 23:00:00	2020-07-24 18:43:00	2020-10-23 18:49:39		si
2020-09-25 18:47:36	2020-10-23 17:22:03	2020-10-23 17:21:46	2020-10-23 17:21:46	2020-10-23 23:00:00	2020-07-24 18:43:00	2020-10-23 17:22:08	completato	NO
			0-22 18:36:27	2020-10-23 23:00:00	2020-07-24 18:43:00	2020-10-22 18:36:54	completato	Si
			0-22 17:08:59	2020-10-22 23:00:00	2020-07-24 18:43:00	2020-10-22 17:09:13	completato	No
			0-21 17:59:47	2020-10-22 23:00:00	2020-07-24 18:43:00	2020-10-21 18:00:12	completato	Si
			0-21 06:52:41	2020-10-21 23:00:00	2020-07-24 18:43:00	2020-10-21 06:52:59	completato	No
			0-20 18:26:19	2020-10-21 23:00:00	2020-07-24 18:43:00	2020-10-20 18:26:37	completato	Si

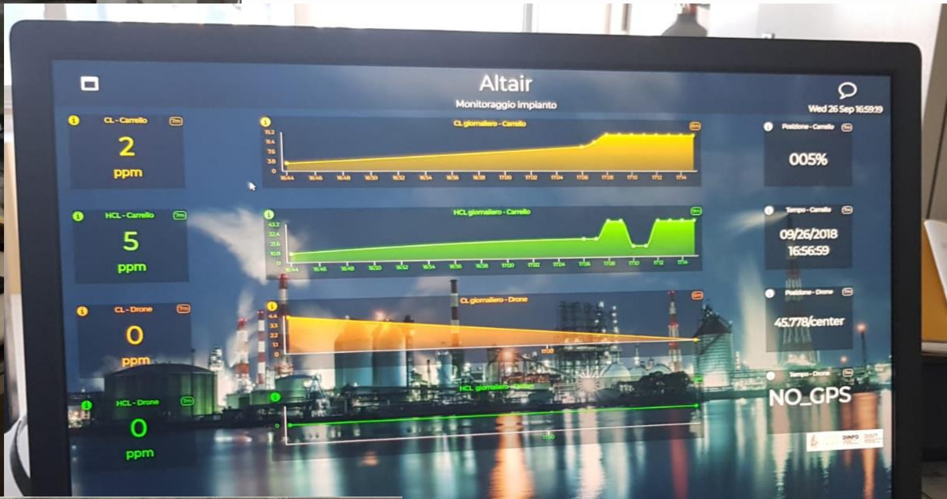
DCS Real Time VS Planning

Fri 23 Oct 18:54:47

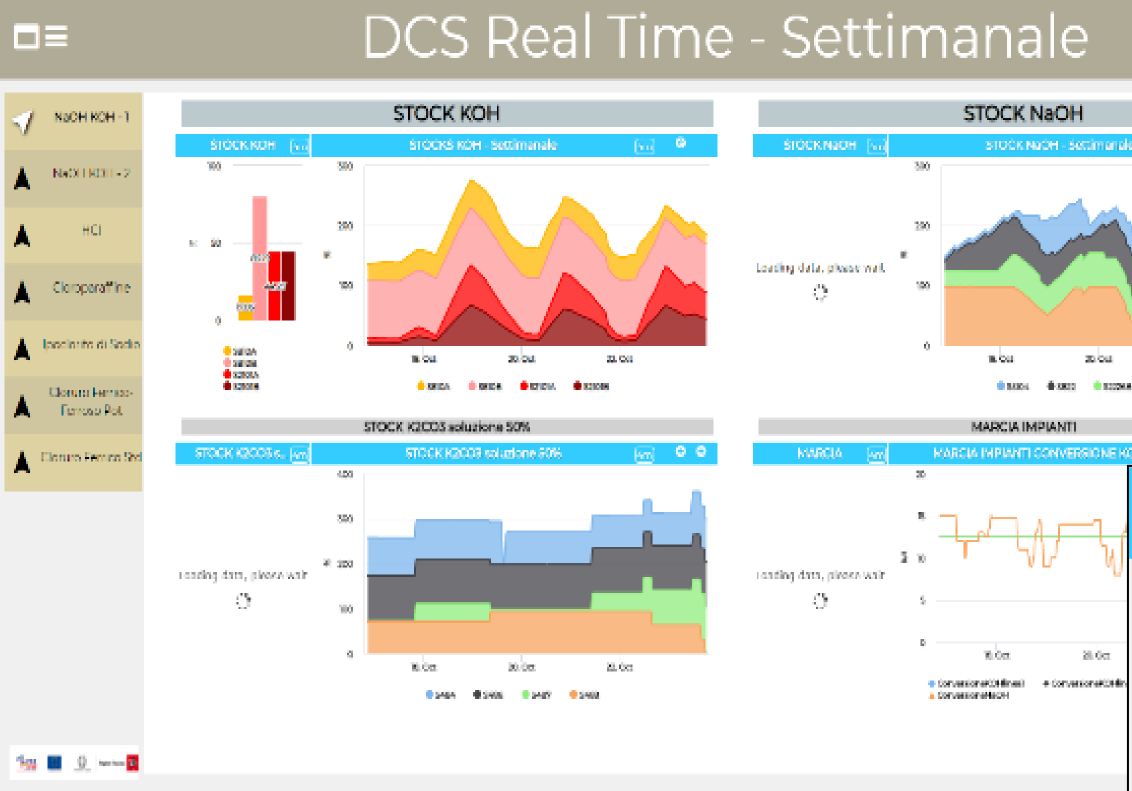
Sinottico Sintesi Impianto Altair 2

Thu 1 Oct 15:32:19

Maintenance Intelligence

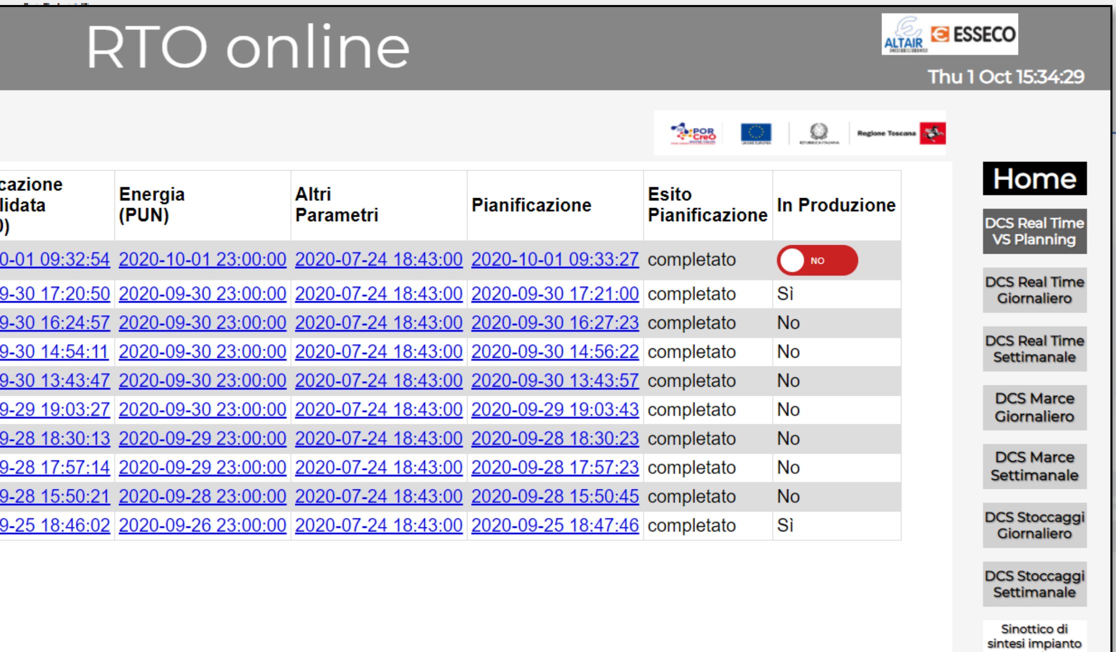


Green Impact Capacity (GIC)
Altair Control room

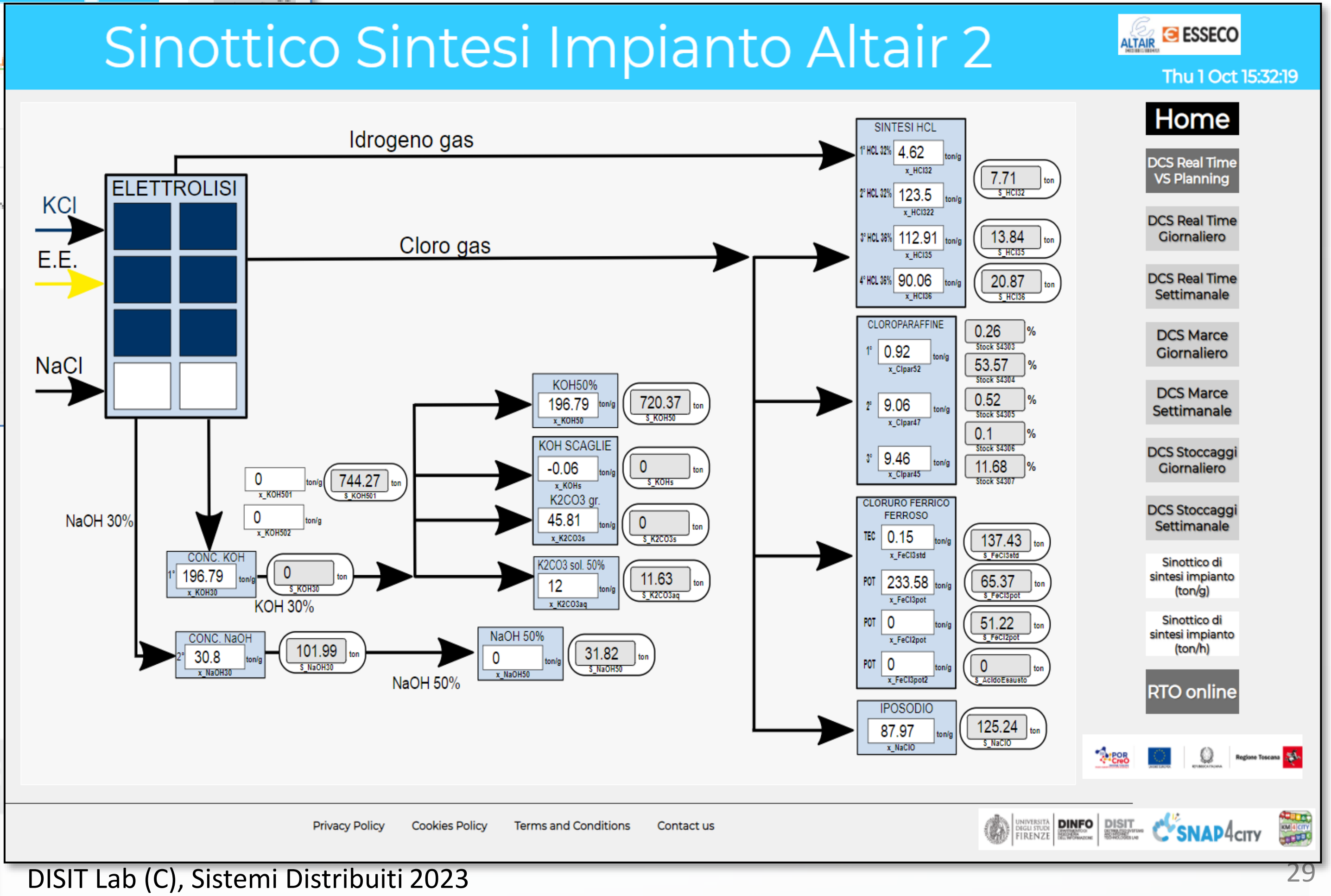


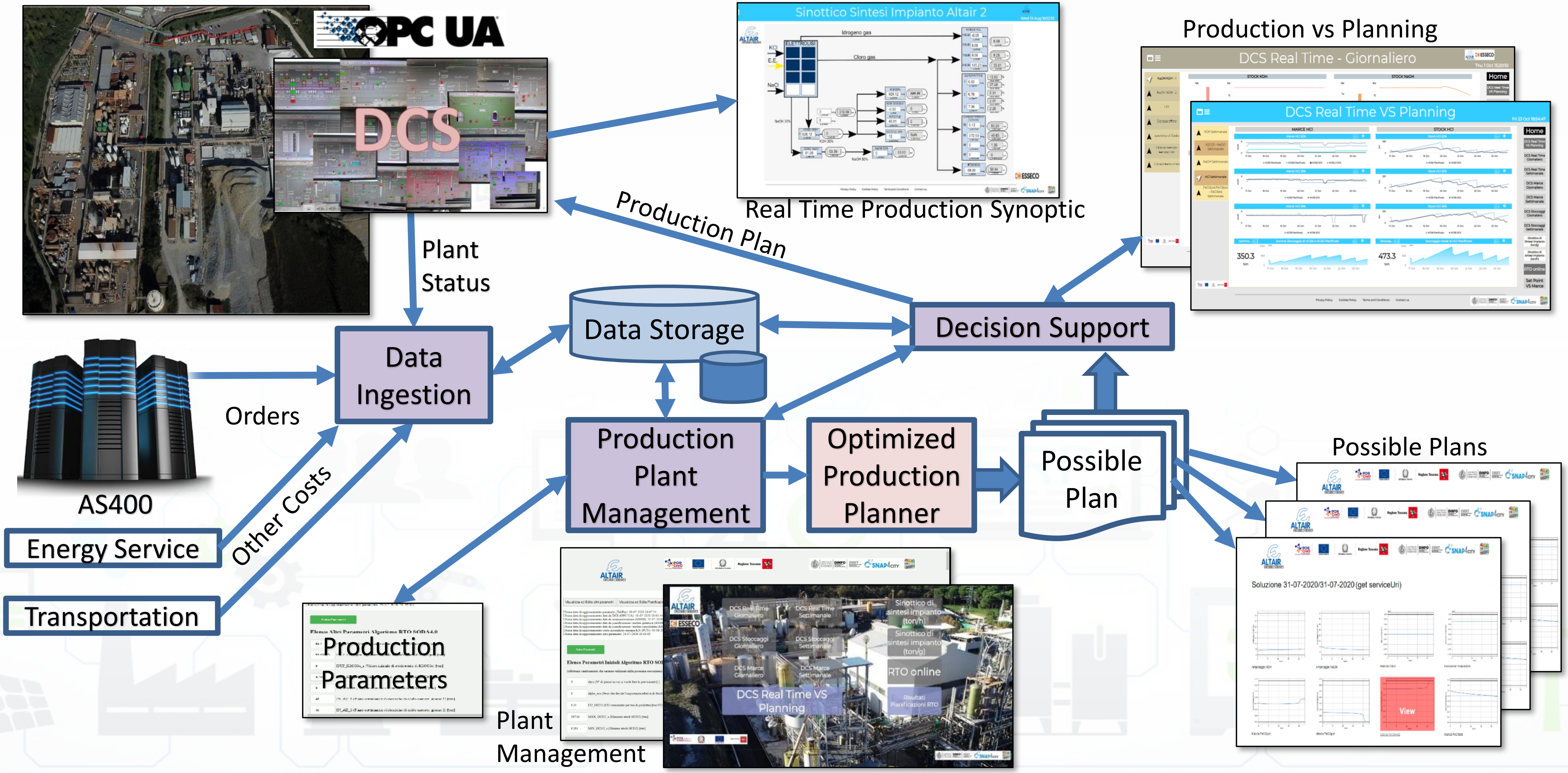
SNAP4INDUSTRY

SNAP4ALTAIR


RTO online
ALTAIR ESSECO
Thu 1 Oct 15:34:29
Home
DCS Real Time VS Planning
DCS Real Time Giornaliero
DCS Real Time Settimanale
DCS Marce Giornaliero
DCS Marce Settimanale
DCS Stoccaggi Giornaliero
DCS Stoccaggi Settimanale
Sinottico di sintesi impianto

cazione lidata)	Energia (PUN)	Altri Parametri	Pianificazione	Esito Pianificazione	In Produzione
0-01 09:32:54	2020-10-01 23:00:00	2020-07-24 18:43:00	2020-10-01 09:33:27	completato	NO
9-30 17:20:50	2020-09-30 23:00:00	2020-07-24 18:43:00	2020-09-30 17:21:00	completato	Sì
9-30 16:24:57	2020-09-30 23:00:00	2020-07-24 18:43:00	2020-09-30 16:27:23	completato	No
9-30 14:54:11	2020-09-30 23:00:00	2020-07-24 18:43:00	2020-09-30 14:56:22	completato	No
9-30 13:43:47	2020-09-30 23:00:00	2020-07-24 18:43:00	2020-09-30 13:43:57	completato	No
9-29 19:03:27	2020-09-30 23:00:00	2020-07-24 18:43:00	2020-09-29 19:03:43	completato	No
9-28 18:30:13	2020-09-29 23:00:00	2020-07-24 18:43:00	2020-09-28 18:30:23	completato	No
9-28 17:57:14	2020-09-29 23:00:00	2020-07-24 18:43:00	2020-09-28 17:57:23	completato	No
9-28 15:50:21	2020-09-28 23:00:00	2020-07-24 18:43:00	2020-09-28 15:50:45	completato	No
9-25 18:46:02	2020-09-26 23:00:00	2020-07-24 18:43:00	2020-09-25 18:47:46	completato	Sì





OPC UA

DCS

Plant Status

Sinottico Sintesi Impianto Altair 2

Real Time Production Synoptic

Production Plan

Production vs Planning

DCS Real Time - Giornaliero

DCS Real Time VS Planning

Data Storage

Data Ingestion

Decision Support

AS400

Orders

Energy Service

Transportation

Other Costs

Production Plant Management

Optimized Production Planner

Possible Plan

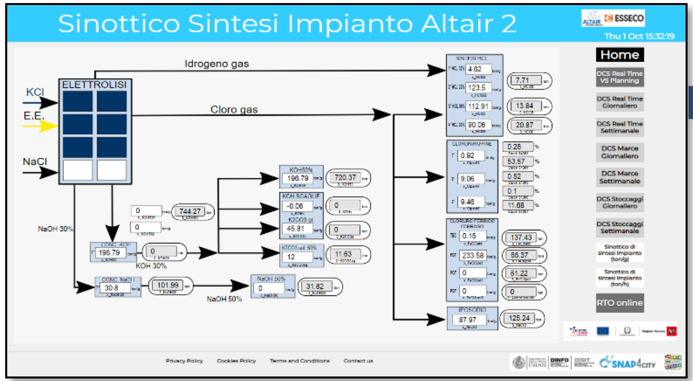
Possible Plans

Production Parameters

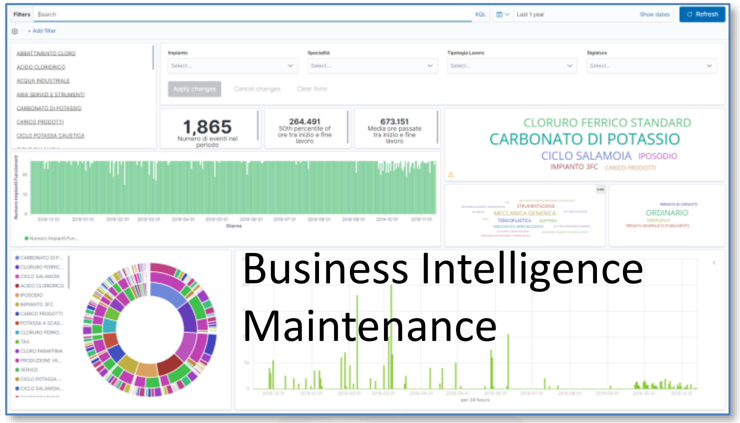
Plant Management

Idrogeno gas
Cloro gas
ELETTROLISI
KCl
E.E.
NaCl
ESSECO
Home
350.3
473.3
ALTAIR
Soluzione 31-07-2020/31-07-2020 (get serviceUri)
View
DCS Real Time Giornaliero
DCS Real Time Settimanale
DCS Stoccaggi Giornaliero
DCS Stoccaggi Settimanale
DCS Marce Giornaliero
DCS Marce Settimanale
DCS Real Time VS Planning
Sinottico di sintesi impianto (ton/h)
Sinottico di sintesi impianto (ton/g)
RTO online
Risultati Pianificazioni RTO
Elenco Altri Parametri Algoritmo RTO SODA4.0
Elenco Parametri Iniziali Algoritmo RTO

Workflow for Ticket management


Sinottico Sintesi Impianto Altair 2
ESSECO
Thu 1 Oct 15:32:19
Idrogeno gas
Cloro gas
KCl
E.E.
NaCl
ELETTROLISI
NaOH 30%
KOH 30%
NaOH 50%
Home
DCS Real Time VS Planning
DCS Real Time Giornaliero
DCS Real Time Settimanale
DCS Marce Giornaliero
DCS Marce Settimanale
DCS Stoccaggi Giornaliero
DCS Stoccaggi Settimanale
Sinottico di sintesi impianto (ton/g)
Sinottico di sintesi impianto (ton/h)
RTO online
Privacy Policy
Cookies Policy
Terms and Conditions
Contact us

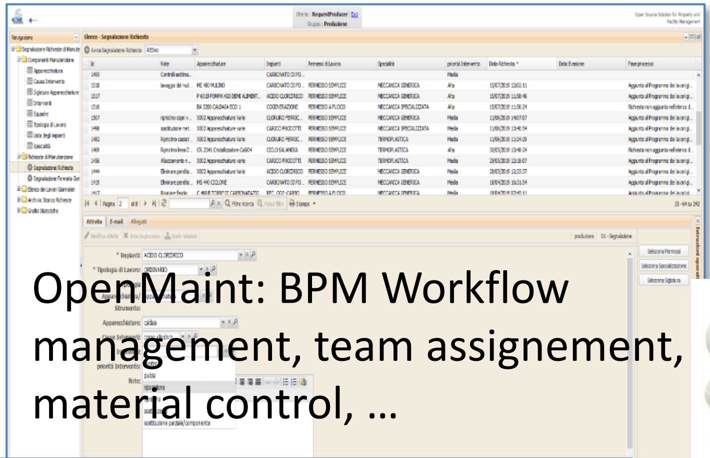
Consumptions/productions



Business Intelligence

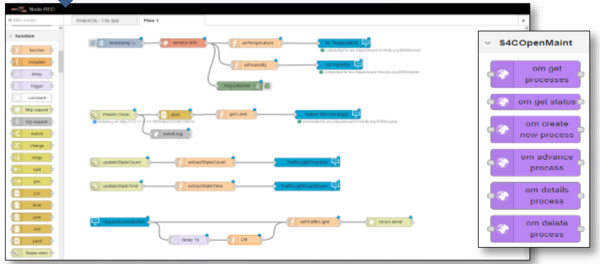
Maintenance

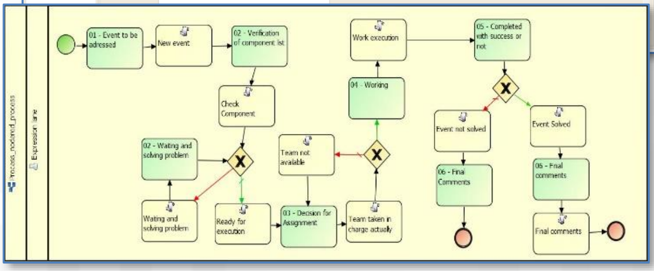
Events/actions



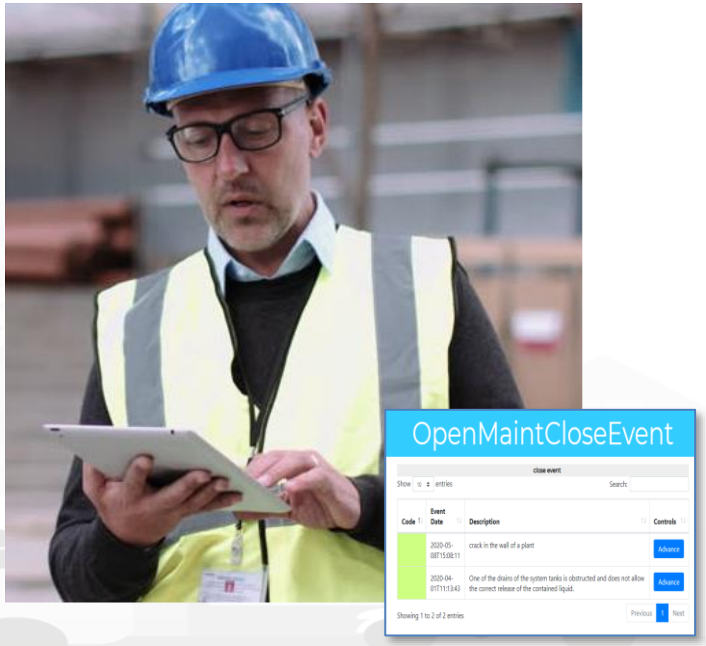
OpenMaint: BPM Workflow management, team assignement, material control, …

Dashboards and actions




Process_notmod_process
Expression lane
01 - Event to be adressed
New event
02 - Verification of component list
Work execution
05 - Completed with success or not
04 - Working
Check Component
Event not solved
Event Solved
02 - Waiting and solving problem
Team not available
06 - Final Comments
06 - Final comments
Waiting and solving problem
Ready for execution
03 - Decision for Assignment
Team taken in charge actually
Final comments

IOT App, Data event firing, event detection and firing Critical event management



OpenMaintCloseEvent

close event

Show 10 entries Search:

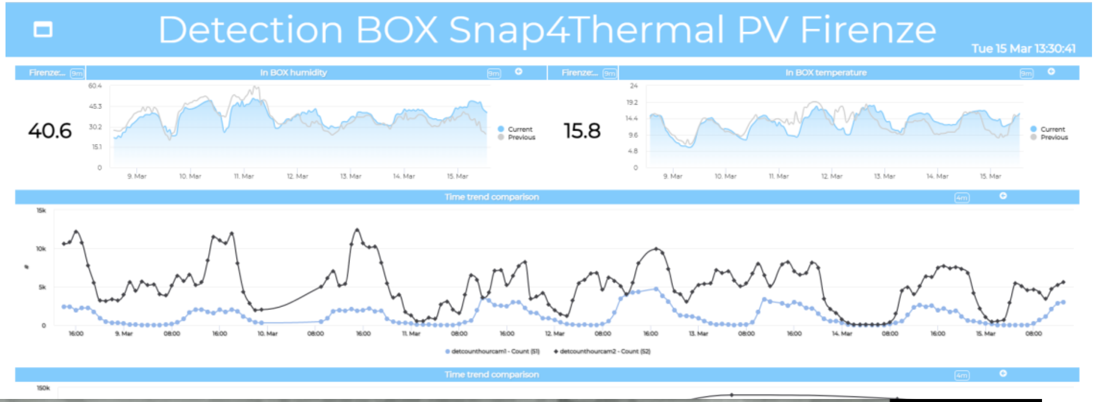
Code	Event Date	Description	Controls
🟩	2020-05-08T15:08:11	crack in the wall of a plant	Advance
🟩	2020-04-01T11:13:43	One of the drains of the system tanks is obstructed and does not allow the correct release of the contained liquid.	Advance

Showing 1 to 2 of 2 entries Previous 1 Next

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

Interreg Mediterranean | HERIT-DATA | AXIS COMMUNICATIONS | SNAP4CITY | KM4CITY

A view and data from the Thermal Camera



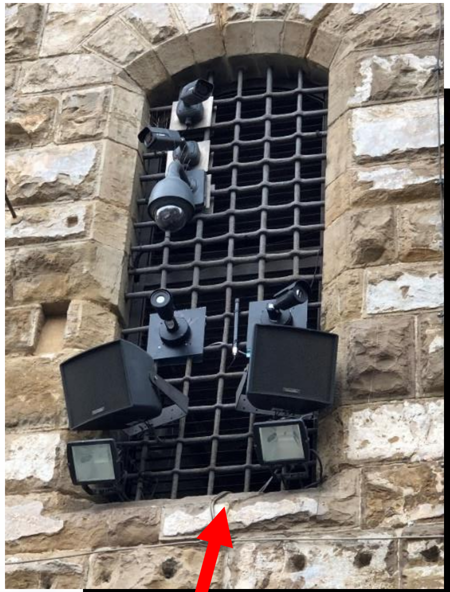
Detection BOX Snap4Thermal PV Firenze

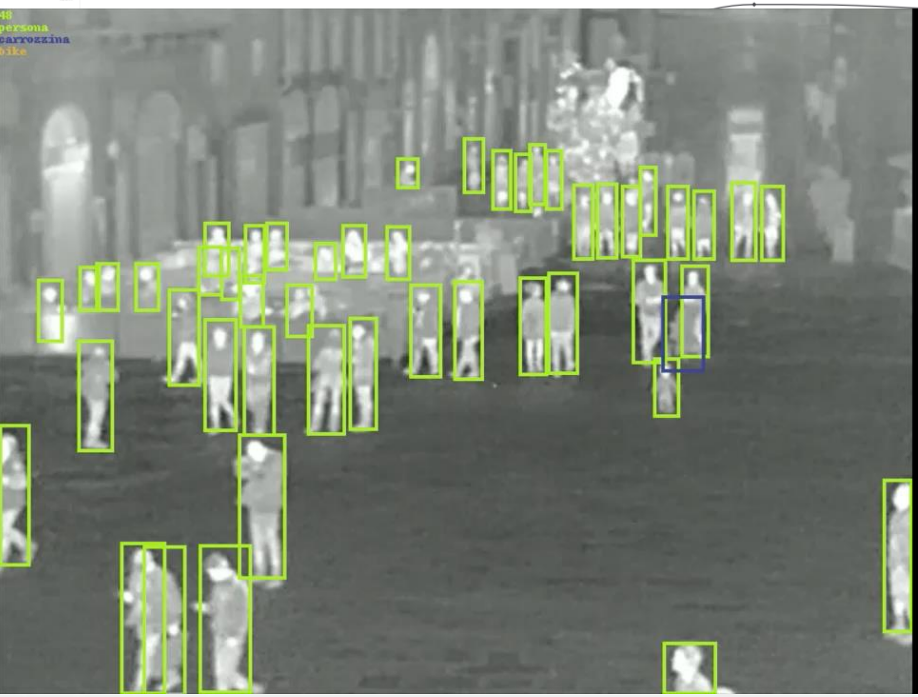
Tue 15 Mar 13:30:41

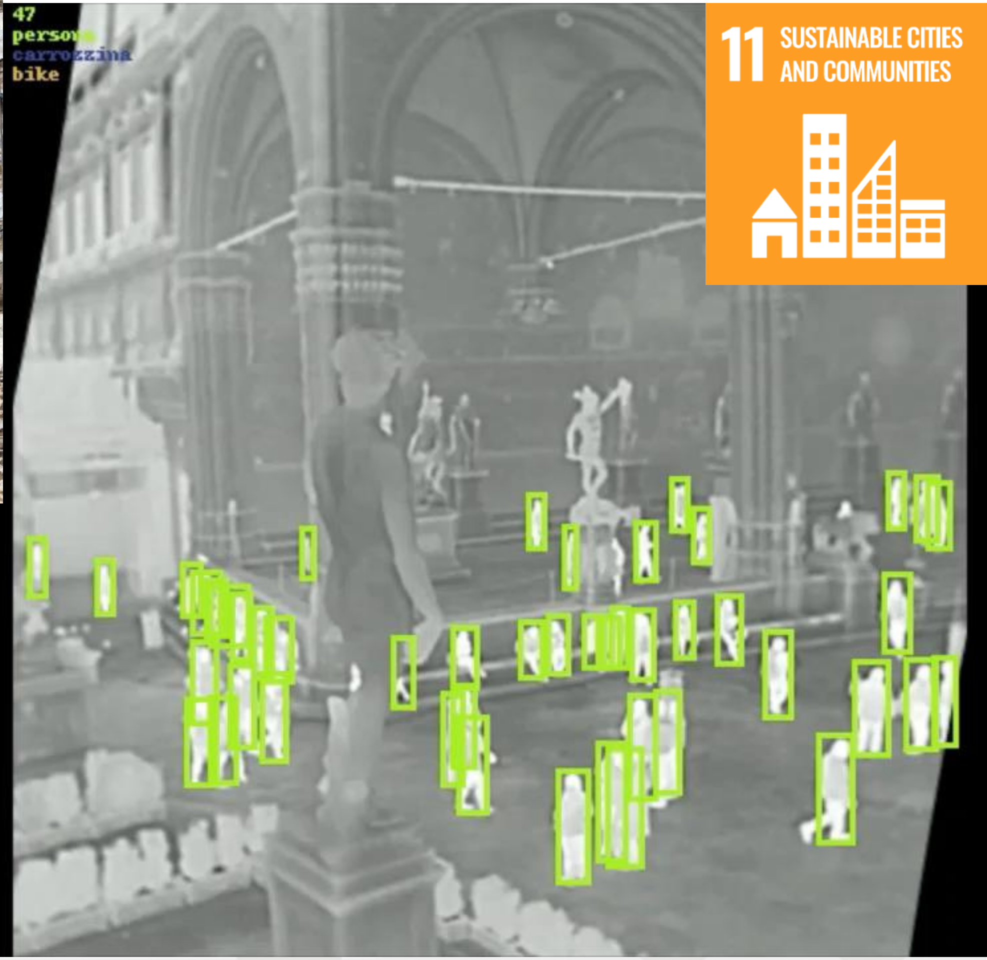
In BOX humidity: 40.6

In BOX temperature: 15.8

Time trend comparison







11 SUSTAINABLE CITIES AND COMMUNITIES

Available Data Analytics

- **Mobility and Transport**
- **City Users and Social**
- **Environment and Weather**
- **Time Series**
- **Semantic Reasoning**
- **Matrices, Images, Maps and 3D Digital Models**
- **Management and strategies**
- **Resilience and Risks Analysis**

https://www.snap4city.org/download/video/course/da/

Part 2 on Data Security and Privacy by Paolo Nesi

Data Protection, Privacy and GDPR, IoT Security and Blockchain

University of Florence, DISIT lab, Https://www.disit.org

Https://www.snap4city.org

Paolo.nesi@unifi.it

Struttura di questo modulo

- Data protection
- GDPR
- IOT Network Security
- BlockChain

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB

www.disit.org

Course: Security and Privacy

Part on Privacy by Paolo Nesi

Topic: Data Protection

University of Florence, DISIT lab, Https://www.disit.org

Https://www.snap4city.org

Paolo.nesi@unifi.it

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Content Services Aspects

- **Scalability**:
  - From a few to millions of transactions per hours
  - From a few to millions of subscribed users
  - From a few to millions of different content items
- **Availability and**
  - High reliability of the service, no or few interruptions → HA
- **Accessibility:**
  - Accessibility of the service, broadcast, mobile coverage
  - User accessibility aspects
- ***Other aspects discussed in the course***
  - ***Privacy of the customers***
  - ***Intellectually property management and protection, IPMP***
  - ***Multichannel distribution***
  - ***Interoperability of content on devices***

- **Architectures**

A. **Content/good *distribution***
B. **Content/good *production and management***
C. **Content/good *Protection and Security***
D. **Content/good *Modeling and Processing***

A) Content distribution models

- **Download, P2P download, …:**
  - 1:N: one sender N receivers/users
  - N copies, propagation of seeding/sources sites
  - Network costs from O(N) → O(1)
  - → ecommerce, any web site
- **Broadcast Streaming (e.g., MPEG2-TS)**:
  - 1:N: one sender N receivers/users
  - N users that play the same content at the same time
  - Network costs O(1)
  - → DVB-T, DVB-S, DVB-H, DVB-SH
- **VOD, progressive download, P2P streaming/progressive:**
  - 1:1 stream processes, one sender process for each receiver/user, that play the same content a different time
  - Network costs O(N) -→ may be going to O(1) if ….
  - → Netflix, Disney+, Sky on demand, …

B) Content production and management

- **Content Processing:**
  - adaptation,
  - production,
  - formatting,
  - packing,
  - protection etc.

- **Scalability GRID for content processing:**
  - User generated content management
  - Indexing for search
  - production on demand
  - massive production
  - transcoding

C) Content Protection and Security, aspects

- CP: Copy Protection
- CAS: Conditional Access Systems
- DRM: Digital Rights Management

- Based on technologies such as
  - **Certification** of: content, users, devices, etc.
  - **Authentication** of: users, actors, devices, etc.
  - **Authorization** of: users, groups, communities, …
  - **Rights** coding: authorized functionalities, actions, etc.
  - **Signature** of: content, DLL, EXE, ..
  - **Identification** of: content, users, devices, etc.
  - **Watermark** and **fingerprint** of: content, descriptors, ...any....
  - **Coding** and Encryption of: ......everything.....

D) Content Modeling and Processing

- **The content model impacts on:**
  - **Format: XML, JSON, binary**
  - **Content gathering and ingestion**
  - **Production and production-process definition**
    - Workflow Management systems
    - Cooperative work
  - **CMS, DMS, Content/Media Management Systems**
    - Database management systems
    - query support, distributed queries, etc.
  - **CRM: Customer Relationship Management**
    - Managing relationships with clients: business models, marketing
  - **Content description for**
    - Search, classification/indexing, retrieval
  - **Content protection for enforcing respect of**
    - IPR: CAS, DRM, ...
  - **Metadata: programme/guide production**
    - EPG, GuidePlus, ShowView, TVAnytime, etc.

Acronyms and Definitions

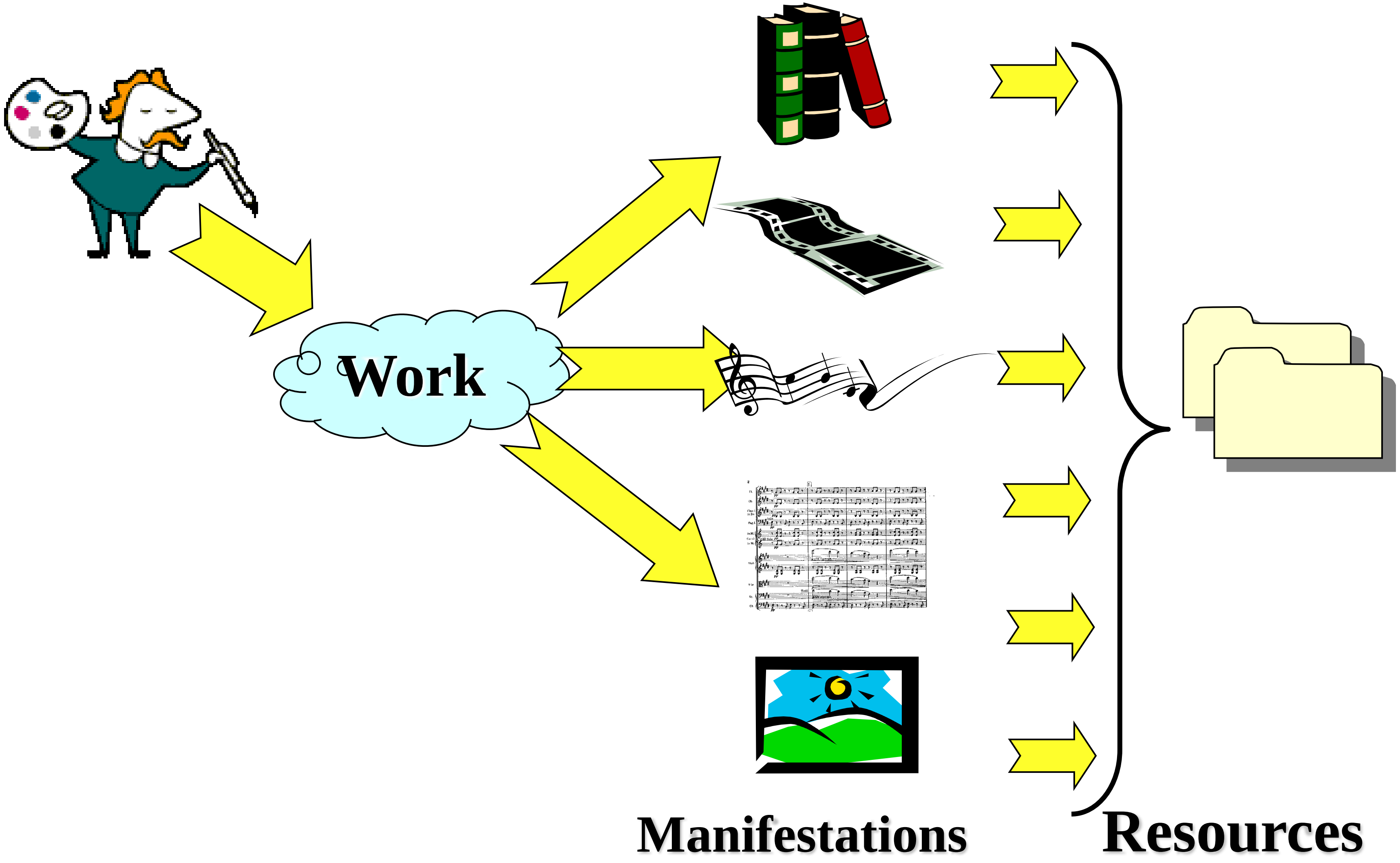
- IPR: Intellectually Property Right
- CA: Certification Authority, chain of certificates
- TPM: Technological Protection Model
- FTA: Fault Tolerance Architectures
- HA: high availability, 99.999% uptime
- VOD: video on demand
- PPP: pay per play
- PPV: pay per view
- VOIP: voice over IP
- TS: Transport Stream
- GDPR: General Data Protection Regulation
- EPG: electronic program guide
- Etc.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Terminology

- The user/artist creates a Work
- The work may be used to produce several manifestations
- The work starts as private data, and may be distributed for business



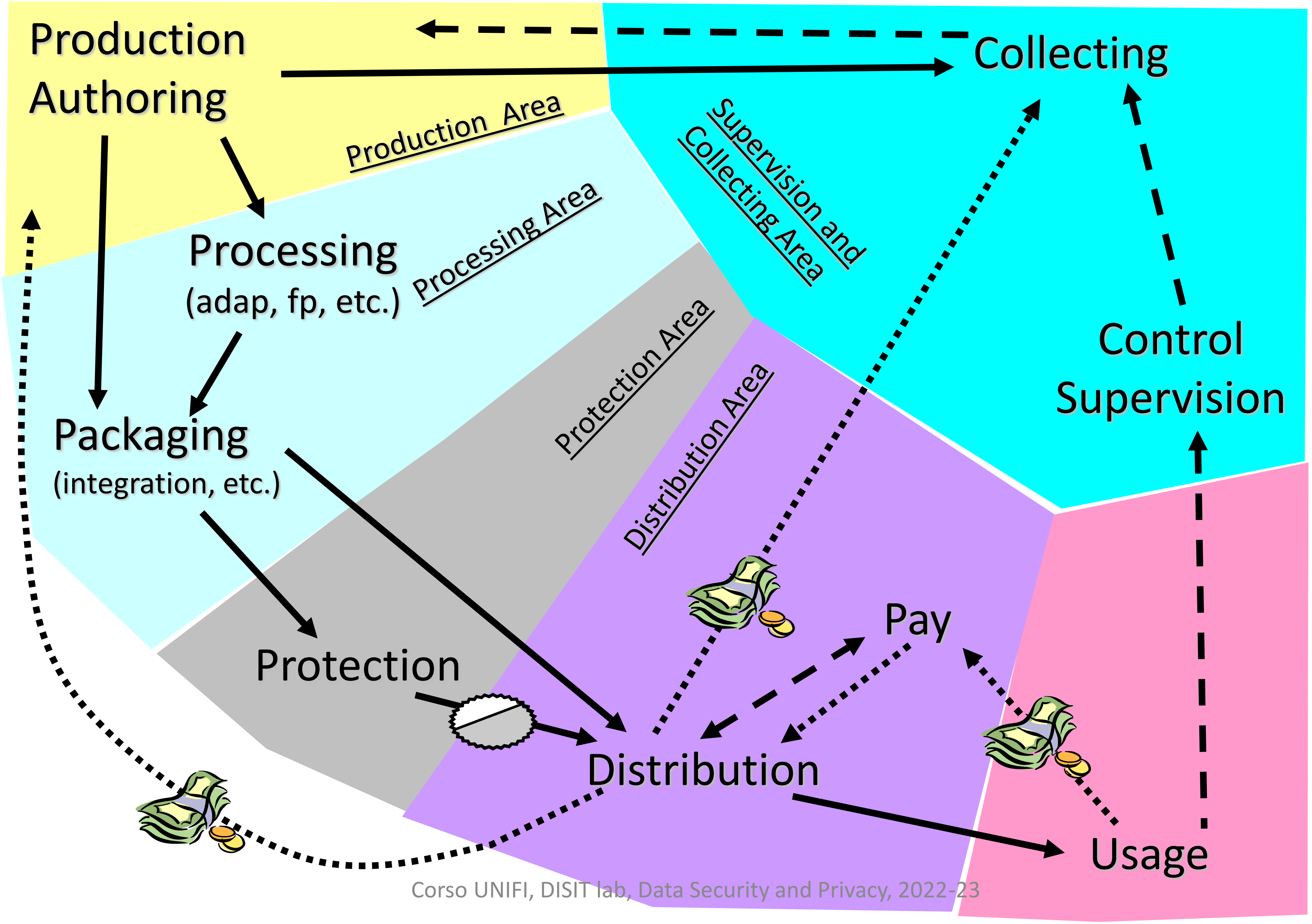
Some Actors of the value chain, “definitions”

- **Right/Content Owners**, artists, normal users, etc.
  - who has the rights on the initial work, non digital
- **Content Producers**, Publishers, also social network are producer/distributors
  - Who is producing the manifestations of the work, define its rights, may produce the digital resources or not, etc.
- **Content Integrators**, aggregators
  - Who is Integration/aggregation: resources + metadata ++ , added value, etc., may be add other rights, etc.
- **Content Distributors**,
  - Who is distributing digital content
- **Final Users**,
  - Who is using (or should use) the digital content on behalf of the rights obtained
- **Users**, in general
  - All the above actors that use in some way content on the basis of the rights obtained

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Simplified Traditional value chain

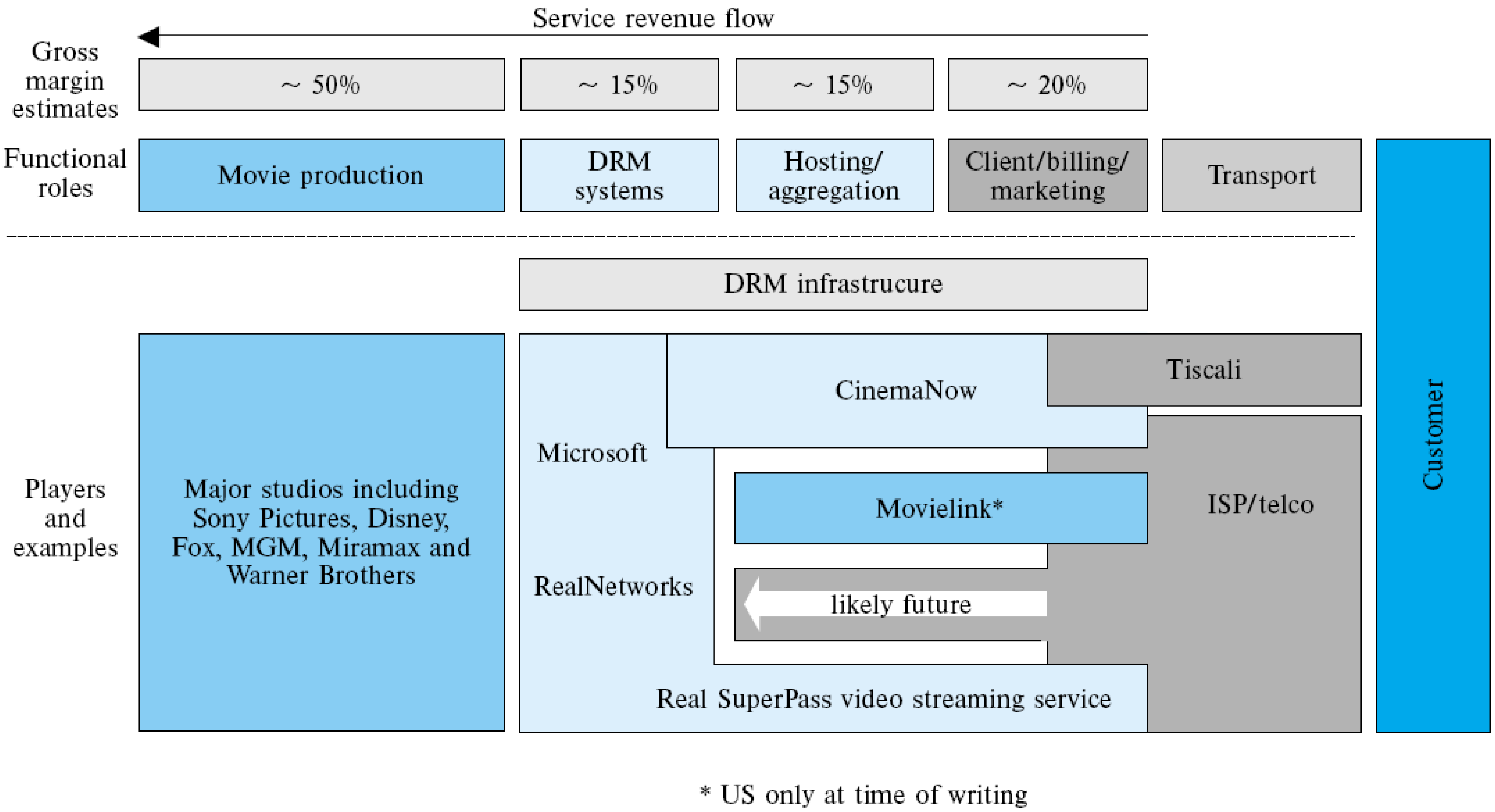


Classification of Transaction Models

- **B2B:** Business to Business
  - Among digital good: producer, publishers, integrator, resellers, distributors, etc.
  - Each of them add a value and thus charge to final prince of the digital good, …
- **B2C:** Business to Consumer
  - From distributors to consumers
  - The final part of the value chain
- **C2C:** Consumer to Consumer
  - File and good sharing
  - UGC (User Generated Content) sharing
  - Recently IPR management

- **B2B2C**
  - Integrated B2B to B2C

Ex: Broadband VOD value chain


Service revenue flow

Gross margin estimates

~ 50%

~ 15%

~ 15%

~ 20%

Functional roles

Movie production

DRM systems

Hosting/ aggregation

Client/billing/ marketing

Transport

Customer

DRM infrastrucure

Players and examples

Major studios including Sony Pictures, Disney, Fox, MGM, Miramax and Warner Brothers

Microsoft

RealNetworks

CinemaNow

Tiscali

Movielink*

ISP/telco

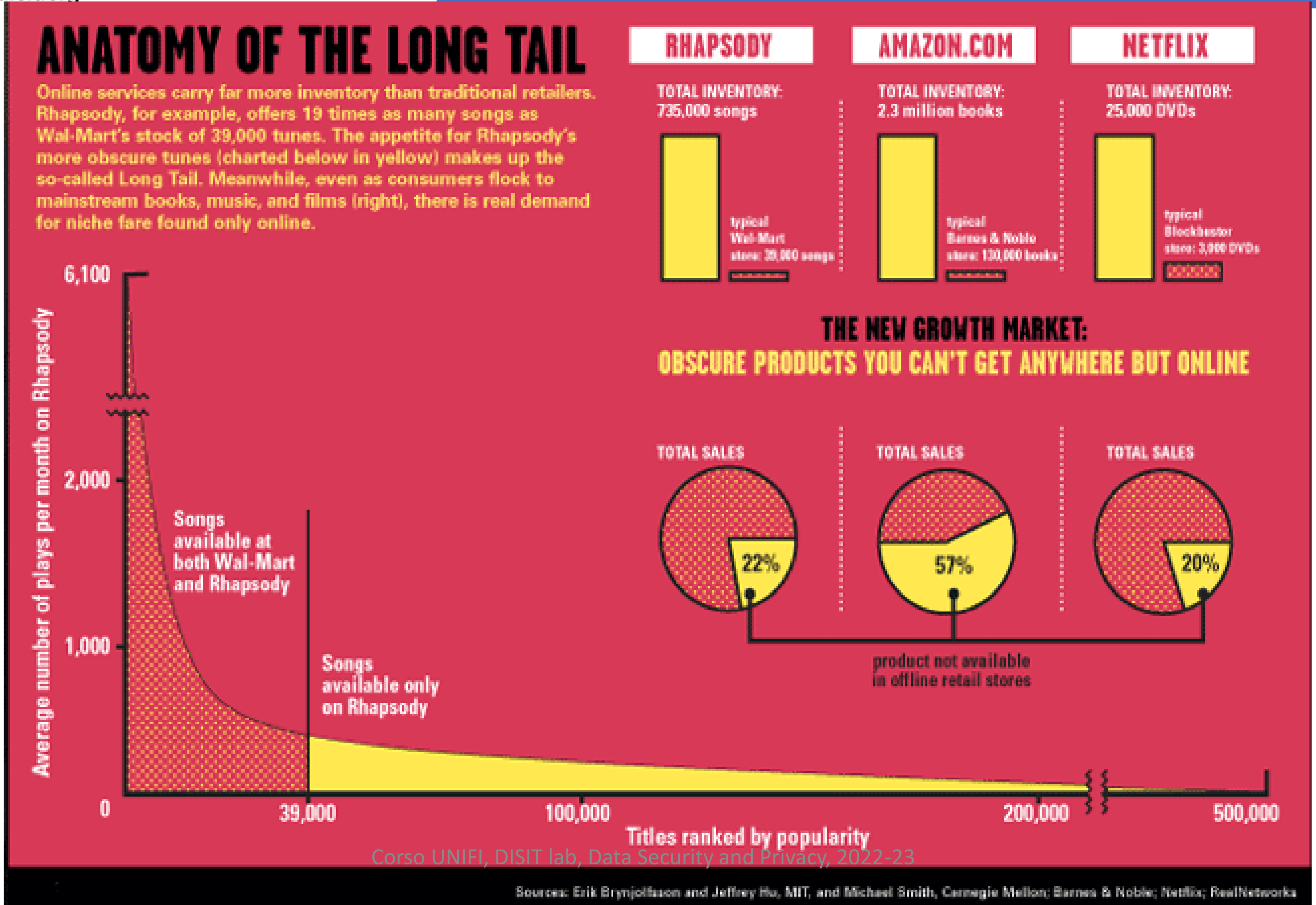
likely future

Real SuperPass video streaming service

* US only at time of writing

Source EITO2005

The Long Tail, paradigm



ANATOMY OF THE LONG TAIL

Online services carry far more inventory than traditional retailers. Rhapsody, for example, offers 19 times as many songs as Wal-Mart's stock of 39,000 tunes. The appetite for Rhapsody's more obscure tunes (charted below in yellow) makes up the so-called Long Tail. Meanwhile, even as consumers flock to mainstream books, music, and films (right), there is real demand for niche fare found only online.

6,100
2,000
1,000
0
Average number of plays per month on Rhapsody
Songs available at both Wal-Mart and Rhapsody
Songs available only on Rhapsody
39,000
100,000
200,000
500,000
Titles ranked by popularity
RHAPSODY
TOTAL INVENTORY: 735,000 songs
typical Wal-Mart store: 39,000 songs
AMAZON.COM
TOTAL INVENTORY: 2.3 million books
typical Barnes & Noble store: 130,000 books
NETFLIX
TOTAL INVENTORY: 25,000 DVDs
typical Blockbuster store: 3,000 DVDs
THE NEW GROWTH MARKET:
OBSCURE PRODUCTS YOU CAN'T GET ANYWHERE BUT ONLINE
TOTAL SALES
22%
TOTAL SALES
57%
TOTAL SALES
20%
product not available in offline retail stores

Sources: Erik Brynjolfsson and Jeffrey Hu, MIT, and Michael Smith, Carnegie Mellon; Barnes & Noble; Netflix; RealNetworks

Long tail paradigm

- **Initial hypothesis**
  - 80% of transactions are developed with the 20% of products
  - 20% of transactions are developed with the rest, 80%
- **The 80/20 ratio** depends on:
  - Content marketing model
  - Content nature and topic
  - Stimulus and recommendations provided to the users
  - User skill and evolution/renovation
  - Etc.

- Due to these facts, in most cases, the ration 80/20 is not anymore true, its trend in many case is towards the 60/40

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Copy Protection solution

- **Digital items can be freely copied**
  - The copy is a feature of the operating system, file system
  - The operating system cannot be typically controlled
  - *Technology Providers are trying to enforce more control on the Operating System → STB*

- **CP (copy protection) solutions**: prevents the Copy of digital content
  - Old Technologies:
    - Programs + hardware key
    - Holes in Floppy Disk
    - Special formatting in CDs/DVDs
    - Etc.

Analog Hole

- **Comunque uno protegga** un certo contenuto audio video quando questo viene riprodotto nel ***dominio analogico dei sensi***:
  - la riproduzione finisce per produrre effetti nel mondo analogico:
    - Il suono percepito dal sistema uditivo umano
    - Le immagini percepite dalla vista
- **Questo implica** che:
  - tramite sistemi di registrazioni del: Suono o delle immagini come registratori si puo' sempre effettuare una copia privata di tale materiale ***registrando nel dominio analogico***
  - la copia da analogico puo' avere una qualita' inferiore dell'orginale dipendentemente dall'originale stesso
- **Dal punto di vista legale**:
  - Puo' essere una violazione dipendentemente da chi fa questa operazione, se non ha il diritto di Copy etc.
  - Chi ha comprato un certo materiale ha il diritto di copia privata

Utilizzo della crittografia

- Encryption è il processo che codifica un messaggio in modo da nasconderne il contenuto
- Si basa sull'uso di parametri segreti: *chiavi*
- Si dividono in due classi fondamentali
  - Chiavi segrete condivise *(secret-key)*
  - Coppie di chiavi pubblica/privata *(public-key)*
- Applicazioni
  - Autenticazione
  - Firma digitale

Algortimi di crittografia

- Un messaggio si dice criptato quando il mittente applica alcune regole per trasformare il testo originale (*plaintext*) in un altro testo (*ciphertext*)

$$E(K_1, M) = \{M\}_K$$

- Il ricevente deve conoscere la trasformazione inversa per ritrasformare il *ciphertext* nel messaggio originale

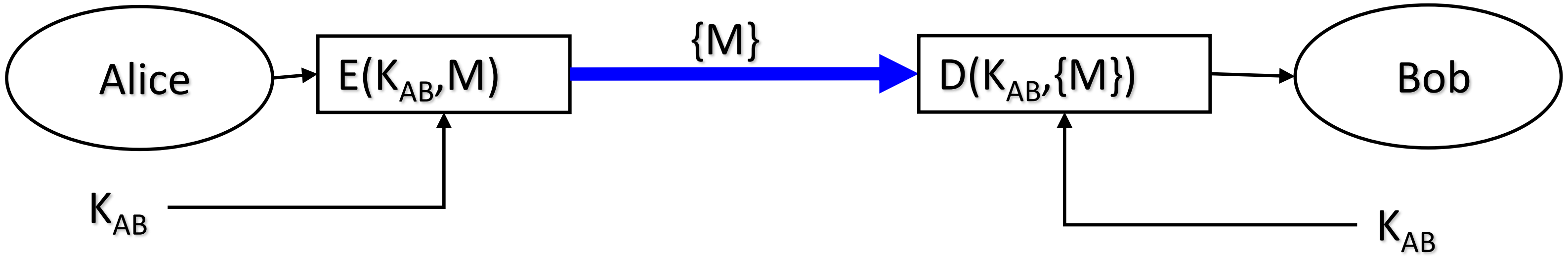
$$D(K_2, \{M\}_K) = M$$

$K_1 = K_2$ **simmetrico**

$K_1 \ != K_2$ **asimmetrico**

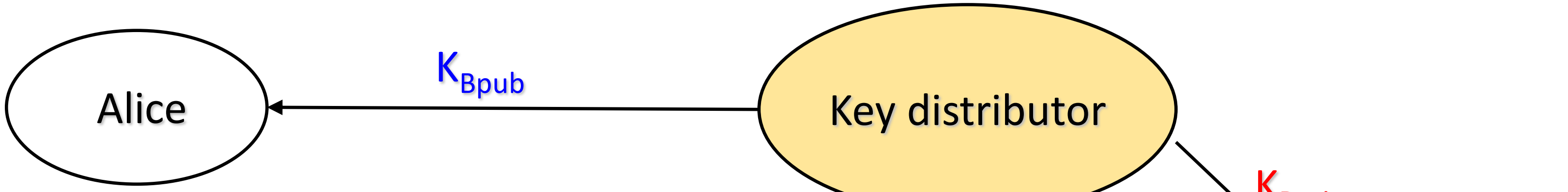
Scenario 1: secret communication

- Alice vuole inviare alcune informazioni segretamente a Bob
  - $\{M\}=E(K_{AB},M)$
- Alice e Bob conoscono entrambi la chiave segreta K_{AB}
- La comunicazione è segreta finchè K_{AB} non è compromessa

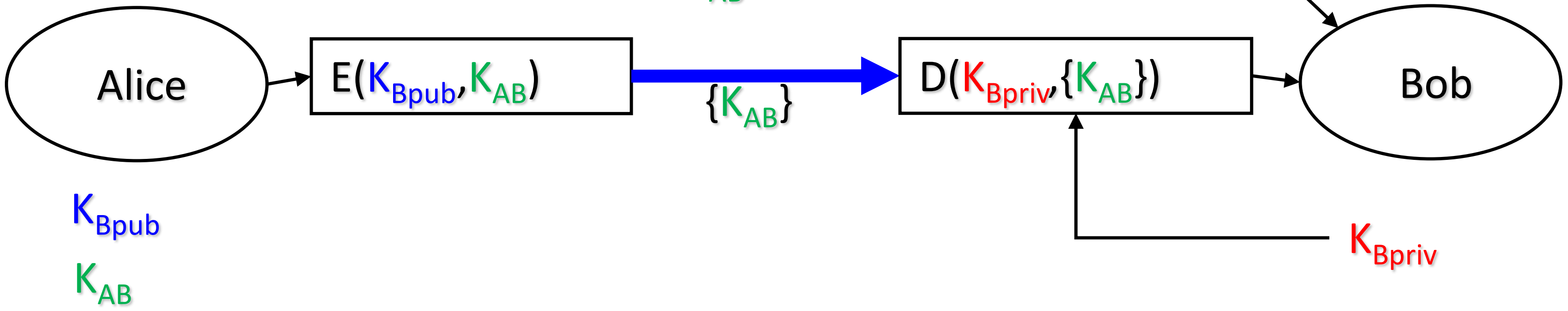


Scenario 3: authenticated with public-key

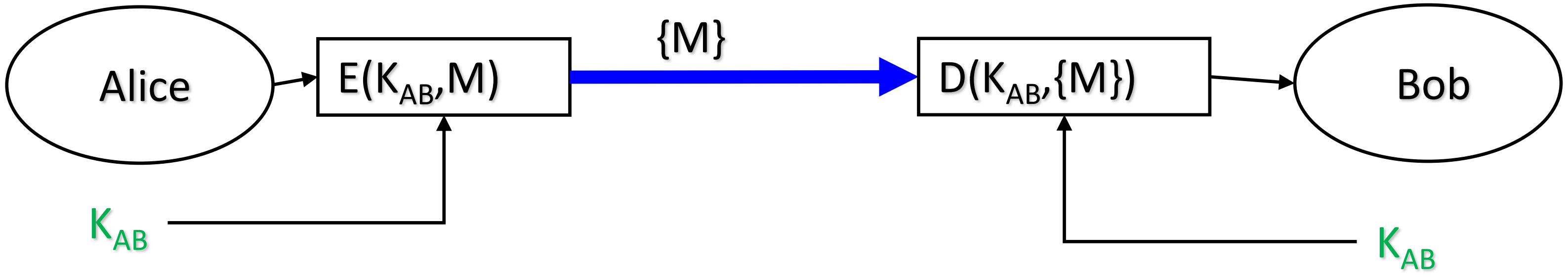
- Richiesta chiave pubblica



- Determinazione chiave di sessione K_{AB}



- Cumunicazione sicura



Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

CAS: Conditional Access Systems

- **Systems that controls the access to the content**
  - Typically used on streaming towards STB/Decoders
  - Copy is assumed not possible since the content is not stored locally and neither accessible to the final user.

- **For PC:**
  - Partially suitable for open platforms such as PC
    - On PC: SSL, HTTPS, etc.
  - Temporary storage of smaller content on the disk, may be encrypted
- **For STB, Set Top Box (commonly named as decoder):**
  - The most interesting and diffuse solution

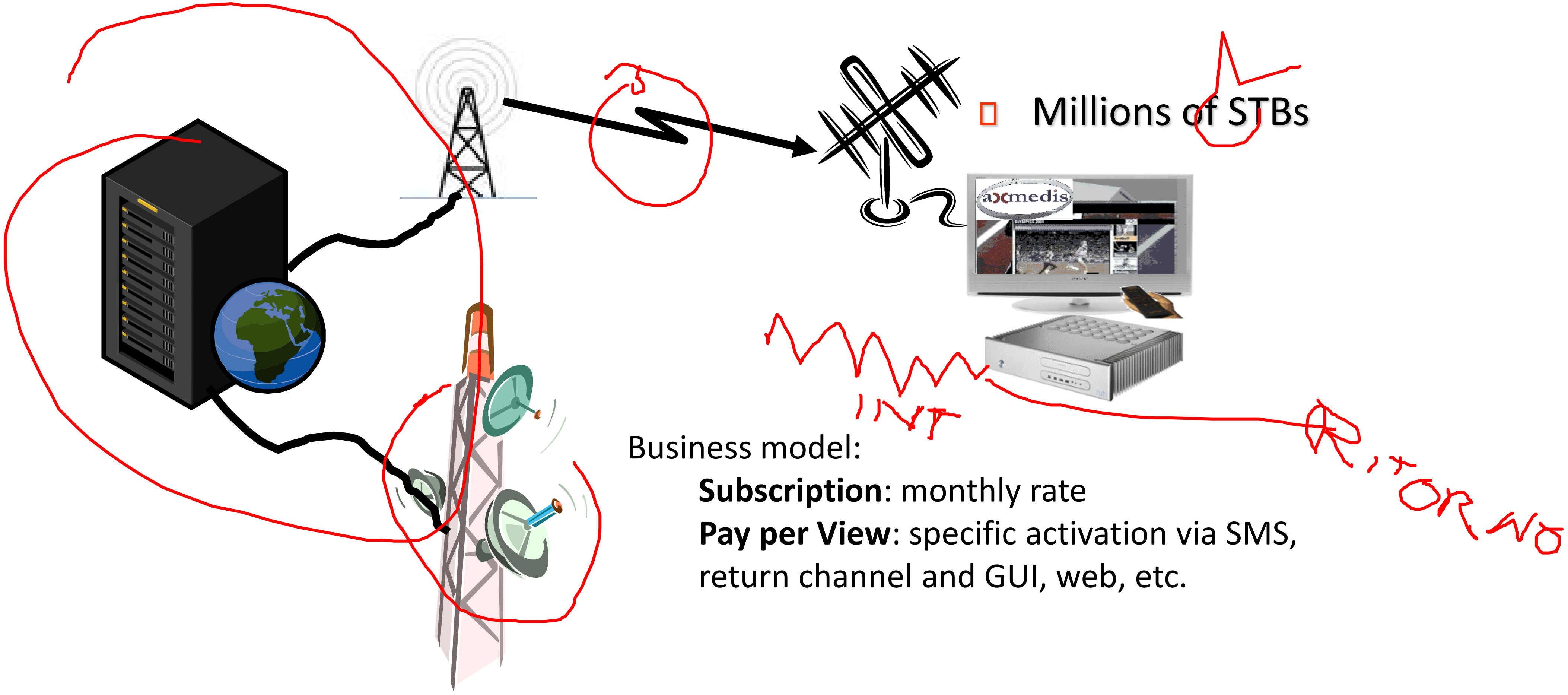
CAS: Conditional Access Systems

- **Systems that controls the access to the content for STB**
  - Streaming towards STB/Decoders
    - DVB-T, DVB-S, DVB standards for CAS
  - Copy is assumed not possible since the content is not locally stored and accessible to the final user. Recently can be temporary stored, see MySky.

- **Protection and solution**
  - Streaming in broadcast
  - Adoption of MPEG-2 TS (other models such as RTSP)
  - *For example*: Irdeto, Nagravision, NDS
  - Key distributed into the stream, accessible with another key
  - Adoption of SmartCard for some business models
  - Adoption of the Return Channel for some business models

DVB-T/DVB-S

- DVB Server



□ Millions of STBs

Business model:

Subscription: monthly rate
Pay per View: specific activation via SMS, return channel and GUI, web, etc.

CAS protezione

- Cifrare il TS da lato Server per poi abilitare lato client solo quelli che stipulano un contratto,
  - E pertanto solo questi ottengono una licenza
- La cifratura avviene tipicamente con algoritmi standard (scrambling) e vengono cambiate le chiavi molto spesso.
- Oltre a questo, nel TS vengono anche inviate alcune info che possono essere usate per recuperare la chiave di decifratura.
- La chiave non viene inviata in chiaro per ovvi motivi.

Sistema di Chiavi

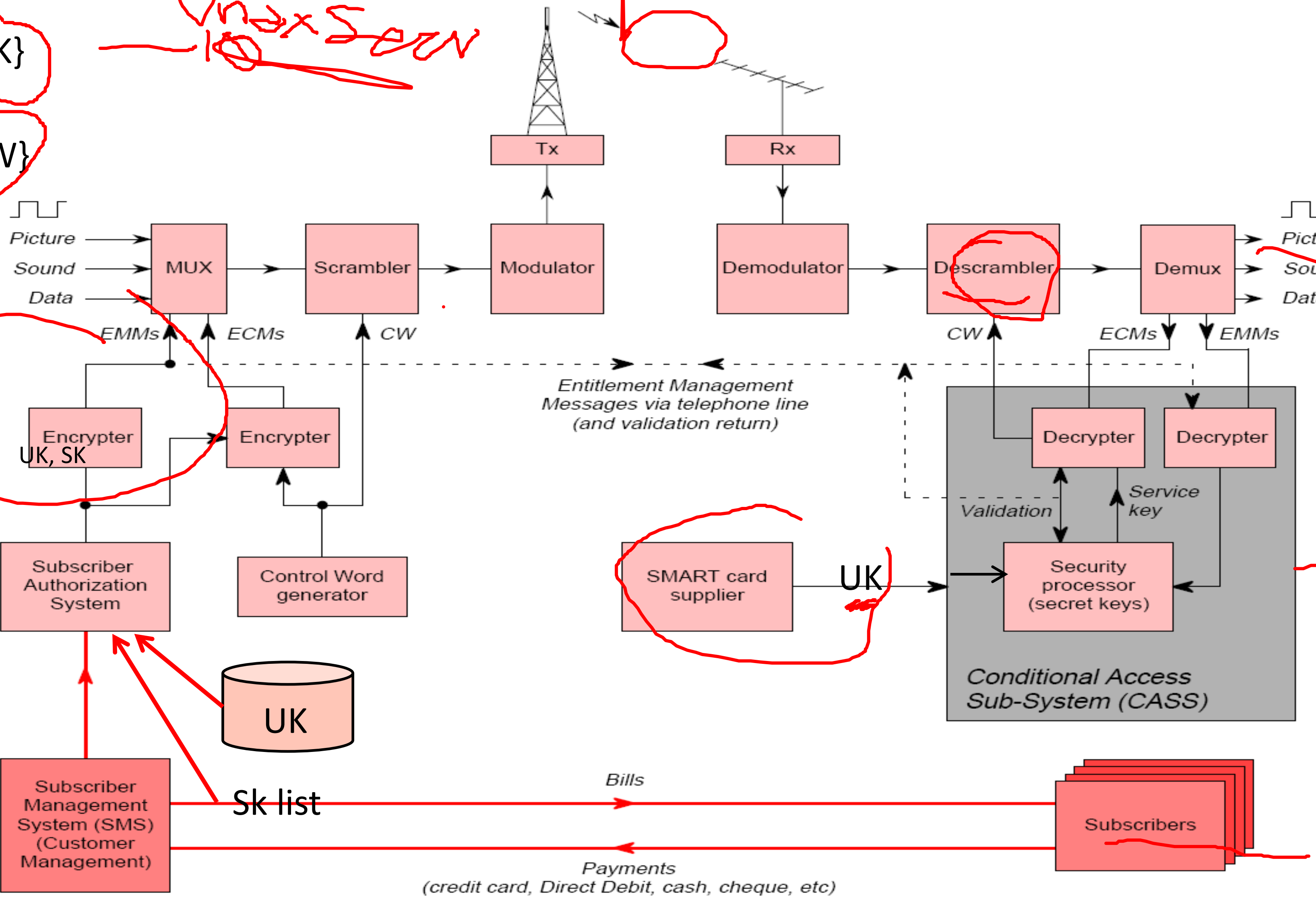
- **CW: Control word**, chiave utilizzata per cifrare il flusso digitale
- **SK: Service Key**, serie di chiavi,
  - una per ogni servizio/canale contenuto nello stream,
  - Per ogni SK viene creato un oggetto cifrato **chiamanto ECM**
- **UK, User key**, permette all'utente di ottenere la SK, decrypt.
  - Ogni utente ha un UK diversa
  - Per esempio nascosta in una SMARTCARD
- **ECM: Entitlement Control Message**, ECM(SK,CW)={CW}
  - viene inviata in broadcast
  - contiene la CW cryptata tramite la SK
- **EMM, Entitled Management Message**, EMM(UK, SK)={SK}
  - viene inviato in broadcast
  - contiene una SK encrypted che puo' essere decifrata solo con una UK (come quella usata per encription)

EMM(UK, SK)={SK}

ECM(SK,CW)={CW}

EMM*(UK, {SK})=SK

ECM*(SK,{CW})=CW


Tx
Rx
Picture
Sound
Data
MUX
Scrambler
Modulator
Demodulator
Descrambler
Demux
Picture
Sound
Data
EMMs
ECMs
CW
CW
ECMs
EMMs
Entitlement Management Messages via telephone line (and validation return)
Encrypter
UK, SK
Encrypter
Decrypter
Decrypter
Validation
Service key
Subscriber Authorization System
Control Word generator
SMART card supplier
UK
Security processor (secret keys)
Conditional Access Sub-System (CASS)
UK
Sk list
Subscriber Management System (SMS) (Customer Management)
Bills
Payments (credit card, Direct Debit, cash, cheque, etc)
Subscribers

- **Client side:**
  1. arriva un EMM per un certo servizio i, dallo stream che viene passato al SecProcessor che ha la UK (user key)
  2. Il SecProcessor produce la SK(i) (service key) usando la sua UK se possibile, cioe' se abbonato al servizio
  3. Questa SK(i) (ve ne sono n, una per ogni servizio/canale) viene usata per estrarre la CW (i) da ECM (i)
  4. CW(i) viene usato per decriptare il ProgStream/servizio (i)
- **Server side**:
  1. Le CW per ogni servizio i sono generate in modo periodico
  2. SK(i) (n elementi) sono generate per ogni servizio i degli n
  3. SK(i) viene usata per codificare CW(i) into ECM(i) del servizio i
  4. La User List viene usata per codificare le n SK(i) into m EMM (I,u), un EMM per ogni servizio e per ogni utente, u.

- **ECMn** = { per ogni servizio i si ha SKi, ECM i = Encrip (CWt, SKi) }
    - Con: i di *n; d*ove: *n* e' il numero di oggetti/servizi
    - CW t cambia nel tempo
  - n ECM, uno per ogni SK
  - complessita' O(n)
  - Invio ogni 2 secondi, in anticipo
  - I servizi possono essere canali diversi, PS diversi

- **EMMm** = { per ogni utente j di m: EMM j,i = Encrip (SKi, UKj) }
    - Con: j di m; dove: m e' il numero di utenti
    - Con: i di n; dove: *n* e' il numero di oggetti/servizi
  - m EMM, uno per ogni servizio i-esimo SK (Service Key si trova dentro la EMM e viene decripted tramite la UK)
  - complessita' O(mn)
  - Invio ogni 10 secondi, in anticipo

References

- http://www.dvb.org
- http://www.mhp.org
- http://www.interactivetvweb.org/
- http://www.etsi.org
- http://erg.abdn.ac.uk/research/future-net/digitalvideo/
- http://www.dgtvi.it
- Memorandum of Understanding http://www.dvb.org/documents/mou2001.pdf
- List of DVB Members, http://www.dvb.org/index.php?id=27
- DVB Worldwide http://www.dvb.org/index.php?id=228

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Rights Management

- **DRM**: Digital Rights Management
  - general term many times abused, confused, ...

- Management of Digital Rights
  - Limited to the management of rights of digital content ? → NO!!!
- **Digital Management of Rights → YES!!!**
  - More correct and reasonable
  - Management of both rights for original *works* and related *manifestations*, digital *resources*, etc.
  - in many solutions DRM is not intended in this way

Digital Rights Management

- **DRM: Digital Rights Management**
  - A set of technologies and solution to cope with Digital Management of Rights

- 1st generation of DRM were covering:
  - security and encryption
  - prevent non authorized copying, i.e., CP solutions
- **2nd generation of DRM covers:**
  - Content: description, identification, trading, protection,
  - monitoring, and tracking of all forms of rights usages over contents, including management of rights holders relationships

Aim of …… Digital Rights Management

- To allow exploiting digital content functionalities (rights) in a controlled manner
  - To who has been **authenticated/certified**
  - To do what (are the rights) is defined in a formal **license**
  - **Verifying/Control/Supervise** if the above conditions and others are respected
  - By using technologies to **protect content** (e.g., encryption, fingerprint, watermark, etc.)

- Cons:
  - Registration of users (in some case can be relaxed)
  - Authentic. of users and/or tools/terminal/devices
  - Control of users
- *It has to be supported by a set of additional technical solutions*

Motivations for Digital Rights Management

- Prevent the rights exploitation to who has not acquired the rights
  - from some rights owner or authorized reseller
- Verifying/Control if the allowed rights are respected:
  - In the whole value chain or at least at the end users
- Support/adoption of protection solution to
  - Enforce the rights control on the players and tools by which the users are accessing to the content.

- **Recently**, strongly rejected by the final users since most the DRM solutions also enforce some limitations with respect to the TRU (traditional rights usages):
  - Cracking the DRM solutions
  - Redistributing the content violating the IPR via P2P, Social Network, direct contacts, etc.

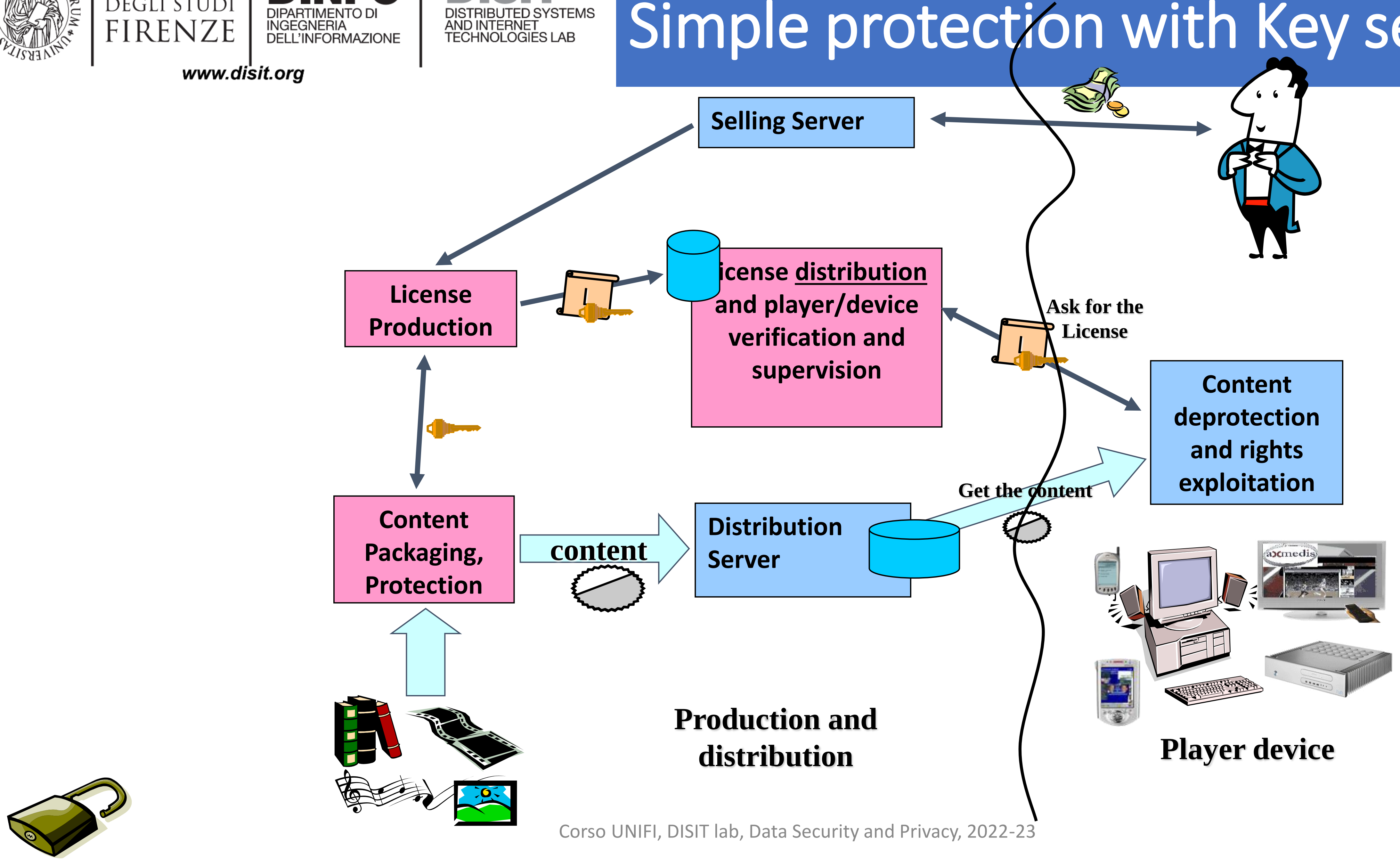
Motivations for Digital Rights Management

- The **collection of money/revenues (creation of revenue streams)** related to the exploitation of rights is traditionally/partially covered by Collecting Societies (clearing houses)

- **Collecting Societies**
  - Are Focussed on one or more rights types
    - thus, one or more for each Country/area
  - Guarantee/protect the interests of the content/rights owners
  - Are territorially distributed, while in Europe some liberalisation has been performed, permitting in some measure the competitions among different European CS

- They are some common agreement among the majors Collecting Societies in Europe: SIAE, SGAE, SAGEMA, etc.

Simple protection with Key sending


Selling Server
License Production
License distribution and player/device verification and supervision
Ask for the License
Content deprotection and rights exploitation
Content Packaging, Protection
content
Distribution Server
Get the content
Production and distribution
Player device

What Should be the DRM

- To allow exploiting the (digital) content functionalities (rights) in a controlled/supervised manner
  - To who has been **authenticated/certified**
  - To do what (are the rights) is defined in a formal **license**
  - By using technologies to **protect content** (e.g., encryption, fingerprint, watermark, etc.)
  - **Verifying/Control/Supervise** if the above conditions and other issues are respected,
    - including the *possibility of keep trace of the activity performed by the users and reporting/using them to the distributors* (this part is disputable since for the privacy)

Technical issues behind the DRM

- **Digital Encryption/decryption**
  - DRM may use strong encryption (# bits) never been cracked

- **Digital signatures**
  - content may be digitally signed to prevent tampering
  - license has to be digitally signed, etc.
  - event reporting has to be digitally signed, etc.

- **Unique identification of elements:**
  - Users, Content Objects, devices/players, ...
  - Distributors and rights, ...

- **Authentication and certification of users and devices**
  - To prevent compromised players or non trusting users to receive or distribute other content, ….
  - Black list of devices, licenses, users, etc.

Technical issues behind the DRM

- **Separation of licenses from content**
  - licenses should be kept separate from content
  - The license formalises what can be done by a given user on a given content
  - thus content can be protected once for all and widely distributed via any kind of channel including P2P
- **Revocation of User, User ID**
  - The user that has violated the solution is black listed, banned.
  - He cannot exploit any right on content !!, may be too strong..
- **Revocation of licenses, via License ID**
  - Revocation of rights authorization, for that content-right
  - various ways to prevent players from exploiting content
- **Revocation of Content, via Content ID**
  - Content with the listed IDs cannot be played on players.
- **Revocation of Player, Player ID**
  - Players with the listed IDs cannot be used to open protected content, lost of certification.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Content Elements

- **Content Packaging to contain the following information**
  - Metadata + semantic descriptors ………
  - Digital Resources: items, digital essences, ……
  - Protection Information: (how to prot/deprot the content)…..
  - License: ……..who can use, when, how, etc...

- **The Package should allow to be**
  - Protected
  - Streamed (so called real-time) and/or downloaded, ….
  - Shared on P2P, etc..
  - Ported on physical supports,
  - Adapted, etc..
  - Coded in binary and/or XML, etc.
  - etc.

Content Elements of the package

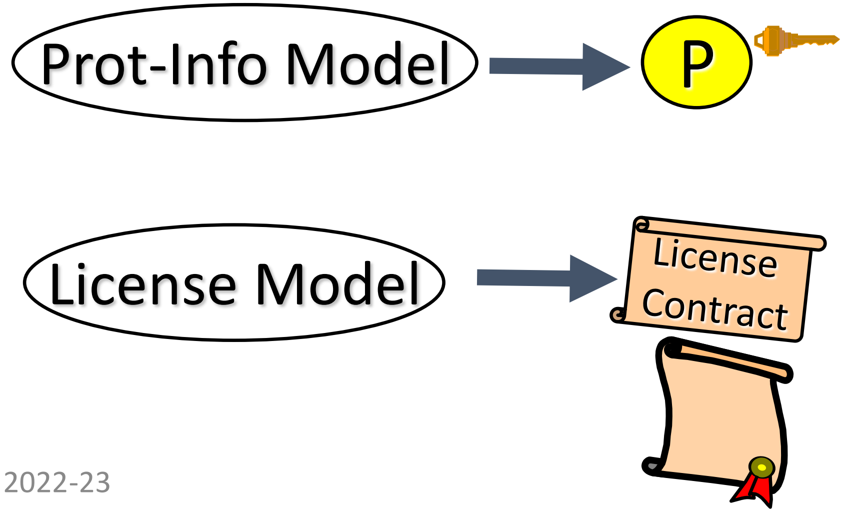
- **Metadata:**
  - Identification information, unique ID, distributor ID, etc.
  - Classification information also for indexing: Dublin core, etc.
  - Semantic Descriptors, MPEG-7, for indexing, etc.
  - References to Owner, to distributor, etc.
  - Etc.

Metadata

- **Digital Resources:**
  - Any digital information: images, doc, txt, video, game, application, file, audio, etc.
  - Hierarchy of digital resources

Resource

- **Protection Information:**
  - What has to be done to access at a given information/resource
  - Tools used, their parameters, etc.
- **License:**
  - Which rights are provided, who is the recipient, conditions, etc.



Packing Content vs other aspects

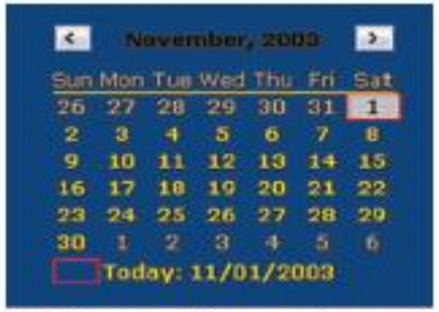
- The **package** may contain several information: metadata, info, several files, etc. →
  - Cross media content
  - hierarchical content and structure
- The **package** to be protected has to encoded in some file and format. For example, to be encrypted with some algorithm
  - Protection by ignorance (algorithm and key)
  - Protection by complexity
- The **key** has to reach the player only via specific protected channels
  - If the key is reached and the algorithm is known the protection is violated
- The **player** has to **enforce** the protection and has to provide a precise semantics for the rights
- The **license** is a description of the conditions under which the key can be taken, passed, used to/by the player

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution ←
- Creative Commons Licensing
- Composition of Licenses, data aggregation

License formal language

- **XrML 2.0:** eXtensible rights Markup Language
  - http://www.xrml.org/
  - General purpose
  - ContentGuard, Nov. 2001, Microsoft
  - Derived from DPRL
  - Usato come base per MPEG-21
- **Windows Media DRM**
  - Derived from XrML
- **MPEG-21:**
  - REL: Rights Expression Language
    - Derived from XrML
  - RDD: Rights Data Dictionary
- **OMA ODRL:** Open Digital Rights Management
  - Expression language for mobiles
  - In some way simpler than MPEG-21 REL
  - ..



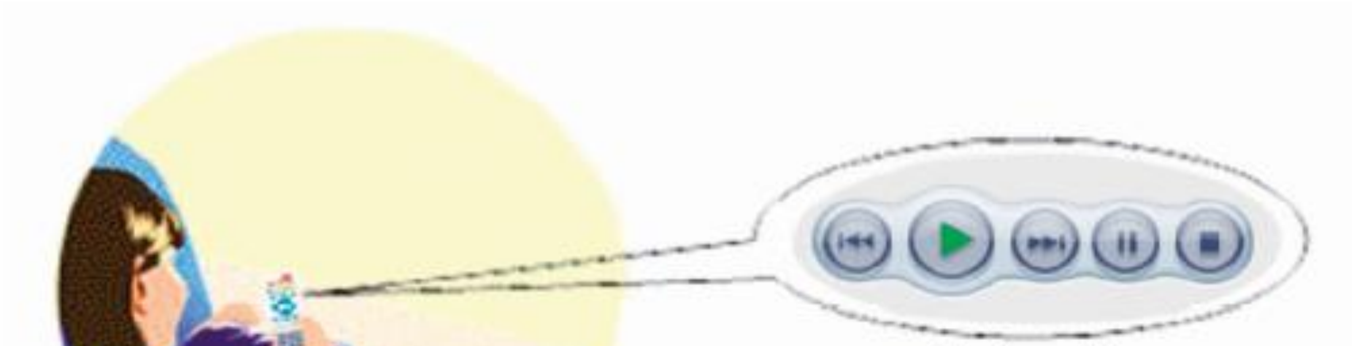
< November, 2003 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Today: 11/01/2003

Condition = November 2003

Resource = Ocean Wilds



Right = Play

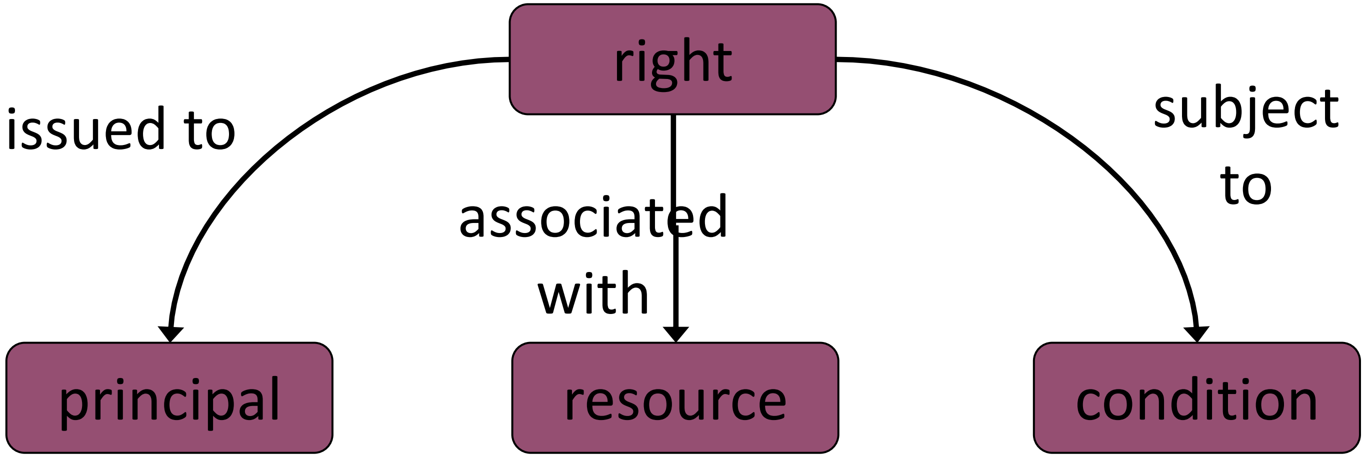
- Rosy can Play 3 times the Ocean Wilds in November 2003.

MPEG-21 — REL, Rights Expression Language

- **REL is** a machine-readable language, XML
  - to declare rights and permissions
  - uses terms defined in the Rights Data Dictionary, RDD
- **REL allows to define licenses** that give specific permissions to Users to perform certain actions on certain resources, given that certain conditions are met
  - Grants can also allow Users to delegate authority to others
- **Systems and device have to**
  - parse and validate the REL formalizations
  - check permissions before any further action is done
- **REL licenses** are wrapped into MPEG-21 Digital Items when the object is governed
- **MPEG-21 DID parser** is responsible for discovering and identifying where to gather licenses

REL data model

- REL grant formalization consists of
  - principal to whom grant is issued
  - rights the grant specifies
  - resource to which right in grant applies
  - condition to be met before grant can be exercised



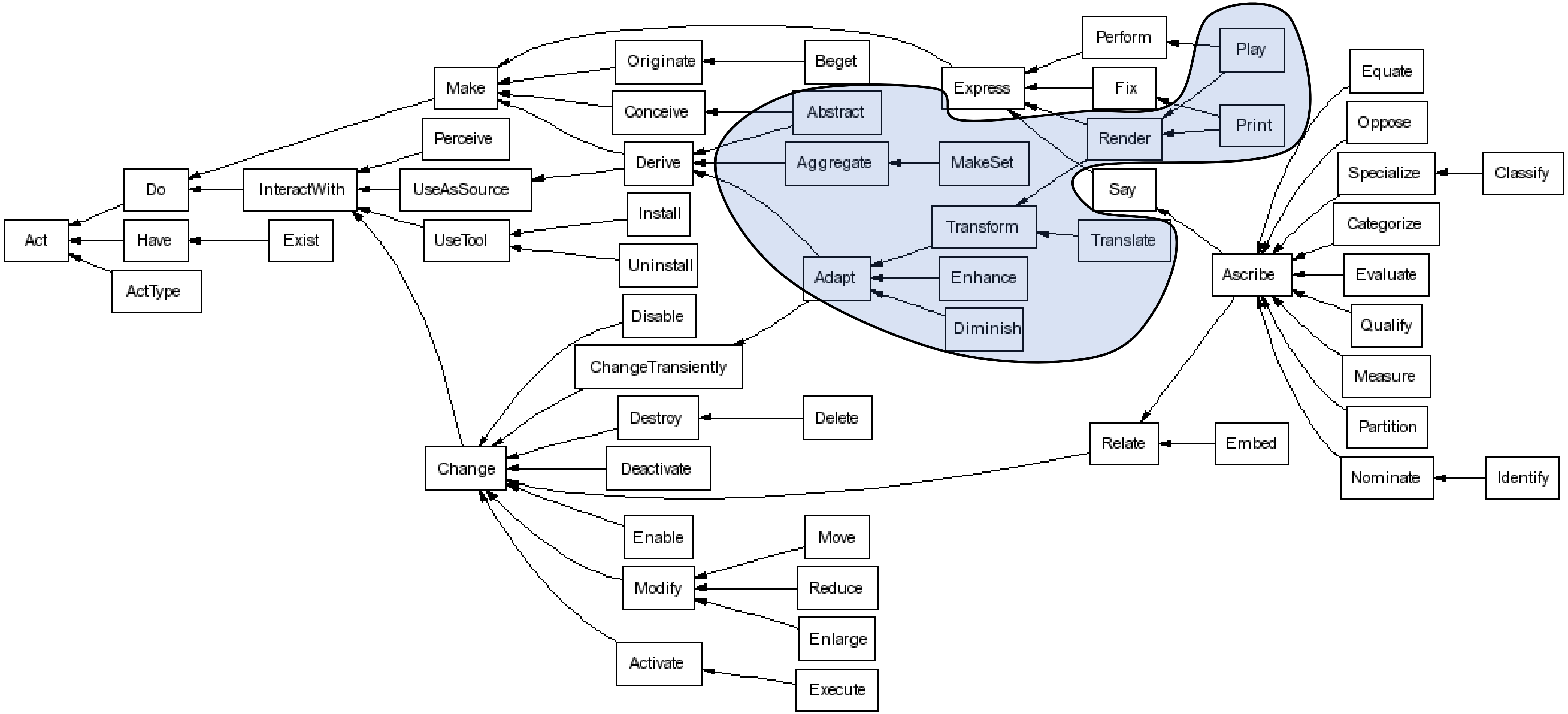
REL – Principal and Rights

- **Principal**: Party to whom a grant conveys usage rights.
  - authentication mechanism by which the principal can prove its identity.
  - a principal that must present multiple credentials, all of them must be simultaneously valid, to be authenticated.
- **Right**:
  - Action or activity that a principal may perform using a resource under some condition.
- **Resource**:
  - Object/content to which the principal can be granted a right.
- **Condition**:
  - Terms under which rights can be exercised.

- **MPEG REL provides** a right element to encapsulate information about rights and provides a set of commonly used, specific rights, notably rights relating to other rights, such as issue, revoke and obtain.
  - Extensions to MPEG REL could define rights appropriate to using specific types of resource.
  - For instance, the MPEG REL content extension defines rights appropriate to using digital works (e.g., play and print)

RDDOnto (Garcia, Delgado, 2007)

- Example: *Act* hierarchy.



Possible values for term

- **Principal**
  - AllPrincipals and KeyHolder
- **Rights**
  - Issue, Obtain, PossesProperty and Revoke
- **Resources**
  - DigitalResource, Revocable and ServiceReference
- **Conditions**
  - AllConditions, ExerciseMechanism, ExistsRight, Fullfiler, PrerequisiteRight, RevocationFreshness, ValidityInterval

- CallForCondition
- ExerciseLimit
- FeeFlat
- FeeMetered
- FeePerInterval
- FeePerUse
- FeePerUsePrePay
- SeekAproval
- Territory
- TrackQuery
- TrackReport
- TransferControl
- ValidityIntervalFloating
- ValidityIntervalStartsNow
- ValidityTimeMetered
- ValidityTimePeriodic

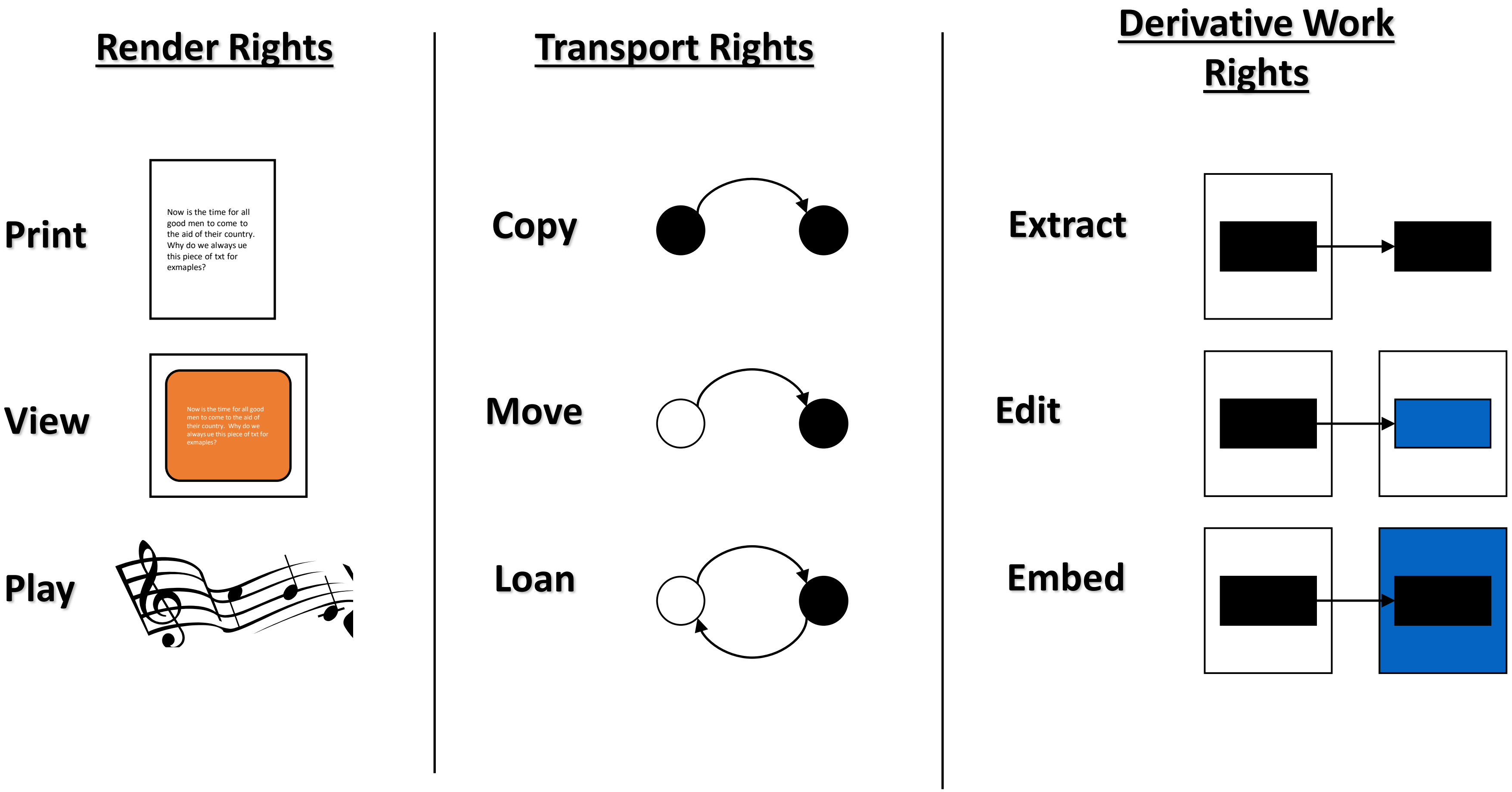
- Examples of Rights
  - Adapt
  - Delete
  - Diminish
  - Embed
  - Enhance
  - Enlarge
  - Execute
  - Install
  - Modify
  - Move
  - Play
  - Print
  - Reduce
  - Uninstall

Esempi di Licenze: creator to distrib

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
 <!-- License model for giving right adapt to the distributor -->
 <r:license xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS" xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS"
    xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-REL-R-
    NS ../schemas/rel-r.xsd  urn:mpeg:mpeg21:2003:01-REL-SX-NS ../schemas/rel-sx.xsd urn:mpeg:mpeg21:2003:01-REL-MX-NS ../schemas/rel-mx.xsd">
    <r:grantGroup>
     <r:grant>  <r:keyHolder>  <r:info><dsig:KeyName>AXDID:Distributor</dsig:KeyName> </r:info>
                 </r:keyHolder>
                 <mx:adapt/>
                  <mx:diReference><mx:identifier>AXOID:Identifier</mx:identifier> </mx:diReference>
             </r:grant>
    </r:grantGroup>
    <!--The license is issued by the creator.-->
    <r:issuer> <r:keyHolder> <r:info> <dsig:KeyName>AXCID:Creator</dsig:KeyName></r:info>
             </r:keyHolder>
    </r:issuer>
</r:license>
```

Riferimenti

- **CAS**
  - Irdeto: http://www.irdeto.com/
  - Nagravision: http://www.nagravision.com/
  - NDS: http://www.nds.com/
- **DRM**
  - MPEG-21: http://www.dsi.unifi.it/~nesi/DISIT-Introduction-to-MPEG-21-v1-0.pdf
  - AXMEDIS DRM for dummies: a full round into the content protection, production of licenses, etc.
  - http://www.axmedis.org
  - http://www.axmedis.org/documenti/view_documenti.php?doc_id=3964



Render Rights

Print

View

Play

Transport Rights

Copy

Move

Loan

Derivative Work Rights

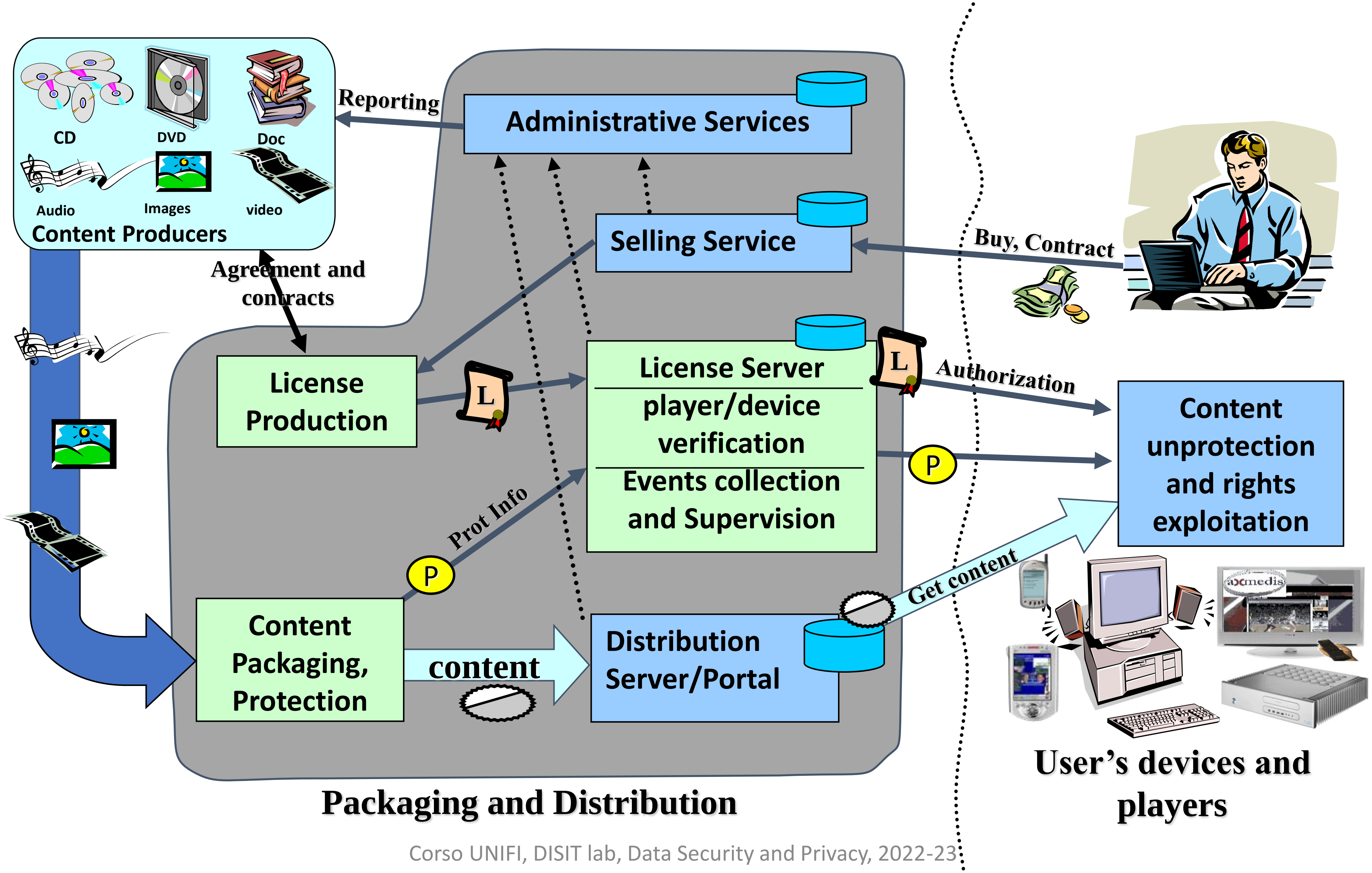
Extract

Edit

Embed

Now is the time for all good men to come to the aid of their country. Why do we always ue this piece of txt for exmaples?
Now is the time for all good men to come to the aid of their country. Why do we always ue this piece of txt for exmaples?

Based model for DRM


CD
DVD
Doc
Audio
Images
video
Content Producers
Reporting
Administrative Services
Selling Service
Buy, Contract
Agreement and contracts
License Production
License Server
player/device verification
Events collection and Supervision
L
Authorization
P
Content unprotection and rights exploitation
Prot Info
Content Packaging, Protection
content
Distribution Server/Portal
Get content
axmedis
User's devices and players
Packaging and Distribution

Different kinds of Packages

	Package	Protection	Which Files	Distribution models	Annotations	Metadata custom + descriptors
MPEG-21	Xml	Yes/DRM	any	Yes/DIS	(Yes)	Yes
MPEG-4	Yes (xml/bin)	Yes/CAS	Audio video	Yes/Stream	No	No
MXF	Yes (xml/bin)	No	Audio video	Download	No	Yes/No
SCORM/IMS	Yes (xml/bin)	Yes /CAS	any	Download	No	Yes
AXMEDIS	Yes (xml/bin)	Yes /DRM	any	Yes all	(Yes)	Yes
ZIP	Bin	Yes (pwd, CAS)	any	Download	No	No
NewsML	Yes (xml/bin)	Yes (Zip, Pwd, cas)	any	Download	No	Yes

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Creative Commons, CC

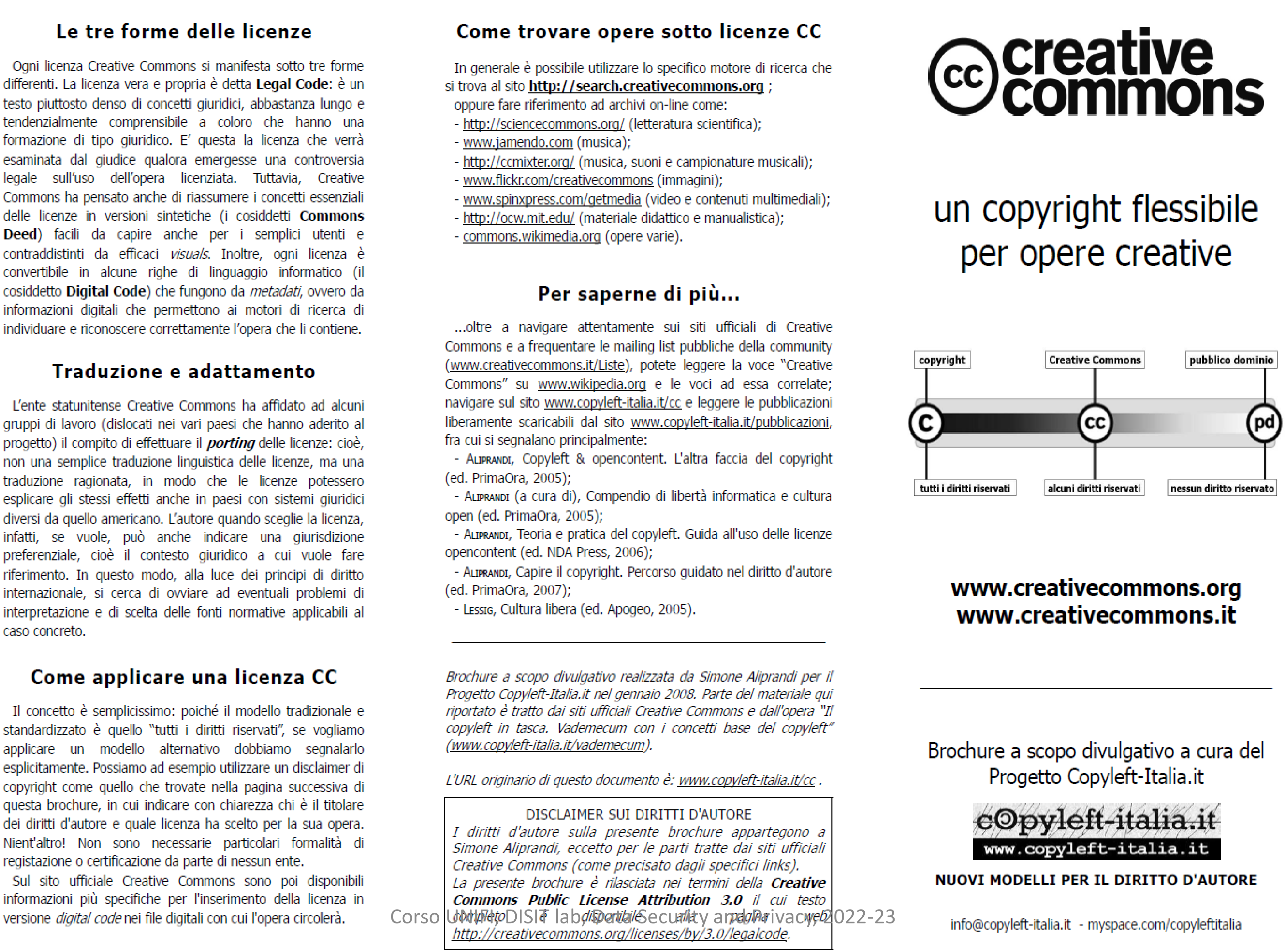
- e’ necessario includere anche alcune slide relative alle licenze CC.
- Fino ad ora abbiamo visto tecnologia al servizio della protezione dei dati e della proprieta’ intellettuale
- CC mette a disposizione degli strumenti, dei formalismi legali che possono essere o meno adottati da chi pubblica i propri contenuti
- Questi sono license formalizzate:
  - **Struttura della Licenza CC:**
    - Legal Code: testo legale che la descrive
    - Commons Deed: short description della licenza
    - Digital Code: metadati da associare

    (see S. Aliprandi, 2005, 2006…)

http://www.copyleft-italia.it/cc/brochureCCv2.pdf

Creative Commons, CC

- ***Le licenze CC***
  - Nate in USA
  - Sono state adattate alla legislazione nazionale di diversi stati e anche a livello europeo
    - specialmente per contenuti generati dagli utenti e in ambito culturale
    - Questo permette in un certo qual modo di avere una trascodifica fra le questioni legali nazionali e quelle di altre nazioni, ma solo per certe questioni.
  - Licenze CC ipotizzano uno share, copyleft
- E' stato fatta una codifica delle licenze CC in MPEG-21 REL
  - Non e' vero l'opposto, tutte le licenze che si possono formalizzare in MPEG-21 non hanno una controparte in CC



Le tre forme delle licenze

Ogni licenza Creative Commons si manifesta sotto tre forme differenti. La licenza vera e propria è detta **Legal Code**: è un testo piuttosto denso di concetti giuridici, abbastanza lungo e tendenzialmente comprensibile a coloro che hanno una formazione di tipo giuridico. E' questa la licenza che verrà esaminata dal giudice qualora emergesse una controversia legale sull'uso dell'opera licenziata. Tuttavia, Creative Commons ha pensato anche di riassumere i concetti essenziali delle licenze in versioni sintetiche (i cosiddetti **Commons Deed**) facili da capire anche per i semplici utenti e contraddistinti da efficaci *visuals*. Inoltre, ogni licenza è convertibile in alcune righe di linguaggio informatico (il cosiddetto **Digital Code**) che fungono da *metadati*, ovvero da informazioni digitali che permettono ai motori di ricerca di individuare e riconoscere correttamente l'opera che li contiene.

Traduzione e adattamento

L'ente statunitense Creative Commons ha affidato ad alcuni gruppi di lavoro (dislocati nei vari paesi che hanno aderito al progetto) il compito di effettuare il ***porting*** delle licenze: cioè, non una semplice traduzione linguistica delle licenze, ma una traduzione ragionata, in modo che le licenze potessero esplicare gli stessi effetti anche in paesi con sistemi giuridici diversi da quello americano. L'autore quando sceglie la licenza, infatti, se vuole, può anche indicare una giurisdizione preferenziale, cioè il contesto giuridico a cui vuole fare riferimento. In questo modo, alla luce dei principi di diritto internazionale, si cerca di ovviare ad eventuali problemi di interpretazione e di scelta delle fonti normative applicabili al caso concreto.

Come applicare una licenza CC

Il concetto è semplicissimo: poiché il modello tradizionale e standardizzato è quello "tutti i diritti riservati", se vogliamo applicare un modello alternativo dobbiamo segnalarlo esplicitamente. Possiamo ad esempio utilizzare un disclaimer di copyright come quello che trovate nella pagina successiva di questa brochure, in cui indicare con chiarezza chi è il titolare dei diritti d'autore e quale licenza ha scelto per la sua opera. Nient'altro! Non sono necessarie particolari formalità di registazione o certificazione da parte di nessun ente.

Sul sito ufficiale Creative Commons sono poi disponibili informazioni più specifiche per l'inserimento della licenza in versione *digital code* nei file digitali con cui l'opera circolerà.

Come trovare opere sotto licenze CC

In generale è possibile utilizzare lo specifico motore di ricerca che si trova al sito **http://search.creativecommons.org** ;
oppure fare riferimento ad archivi on-line come:
- http://sciencecommons.org/ (letteratura scientifica);
- www.jamendo.com (musica);
- http://ccmixter.org/ (musica, suoni e campionature musicali);
- www.flickr.com/creativecommons (immagini);
- www.spinxpress.com/getmedia (video e contenuti multimediali);
- http://ocw.mit.edu/ (materiale didattico e manualistica);
- commons.wikimedia.org (opere varie).

Per saperne di più...

...oltre a navigare attentamente sui siti ufficiali di Creative Commons e a frequentare le mailing list pubbliche della community (www.creativecommons.it/Liste), potete leggere la voce "Creative Commons" su www.wikipedia.org e le voci ad essa correlate; navigare sul sito www.copyleft-italia.it/cc e leggere le pubblicazioni liberamente scaricabili dal sito www.copyleft-italia.it/pubblicazioni, fra cui si segnalano principalmente:
- Aliprandi, Copyleft & opencontent. L'altra faccia del copyright (ed. PrimaOra, 2005);
- Aliprandi (a cura di), Compendio di libertà informatica e cultura open (ed. PrimaOra, 2005);
- Aliprandi, Teoria e pratica del copyleft. Guida all'uso delle licenze opencontent (ed. NDA Press, 2006);
- Aliprandi, Capire il copyright. Percorso guidato nel diritto d'autore (ed. PrimaOra, 2007);
- Lessig, Cultura libera (ed. Apogeo, 2005).

Brochure a scopo divulgativo realizzata da Simone Aliprandi per il Progetto Copyleft-Italia.it nel gennaio 2008. Parte del materiale qui riportato è tratto dai siti ufficiali Creative Commons e dall'opera "Il copyleft in tasca. Vademecum con i concetti base del copyleft" (www.copyleft-italia.it/vademecum).

L'URL originario di questo documento è: www.copyleft-italia.it/cc .

DISCLAIMER SUI DIRITTI D'AUTORE
I diritti d'autore sulla presente brochure appartegono a Simone Aliprandi, eccetto per le parti tratte dai siti ufficiali Creative Commons (come precisato dagli specifici links).
La presente brochure è rilasciata nei termini della ***Creative Commons Public License Attribution 3.0*** *il cui testo completo è disponibile alla pagina web http://creativecommons.org/licenses/by/3.0/legalcode.*

creative commons

un copyright flessibile
per opere creative

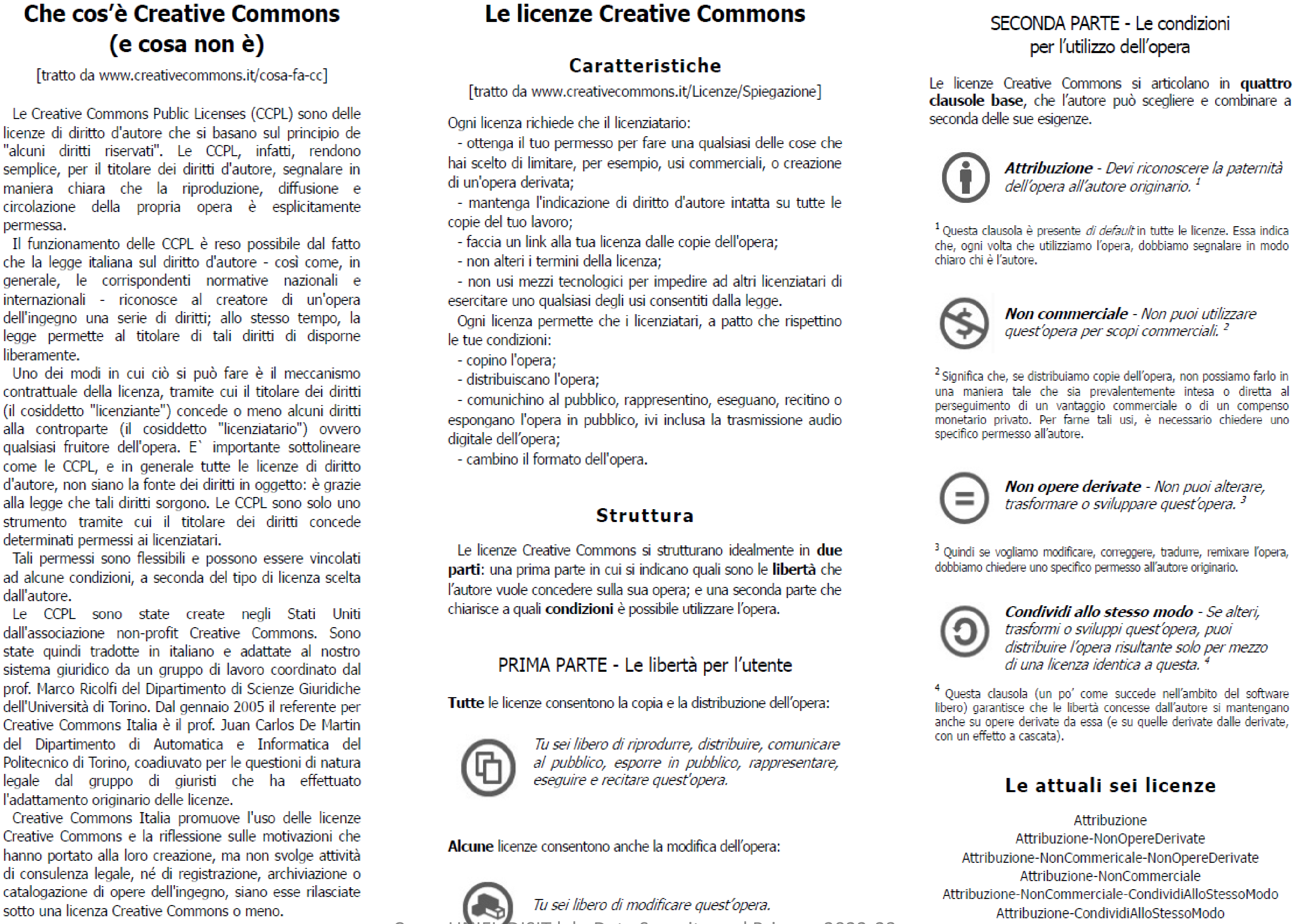
www.creativecommons.org
www.creativecommons.it

Brochure a scopo divulgativo a cura del
Progetto Copyleft-Italia.it

copyleft-italia.it
www.copyleft-italia.it

NUOVI MODELLI PER IL DIRITTO D'AUTORE

info@copyleft-italia.it - myspace.com/copyleftitalia



Che cos'è Creative Commons (e cosa non è)

[tratto da www.creativecommons.it/cosa-fa-cc]

Le Creative Commons Public Licenses (CCPL) sono delle licenze di diritto d'autore che si basano sul principio de "alcuni diritti riservati". Le CCPL, infatti, rendono semplice, per il titolare dei diritti d'autore, segnalare in maniera chiara che la riproduzione, diffusione e circolazione della propria opera è esplicitamente permessa.

Il funzionamento delle CCPL è reso possibile dal fatto che la legge italiana sul diritto d'autore - così come, in generale, le corrispondenti normative nazionali e internazionali - riconosce al creatore di un'opera dell'ingegno una serie di diritti; allo stesso tempo, la legge permette al titolare di tali diritti di disporne liberamente.

Uno dei modi in cui ciò si può fare è il meccanismo contrattuale della licenza, tramite cui il titolare dei diritti (il cosiddetto "licenziante") concede o meno alcuni diritti alla controparte (il cosiddetto "licenziatario") ovvero qualsiasi fruitore dell'opera. E` importante sottolineare come le CCPL, e in generale tutte le licenze di diritto d'autore, non siano la fonte dei diritti in oggetto: è grazie alla legge che tali diritti sorgono. Le CCPL sono solo uno strumento tramite cui il titolare dei diritti concede determinati permessi ai licenziatari.

Tali permessi sono flessibili e possono essere vincolati ad alcune condizioni, a seconda del tipo di licenza scelta dall'autore.

Le CCPL sono state create negli Stati Uniti dall'associazione non-profit Creative Commons. Sono state quindi tradotte in italiano e adattate al nostro sistema giuridico da un gruppo di lavoro coordinato dal prof. Marco Ricolfi del Dipartimento di Scienze Giuridiche dell'Università di Torino. Dal gennaio 2005 il referente per Creative Commons Italia è il prof. Juan Carlos De Martin del Dipartimento di Automatica e Informatica del Politecnico di Torino, coadiuvato per le questioni di natura legale dal gruppo di giuristi che ha effettuato l'adattamento originario delle licenze.

Creative Commons Italia promuove l'uso delle licenze Creative Commons e la riflessione sulle motivazioni che hanno portato alla loro creazione, ma non svolge attività di consulenza legale, né di registrazione, archiviazione o catalogazione di opere dell'ingegno, siano esse rilasciate sotto una licenza Creative Commons o meno.

Le licenze Creative Commons

Caratteristiche

[tratto da www.creativecommons.it/Licenze/Spiegazione]

Ogni licenza richiede che il licenziatario:
- ottenga il tuo permesso per fare una qualsiasi delle cose che hai scelto di limitare, per esempio, usi commerciali, o creazione di un'opera derivata;
- mantenga l'indicazione di diritto d'autore intatta su tutte le copie del tuo lavoro;
- faccia un link alla tua licenza dalle copie dell'opera;
- non alteri i termini della licenza;
- non usi mezzi tecnologici per impedire ad altri licenziatari di esercitare uno qualsiasi degli usi consentiti dalla legge.

Ogni licenza permette che i licenziatari, a patto che rispettino le tue condizioni:
- copino l'opera;
- distribuiscano l'opera;
- comunichino al pubblico, rappresentino, eseguano, recitino o espongano l'opera in pubblico, ivi inclusa la trasmissione audio digitale dell'opera;
- cambino il formato dell'opera.

Struttura

Le licenze Creative Commons si strutturano idealmente in **due parti**: una prima parte in cui si indicano quali sono le **libertà** che l'autore vuole concedere sulla sua opera; e una seconda parte che chiarisce a quali **condizioni** è possibile utilizzare l'opera.

PRIMA PARTE - Le libertà per l'utente

Tutte le licenze consentono la copia e la distribuzione dell'opera:

Tu sei libero di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera.

Alcune licenze consentono anche la modifica dell'opera:

Tu sei libero di modificare quest'opera.

SECONDA PARTE - Le condizioni per l'utilizzo dell'opera

Le licenze Creative Commons si articolano in **quattro clausole base**, che l'autore può scegliere e combinare a seconda delle sue esigenze.

Attribuzione *- Devi riconoscere la paternità dell'opera all'autore originario.* [1]

[1] Questa clausola è presente *di default* in tutte le licenze. Essa indica che, ogni volta che utilizziamo l'opera, dobbiamo segnalare in modo chiaro chi è l'autore.

Non commerciale *- Non puoi utilizzare quest'opera per scopi commerciali.* [2]

[2] Significa che, se distribuiamo copie dell'opera, non possiamo farlo in una maniera tale che sia prevalentemente intesa o diretta al perseguimento di un vantaggio commerciale o di un compenso monetario privato. Per farne tali usi, è necessario chiedere uno specifico permesso all'autore.

Non opere derivate *- Non puoi alterare, trasformare o sviluppare quest'opera.* [3]

[3] Quindi se vogliamo modificare, correggere, tradurre, remixare l'opera, dobbiamo chiedere uno specifico permesso all'autore originario.

Condividi allo stesso modo *- Se alteri, trasformi o sviluppi quest'opera, puoi distribuire l'opera risultante solo per mezzo di una licenza identica a questa.* [4]

[4] Questa clausola (un po' come succede nell'ambito del software libero) garantisce che le libertà concesse dall'autore si mantengano anche su opere derivate da essa (e su quelle derivate dalle derivate, con un effetto a cascata).

Le attuali sei licenze

Attribuzione
Attribuzione-NonOpereDerivate
Attribuzione-NonCommericale-NonOpereDerivate
Attribuzione-NonCommerciale
Attribuzione-NonCommerciale-CondividiAlloStessoModo
Attribuzione-CondividiAlloStessoModo

Ogni Licenza chiede che il Licensiatario

- Ottenga il tuo permesso per fare una qualsiasi delle cose che
  - hai scelto di limitare con la licenza,
  - for example: limitare gli usi commerciali o quelli di opera derivata
- Mantenga l'indicazione di diritto di autore intatta su tutte le copie del tuo lavoro
- Riporti un link alla licenza originale dalle copie dell'opera
- Non alteri i termini della licenza originale
- Non usi mezzi tecnologici per impedire ad altri licenziatari di esercitare uno qualsiasi degli usi consentiti dalla legge

seguenti azioni a patto che:
i licenziatari rispettino le condizioni della licenza

- Possono
  - Copiare l’opera;
  - Distribuire l’opera;
  - Comunicare al pubblico, rappresentare, esegure, recitare o esporre l’opera in pubblico,
  - trasmissione audio digitale dell’opera;
  - Cambiare il formato dell’opera (adattare)

Alcuni marker CC

creative commons

- **Liberta' per l'utente**
  - Sei libero di distribuire, comunicare, rappresentare, eseguire, recitare o esporre l'opera in pubblico, ivi inclusa la trasmissione audio digitale dell'opera;
  - Sei libero di modificare questa opera
- **Condizioni di uso**
  - Devi riconoscere la paternita' di questa opera
  - Per esempio citando e riportando un link alla sorgente

Licenze Creative Commons

creative commons

- Offrono 6 diverse articolazioni
  - per artisti, giornalisti, docenti, istituzioni e, in genere, creatori che desiderino **condividere in maniera ampia** le proprie opere secondo il modello **"alcuni diritti riservati"**.

- **Altre condizioni d'uso, il detentore dei diritti puo'**
  - non autorizzare a priori **usi prevalentemente commerciali** dell'opera (opzione *Non commerciale*, acronimo inglese: *NC*)
  - non autorizzare la creazione di **opere derivate** (*Non opere derivate*, acronimo: *ND*); no extract, no aggregate, ..
  - Imporre di rilasciarle **con la stessa licenza dell'opera originaria** (*Condividi allo stesso modo*, acronimo: *SA*, da "Share-Alike").

Le combinazioni di queste scelte generano 6 licenze CC, disponibili anche in versione italiana, come descritto in seguito!

2 of the 6 CC licenses, 1/3

- **Attribution Non-commercial No Derivatives (by-nc-nd)**
  - The most restrictive of our six main licenses, allowing redistribution.
  - This license is often called the "free advertising" license
  - *it allows others to download your works and share them with others as long as they mention you and link back to you,*
  - they can't change them in any way or use them commercially
- **Attribution Non-commercial Share Alike (by-nc-sa)**
  - *Let others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.*
  - Others can download and redistribute your work just like the by-nc-nd license, but they can also translate, make remixes, and produce new stories based on your work.
  - All new work based on yours will carry the same license, so any derivatives will also be non-commercial in nature.

2 of the 6 CC licenses, 2/3

creative commons

- **Attribution Non-commercial (by-nc)**
  - Let others remix, tweak, and build upon your work non-commercially, and their new works must also acknowledge you and be non-commercial,
  - they don’t have to license their derivative works on the same terms.

- **Attribution No Derivatives (by-nd)**
  - allows for redistribution, commercial and non-commercial,
  - as long as it is passed along unchanged and in whole, with credit to you

2 of the 6 CC licenses, 3/3

creative commons

- **Attribution Share Alike (by-sa)**
  - *lets others remix, tweak, and build upon your work even for commercial reasons, as long as they credit you and license their new creations under the identical terms.*
  - This license is often compared to open source software licenses.
  - All new works based on yours will carry the same license, so any derivatives will also allow commercial use.

- **Attribution (by)**
  - *lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation.*
  - This is the most accommodating of licenses offered, in terms of what others can do with your works licensed under Attribution.

Part 1a: sistemi di protezione

- Distribution models
- Terminologies
- Business Models & Value Chain
- Copy protection
- Conditional Access Systems
- Digital Rights Management
- Content Modeling and Packaging
- Licensing and content distribution
- Creative Commons Licensing
- Composition of Licenses, data aggregation

Compatibility Chart

A

B

	PUBLIC DOMAIN	0 PUBLIC DOMAIN	cc BY	cc BY SA	cc BY NC	cc BY ND	cc BY NC SA	cc BY NC ND
PUBLIC DOMAIN	✓	✓	✓	✓	✓	✗	✓	✗
0 PUBLIC DOMAIN	✓	✓	✓	✓	✓	✗	✓	✗
cc BY	✓	✓	✓	✓	✓	✗	✓	✗
cc BY SA	✓	✓	✓	✓	✗	✗	✗	✗
cc BY NC	✓	✓	✓	✗	✓	✗	✓	✗
cc BY ND	✗	✗	✗	✗	✗	✗	✗	✗
cc BY NC SA	✓	✓	✓	✗	✓	✗	✓	✗
cc BY NC ND	✗	✗	✗	✗	✗	✗	✗	✗

Licenses and More..

- **Licenses**: MPEG-21, ODRL, XACML, Xrml, etc..
  - Suitable for media, Unsuitable for data
- **Data Licenses**: CC, ODC, OGL, IODL
  - Mainly open data and declinations
  - **Permissions**: derivative, commercialize, derivative...
  - **Restrictions/duties**: attribution, notice, ...
- **Getting Composing Data Set → Licences Composition is needed**
  - **See www.disit.org/6877 extension**
- Formal models to **grant rights**
- Techniques for **right enforcement/verification**
  - **Almost missing on RDF stores**

License Combination example

dataset/graph description	license	SD	Duties		permisions				user categories				
		sharealike	attribution	notice	derivative	commecialize	redistribute	reproduce	Citizen	Tourist	Police	Civil protection	Firefighters
DigitalLocation	CC-By-NC-SA	✔	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔
Eneergy Cabins	protected	✘	✘	✘	✘	✘	✘	✔	✘	✘	✔	✔	✔
Commercial firms	CC-By	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Graph street	CC-By	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Services on the city	CC-By-NC	✘	✔	✔	✔	✘	✔	✔	✔	✔	✔	✔	✔
Renting bikes	CC-By	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Taxi	CC-By	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Enogastronomy	CC-By	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Course: Security and Privacy

Part on Privacy by Paolo Nesi

Topic: Privacy and GDPR

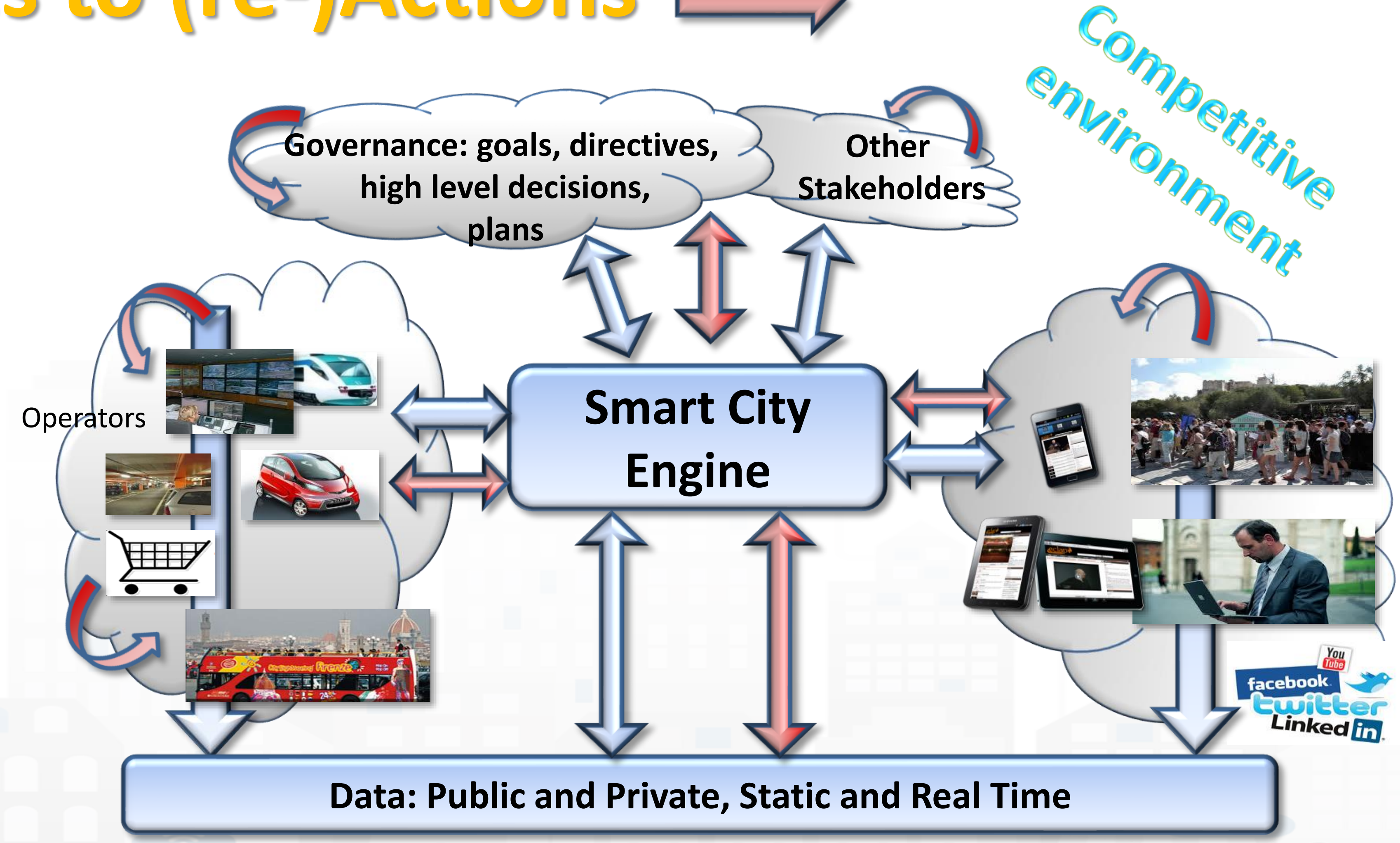
University of Florence, DISIT lab, Https://www.disit.org

Https://www.snap4city.org

Paolo.nesi@unifi.it

From Strategies to (re-)Actions

- Analyze
- Alerting, Early Warning
- Support Decision makers
- Plans
- Prescriptions
- Inform
- Suggest
- Engage
- Research

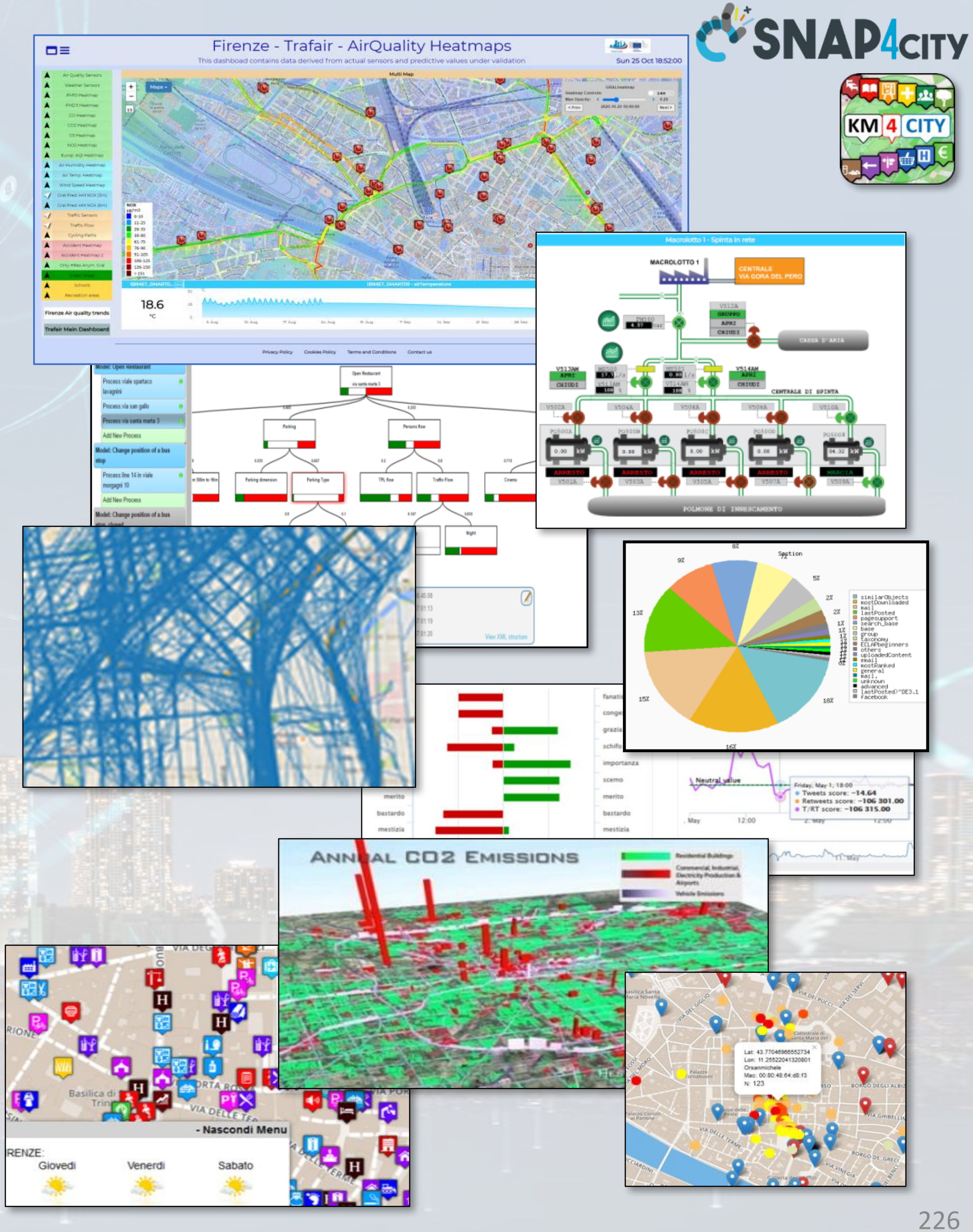

Competitive environment
Governance: goals, directives, high level decisions, plans
Other Stakeholders
Operators
Smart City Engine
Data: Public and Private, Static and Real Time
facebook
twitter
Linked in
You Tube

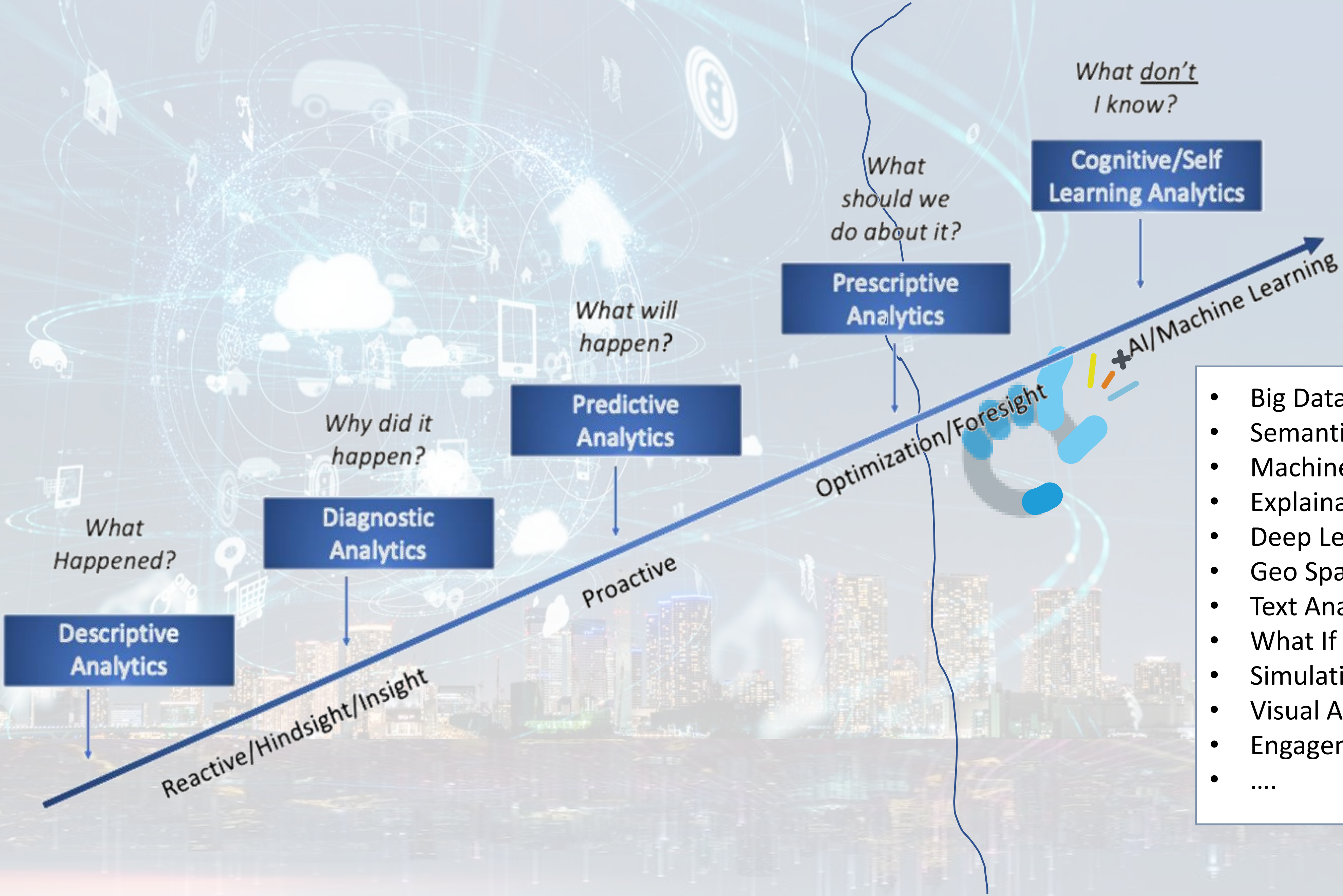
Security/Privacy Requirements

- **Managing** private data together with public data
- **Private data management** according to GDPR
  - Browsing, downloading, controlling rights, delegating access, revoking accesses, etc.
  - Keep them safe
- Secure enough to delegate management of data regarding public security:
  - Data that could be used against us by some terrorist, or anyway by someone with some bad intention, for example to access in our home when we are far away, etc.

Data Driven Decision Support

- Decision Support system
- Assessment / Strategies
- Data Rendering, visual analytics
- Data Processing
- Data aggregation, Storage, indexing
- Data Ingestion

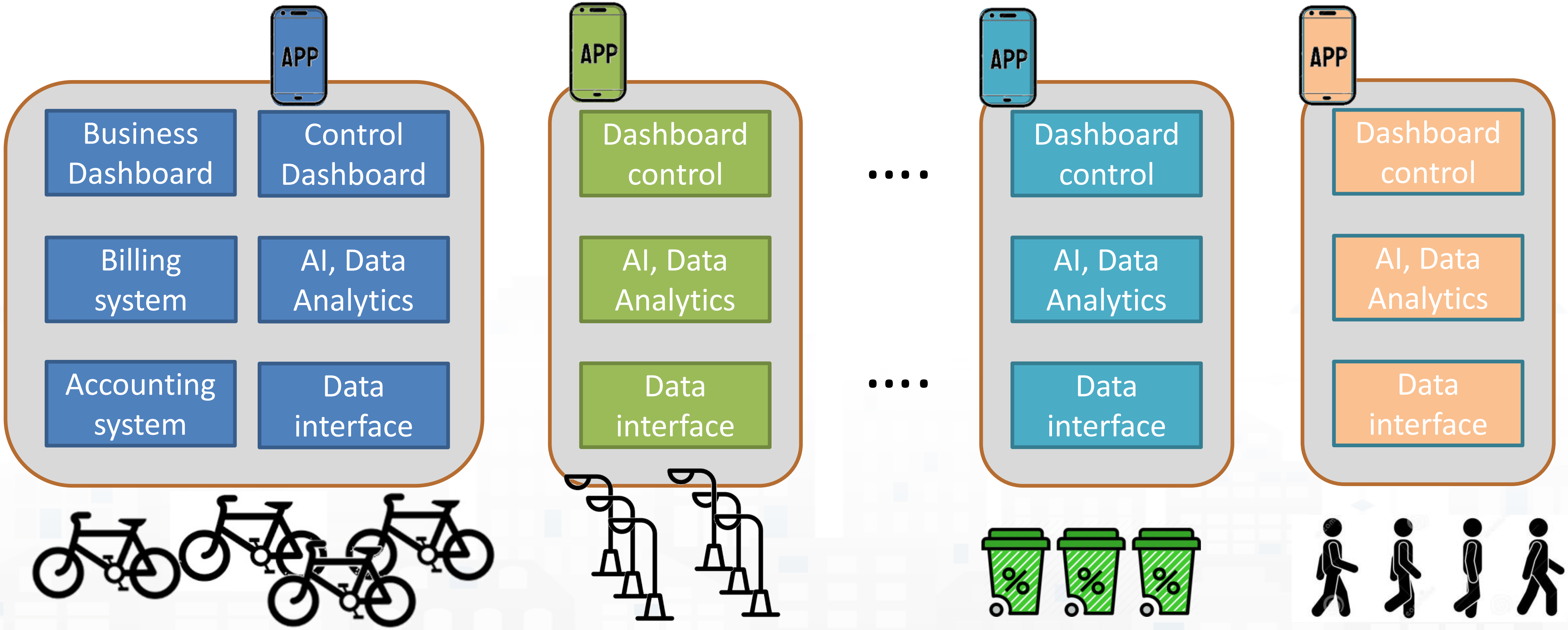

Firenze - Trafair - AirQuality Heatmaps
This dashboard contains data derived from actual sensors and predictive values under validation
Sun 25 Oct 18:52:00
Multi Map
18.6
Firenze Air quality trends
Trafair Main Dashboard
Macrolotto 1 - Spinta in rete
MACROLOTTO 1
CENTRALE VIA GORA DEL PERO
CASSA D'ARIA
CENTRALE DI SPINTA
POLMONE DI INNESCAMENTO
Model: Open Restaurant
Add New Process
Model: Change position of a bus stop
Neutral value
ANNUAL CO2 EMISSIONS
Residential Buildings
Commercial, Industrial, Electricity Production & Airports
Vehicle Emissions
- Nascondi Menu
Giovedì
Venerdì
Sabato



Sentient and active processes

- Big Data Analytics
- Semantic Computing
- Machine Learning
- Explainable Artificial Intelligence
- Deep Learning
- Geo Spatial Reasoning
- Text Analysis, Sentiment Analysis
- What If Analysis
- Simulations
- Visual Analytics
- Engagement Analysis
- ….

Avoiding to have a collection of verticals



Simplifying the development and integration of verticals

UNIVERSITÀ DEGLI STUDI FIRENZE | DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE | DISIT DISTRIBUTED SYSTEMS AND INTERNET TECHNOLOGIES LAB | SNAP4CITY | KM4CITY

www.snap4city.org

Tools for rapid implementation of sustainable Smart Solutions and Decision Support Systems

100% OPEN SOURCE

Powered by FIWARE

FREE TRIAL

PEN Test Passed

EU GDPR COMPLIANT

SNAP4 Appliances and Dockers Installations

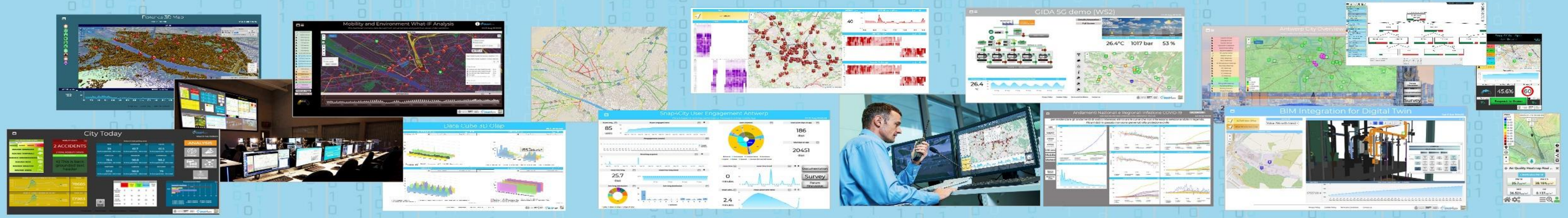
EUROPEAN OPEN SCIENCE CLOUD

Node-RED

JS Foundation

E015 digital ecosystem

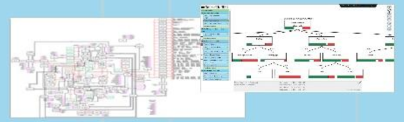
NVIDIA



Florence3D Map
Mobility and Environment What-IF Analysis
City Today
2 ACCIDENTS
ANALYSIS
Data Cube 3D Olap
Snap4City User Engagement Antwerp
186
20451
Survey
GIDA 5G demo (WS2)
26.4°C
1017 bar
53 %
Antwerp City Overview
BIM Integration for Digital Twin
Andamento Nazionale e Regionale Infezioni COVID-19
45.6%
Air Quality Heatmap

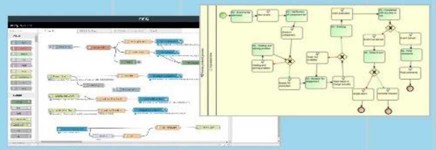
DASHBOARDS AND APPS - CONTROL ROOMS - DECISION SUPPORT SYSTEMS - WHAT-IF ANALYSIS - VISUAL ANALYTICS

PREDICTION - ANOMALY DETECTION - ENVIRONMENTAL MODEL - 3D MODEL
KPI - SIMULATION - EARLY WARNING - SYNOPTIC - DIGITAL TWIN - VIRTUAL REALITY



EXPERT SYSTEM
KNOWLEDGE BASE
STORAGE

BIG DATA ANALYTICS
EXPLAINABLE ARTIFICIAL INTELLIGENCE
BUSINESS INTELLIGENCE
MACHINE LEARNING

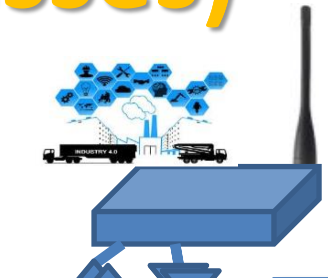


DATA FLOWS, DATA DRIVEN
WORKFLOWS, MICROSERVICES
PARALLEL DISTRIBUTED PROCESSING

METHODOLOGIES
COURSES AND COMMUNITY
LIVING LABS
DEVELOPMENT TOOLS

Data Collection, ingestion (processes)

- **Data**
  - Open and private: Open Data: CKAN
    - licensing, private, GDPR
  - Static vs Real time
  - Any protocol, any standard: Push and Pull
  - Any format
- From **observations and milestones**:
  - sensors, database, KPI, etc.
- From **legacy services** of in-place operators
  - External Services: call of any kind
  - MicroServices, MicroApplications
  - Local databases
- From **citizens, city users, tourists, operators, ..**:
  - participated processes, feedback, Apps, etc.
  - Crawling web pages, etc.



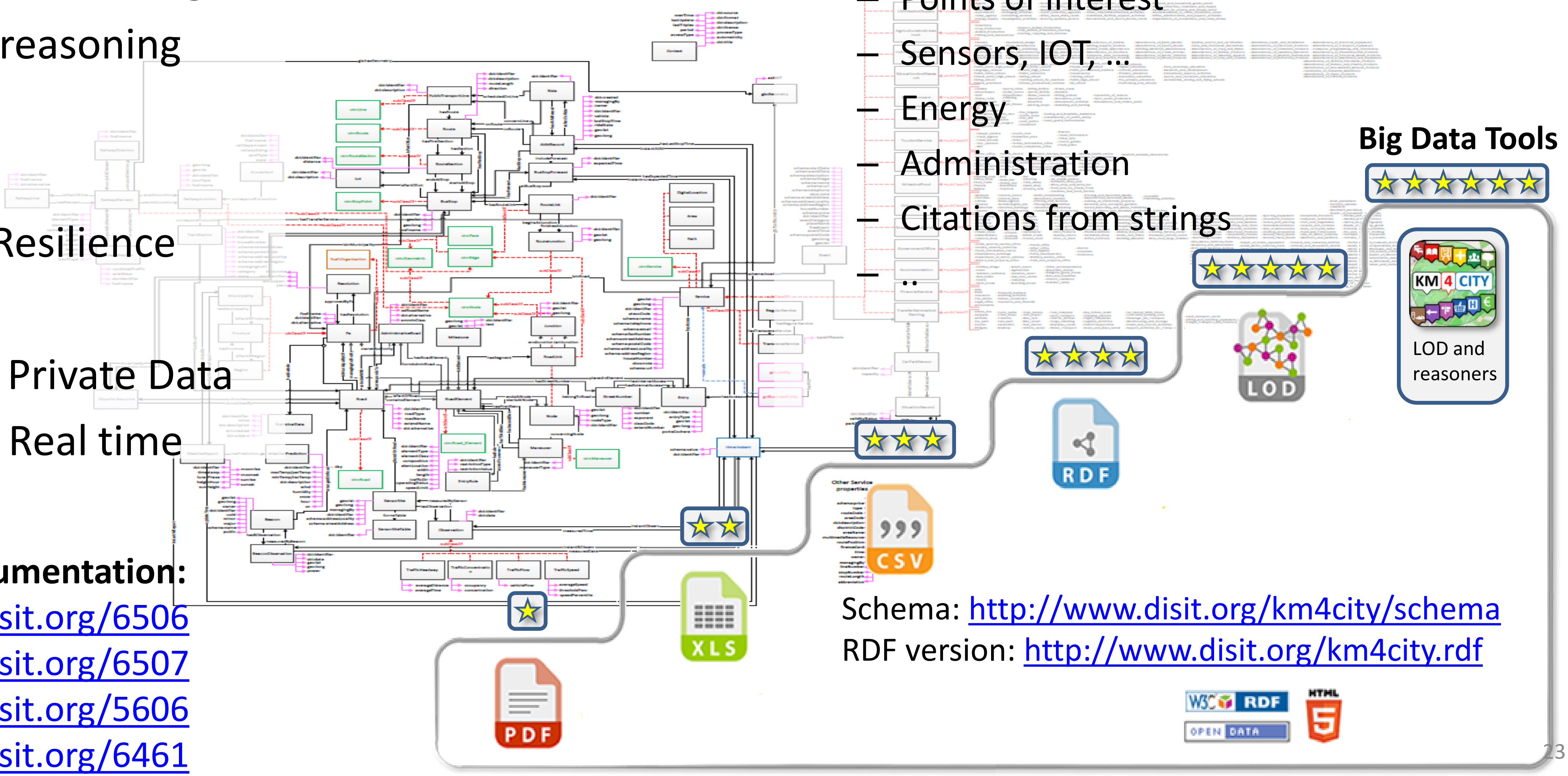
ckan

IOT Device
Air Quality Map
What kind of air are you breathing outside right now?
Reset
Calculate
user-analisi-v2-0.xlsx
user-analisi-v2-0-anonymous.xlsx
users-analysis.xlsx

Km4City: Knowledge Base

- **Multiple DOMAINS**
- Geospatial reasoning
- Temporal reasoning
- Metadata
- Statistics
- Risk and Resilience
- Licensing
- Open and Private Data
- Static and Real time
- IOT/IOE

- Street-Guide
- Mobility and transport
- Points of interest
- Sensors, IOT, …
- Energy
- Administration
- Citations from strings
- ..



Schema: http://www.disit.org/km4city/schema

RDF version: http://www.disit.org/km4city.rdf

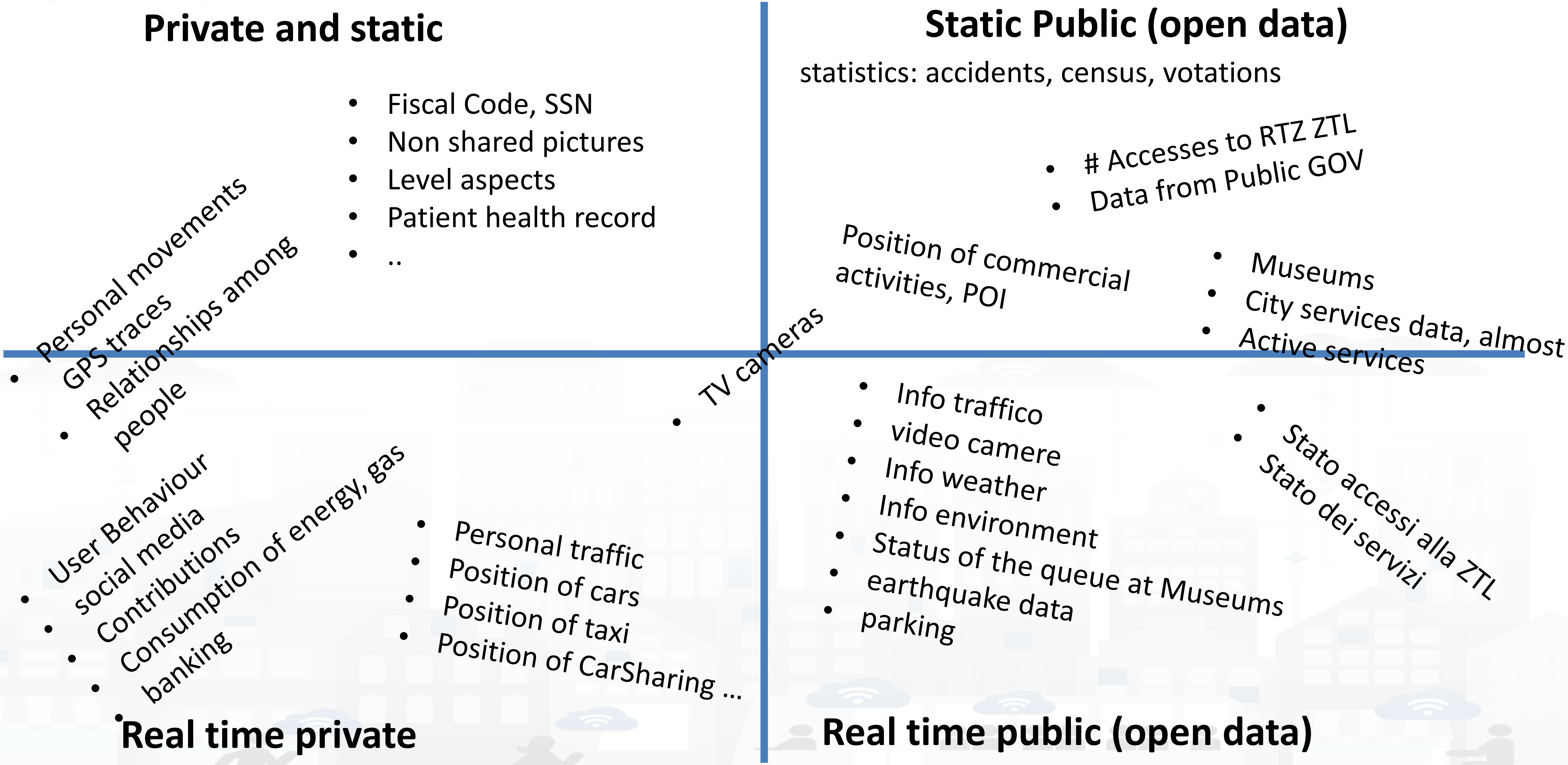
Ontology Documentation:

http://www.disit.org/6506

http://www.disit.org/6507

http://www.disit.org/5606

http://www.disit.org/6461



Private and static

- Fiscal Code, SSN
- Non shared pictures
- Level aspects
- Patient health record
- ..

- Personal movements
- GPS traces
- Relationships among people

Static Public (open data)

statistics: accidents, census, votations

- # Accesses to RTZ ZTL
- Data from Public GOV

Position of commercial activities, POI

- Museums
- City services data, almost
- Active services

- TV cameras

- User Behaviour
- social media
- Contributions
- Consumption of energy, gas
- banking

- Personal traffic
- Position of cars
- Position of taxi
- Position of CarSharing …

Real time private

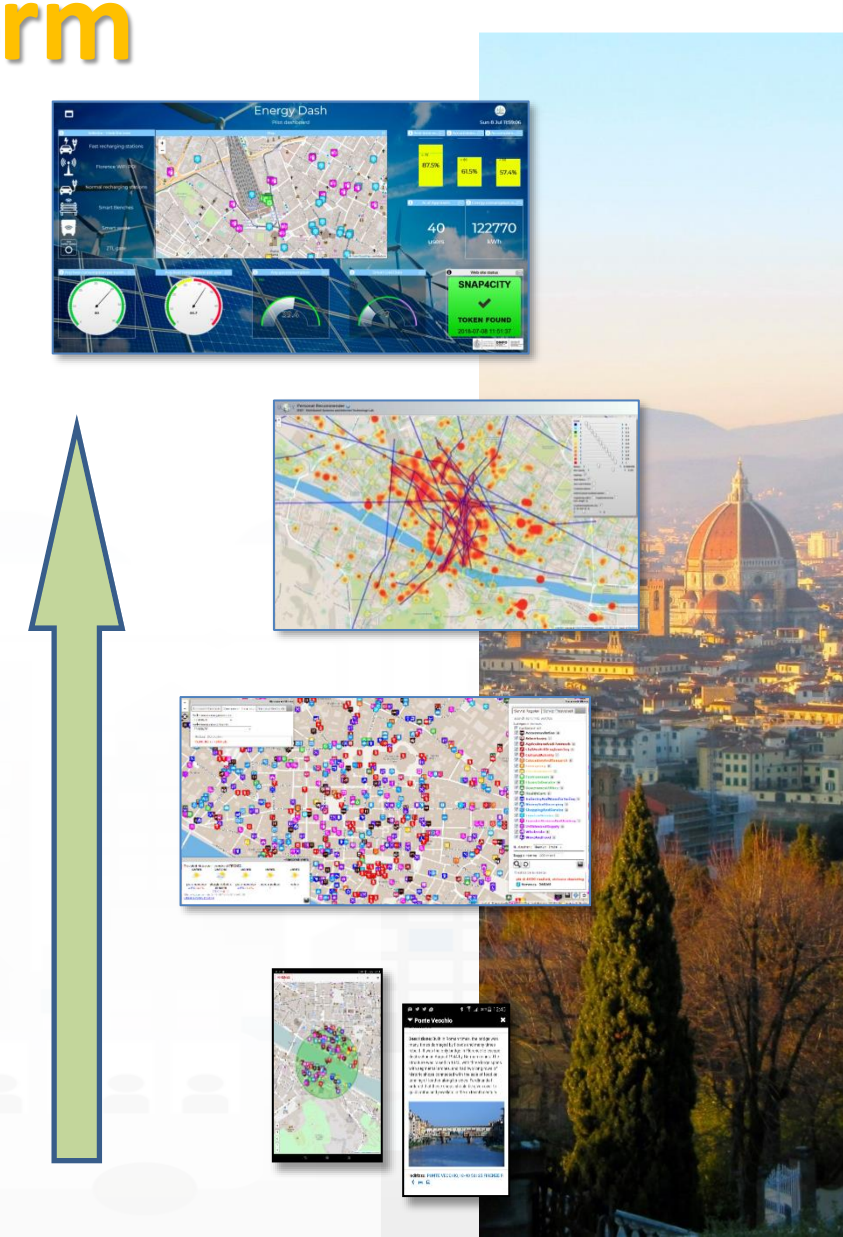
- Info traffico
- video camere
- Info weather
- Info environment
- Status of the queue at Museums
- earthquake data
- parking

- Stato accessi alla ZTL
- Stato dei servizi

Real time public (open data)

Integrated Urban Platform

- **Produce value from data supporting Living lab**
  - Stimulate virtuous behavior, influence City Users!
  - Put in action CITY Strategies
- **Data Exploitation performing**
  - predictions, reasoning, business intelligence, ..
  - users behavior analysis, decision support system, ..
  - Control Room, Real Time Monitoring tools, ….
- **Aggregate & integrate data**
  - Multiple protocols from urban operators, ...
  - open data, IOT, sensors, internet of everything, cloud, mobile devices, Wi-Fi, social media, ...



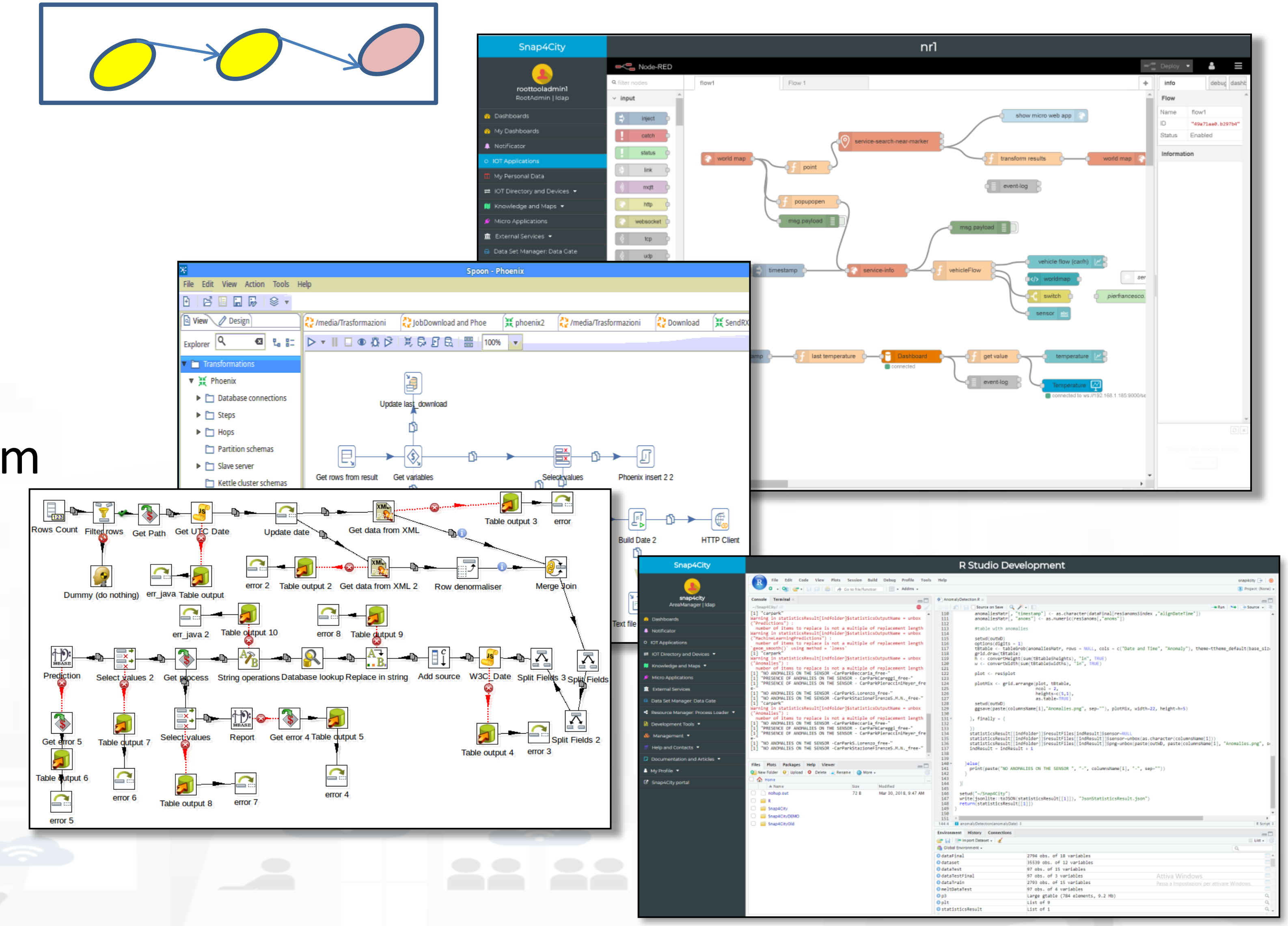
Data Indexing & Semantic Data Indexing

- **Textual**, multilingual, NLP (Natural Language Processing)
  - For social media data, but also for metadata, descriptions
- **Spatial**, **geographical**, georeversing → Knowledge Base, Km4City
  - Around a point, along a line/path, near a path, into a polyline, etc.
- **Temporal** → Historical data
- **Semantic:** relationships among city entities.
- **Data Value** different data type (Data Lake/normalization), data unit, etc. → the so called IOT shadowing of Azure, AWS
  - Relating to Knowledge Base reciprocally

- ***Traffic** / volume of Data (KBps) → Network Analysis, monitoring*

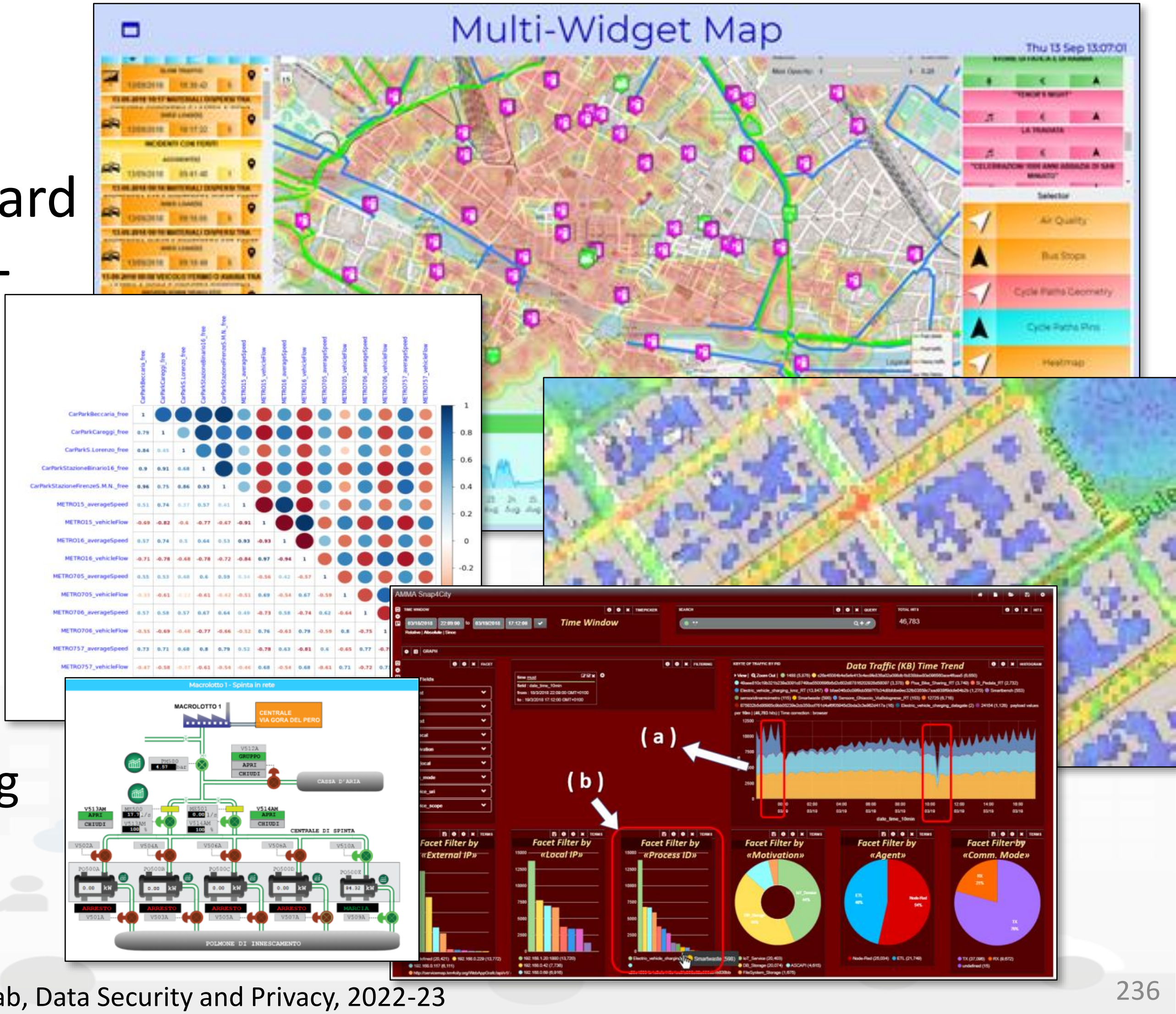
Data processing

- **Data analytics**
  - Periodic or event driven
    - On demand
  - Data transformation
    - ETL: extract transform load
  - Control Flow, data transform
    - Node-RED: Node.JS
- **For example**:
  - Assessment/monitoring
  - Predictions
  - Anomaly detection
  - Simulations
  - Etc.



Data Rendering vs Control Room Dashboards

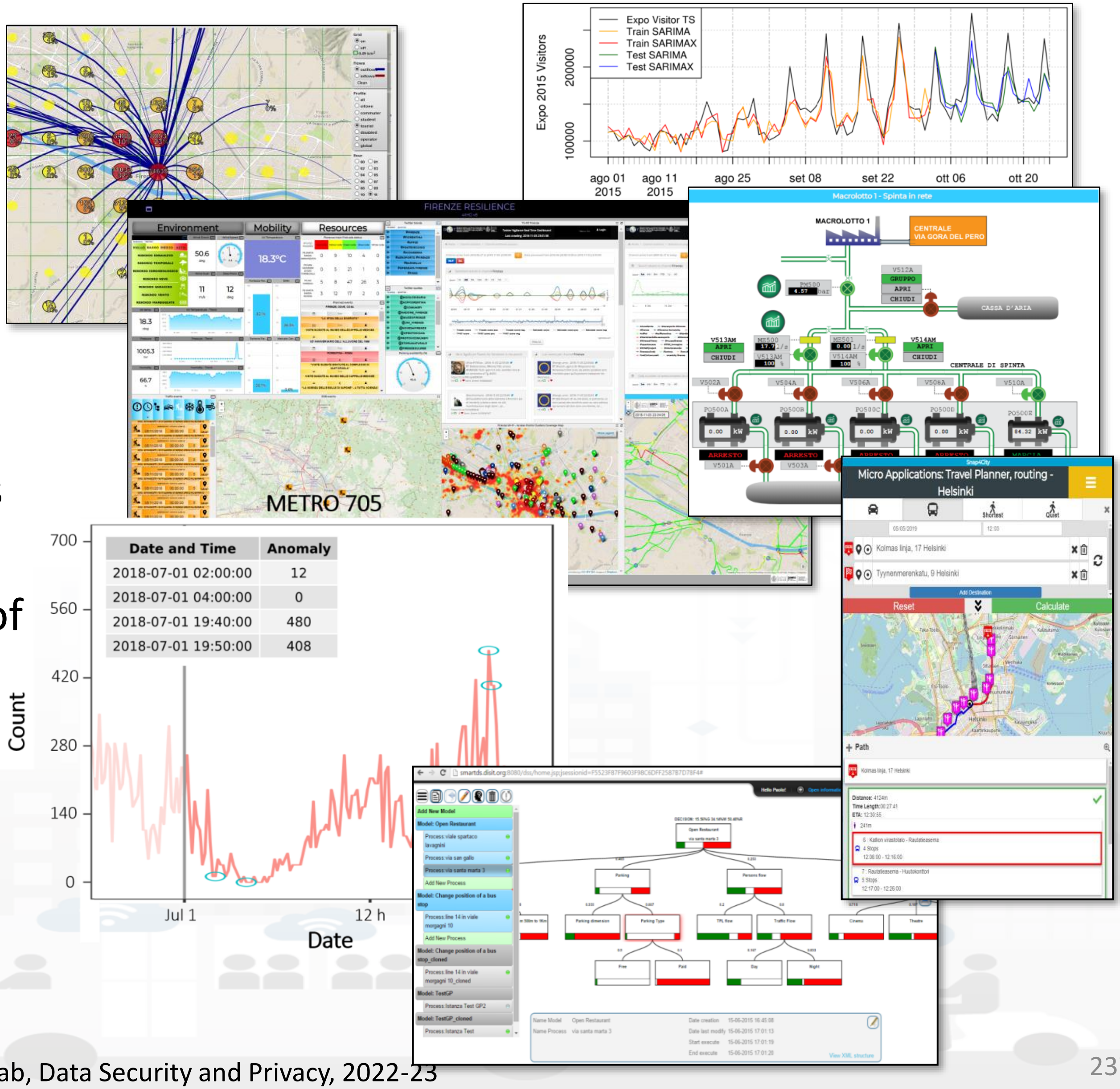
- **GIS** rendering by layers
- **Business intelligence** mainly focused on making statistics from tabular: no layer, hard relationships, ... Exploit Data Analytic, ETL
- **Visual Analytics**, data understanding
  - Rendering and drill down
  - Faceting/grouping (Elastic Search/SOLR)
  - Cross filtering (Kibana, Grafana, Banana)
  - Interactive, Cross Widgeting
- **Control Room Dashboards:**
  - Need: Visual Analytics, Data Analytic, geospatial reasoning, data driven processing
  - H24, alerting, Flexible rendering, custom widgets, interactive dashboards


Multi-Widget Map
Thu 13 Sep 13:07:01
Air Quality
Bus Stops
Cycle Paths Geometry
Cycle Paths Pins
Heatmap
Macrolotto 1 - Spinta in rete
MACROLOTTO 1
CENTRALE VIA GORA DEL PERO
CASSA D'ARIA
POLMONE DI INNESCAMENTO
Time Window
Data Traffic (KB) Time Trend
(a)
(b)
Facet Filter by «External IP»
Facet Filter by «Local IP»
Facet Filter by «Process ID»
Facet Filter by «Motivation»
Facet Filter by «Agent»
Facet Filter by «Comm. Mode»

Decision Support, Act!

Smart City Control Room, SCCR, SCR

- – Not only a collection of verticals
- **Exploiting analytics**: prediction, simulations, anomaly detection. ..
  - – Big data approach to Data Analytics
- **Connecting Heterogeneous data** to defined strategies and alerting
- **Connected interactive dashboards** for different kind of decision makers: operators and majors
- **What-if Analysis taking into account multiple data sources**



Date and Time	Anomaly
2018-07-01 02:00:00	12
2018-07-01 04:00:00	0
2018-07-01 19:40:00	480
2018-07-01 19:50:00	408

From strategies to Actions

- Public vs private
  - What is private and what is public
  - Privacy vs safety
  - GDPR
- Data Privacy
- Data Analytics
  - Bias
  - Data anonymization
- AI:
  - Unbias learning
  - Explainable AI
  - Trsutworthy
  - Ethical aspects: incidental finding
- Slide su snap4city:
  - Connesse alla security
  - Connesse alla privacy e GDPR
  - GDPR verification

TOP

Data Protection, Personal Data vs GDPR

GDPR: General Data Protection Regulation

Users may decide to:

- provide access to who, for do what, until when consented
- accept terms of use by **signed** consent **for** data management **service**

From each service, the user is capable to:

- **See** what we collect in terms of Data Type: traces, logs, paths, profiles, accesses, IOT devices, sensors, maps, etc.
- **Download**, **delete**, **inspect** Data
- **Auditing** and **Revoke access** or **grant** access right to each **single Data**
- **Delete all Data in single shot** or singularly (**forget all about me**)

- Correctness
- Transparency
- Security
- Integrity
- Privacy
- Auditing
- …

GDPR: General Data Protection Regulation

If personal data are **published by the owner:**

– the data are **released anonymously**,
→ also in this case they can be **revoked at any time**:

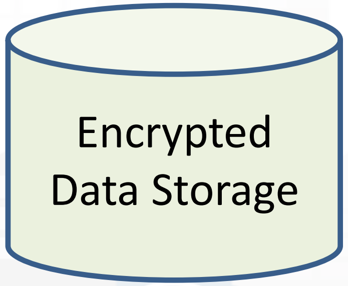
Snap4City is also compliant to GDPR **Technical Constraints** as:

– **Secure connection** in any private data exchange

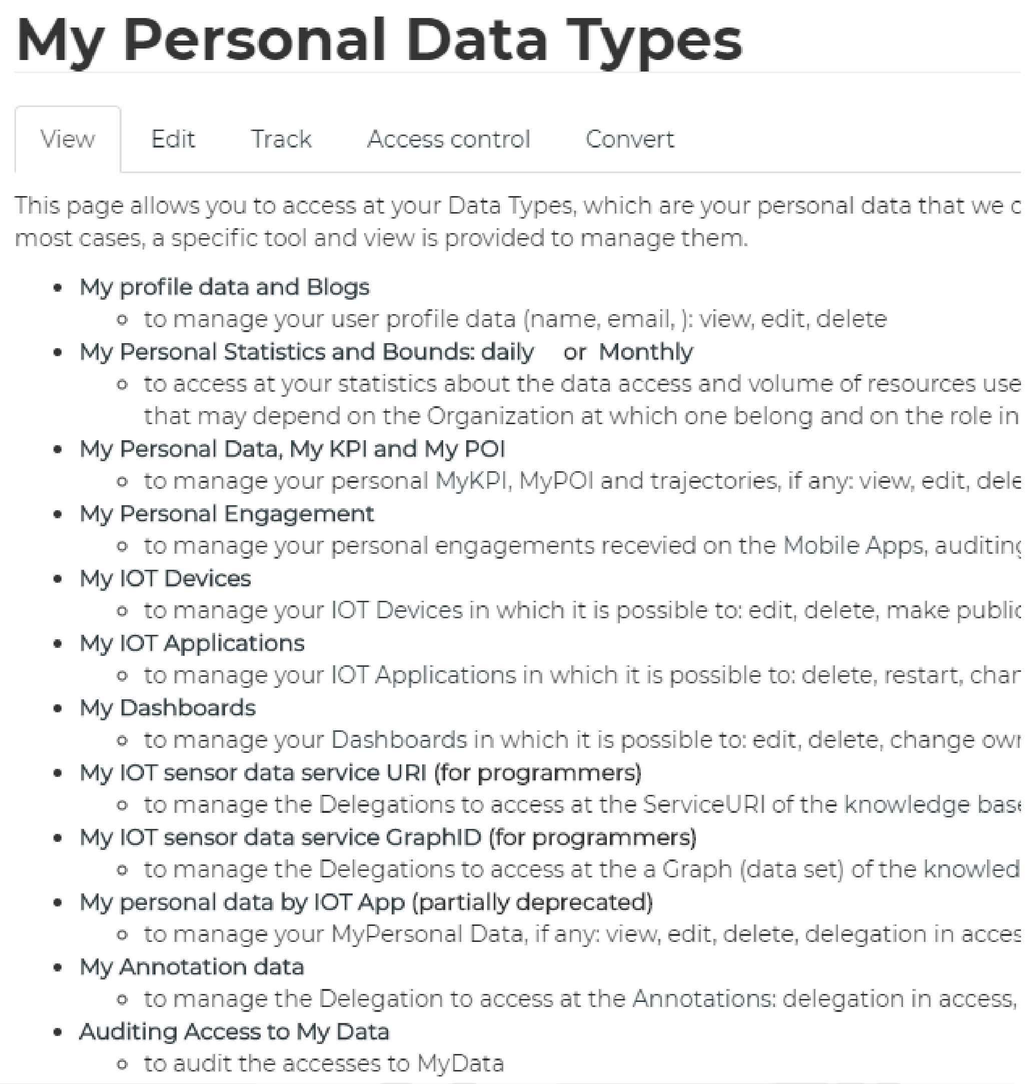
– **Encrypted** data store for all private data

– **Decoupling** data and personal IDs

– Allow the **Auditing** of private data usage


Encrypted Data Storage

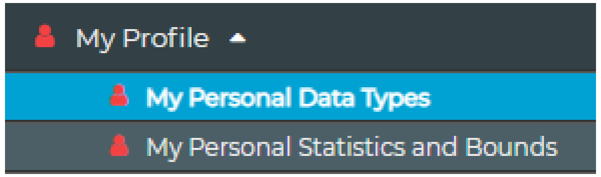
GDPR Compliant



My Personal Data Types

This page allows you to access at your Data Types, which are your personal data that we c
most cases, a specific tool and view is provided to manage them.

- My profile data and Blogs
  - to manage your user profile data (name, email,): view, edit, delete
- My Personal Statistics and Bounds: daily   or Monthly
  - to access at your statistics about the data access and volume of resources use that may depend on the Organization at which one belong and on the role in
- My Personal Data, My KPI and My POI
  - to manage your personal MyKPI, MyPOI and trajectories, if any: view, edit, dele
- My Personal Engagement
  - to manage your personal engagements recevied on the Mobile Apps, auditing
- My IOT Devices
  - to manage your IOT Devices in which it is possible to: edit, delete, make public
- My IOT Applications
  - to manage your IOT Applications in which it is possible to: delete, restart, char
- My Dashboards
  - to manage your Dashboards in which it is possible to: edit, delete, change own
- My IOT sensor data service URI (for programmers)
  - to manage the Delegations to access at the ServiceURI of the knowledge base
- My IOT sensor data service GraphID (for programmers)
  - to manage the Delegations to access at the a Graph (data set) of the knowled
- My personal data by IOT App (partially deprecated)
  - to manage your MyPersonal Data, if any: view, edit, delete, delegation in acces
- My Annotation data
  - to manage the Delegation to access at the Annotations: delegation in access,
- Auditing Access to My Data
  - to audit the accesses to MyData



Manage Profile and MyPersonalData

For each Data Type:

- Start as private → making them public (anonymous) and revoke
- The Owner is the only one that can: (1) modify values; (2) change the ownership
- Define/revoke Delegation to Access
- Delete/forget per Data Type and “me all”!
- Auditing

GDPR vs Snap4City

GDPR Compliance Verification Feature	Verif.	Reqs.
Signed consent	UI	R8
User profile management and control	UI	R13
Data Type private as default	UI	R8
Rights to access per element	UI	R9
Rights to transfer per element	UI	R10
Rights to erase per element and total	UI	R13
Rights to revoke/change per Data Type	UI	R10
An interface for Right management for Data Type	UI	R9
Clear Terms of Use and Privacy Policy	UI	--
Auditing Tools for Data Type	UI	R14
Publish as Anonymous	UI	R9
Encrypt personal users’ data	Code	R12
Secure Authentication and Authorization	Code	R3
Data protection by Design	Code	R17
Secure connection	Code	R6
Security Control, data breach control, anonymization, etc.	PEN Test	R15, R16, R18

- C. Badii, P. Bellini, A. Difino, P. Nesi, "Smart City IoT Platform Respecting GDPR Privacy and Security Aspects", accepted for publication on IEEE Access, 2020. 10.1109/ACCESS.2020.2968741 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8966344

IEEE Access
Multidisciplinary ⁞ Rapid Review ⁞ Open Access Journal

Received January 7, 2020, accepted January 19, 2020, date of publication January 22, 2020, date of current version February 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2968741

Smart City IoT Platform Respecting GDPR Privacy and Security Aspects

CLAUDIO BADII, PIERFRANCESCO BELLINI, ANGELO DIFINO, AND PAOLO NESI, (Member, IEEE)
Department of Information Engineering, University of Florence, 50121 Florence, Italy

Corresponding author: Paolo Nesi (paolo.nesi@unifi.it)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Program under Agreement 688196.

ABSTRACT The Internet of Things (IoT) paradigm enables computation and communication among tools that everyone uses daily. The vastness and heterogeneity of devices and their composition offer innovative services and scenarios that require a new challenging vision in interoperability, security and data management. Many IoT frameworks and platforms claimed to have solved these issues, aggregating different sources of information, combining their data flows in new innovative services, providing security robustness with respect to vulnerability and respecting the GDPR (General Data Protection Regulation) of the European Commission. Due to the potentially very sensible nature of some of these data, privacy and security aspects have to be taken into account by design and by default. In addition, an end-to-end secure solution has to guarantee a secure environment at the final users for their personal data, in transit and storage, which have to remain under their full control. In this paper, the Snap4City architecture and its security solutions that also respect the GDPR are presented. The Snap4City solution addresses the full stack security, ranging from IoT Devices, IoT Edge on premises, IoT Applications on the cloud and on premises, Data Analytics, and Dashboarding, presenting a number of integrated security solutions that go beyond the state of the art, as shown in the platform comparison. The stress test also included the adoption of penetrations tests verifying the robustness of the solution with respect to a large number of potential vulnerability aspects. The stress security assessments have been performed in a piloting period with more than 1200 registered users, thousands of processes per day, and more than 1.8 million of complex data ingested per day, in large cities such as Antwerp, Helsinki and the entire Tuscany region. Snap4City is a solution produced in response to a research challenge launched by the Select4Cities H2020 research and development project of the European Commission. Select4Cities identified a large number of requirements for modern Smart Cities that support IoT/IoE (Internet of Things/Everything) in the hands of public administrations and Living Labs, and selected a number of solutions. Consequently, at the end of the process after 3 years of work, Snap4City has been identified as the winning solution.

INDEX TERMS End-2-end, GDPR, IoT, security, smart city.

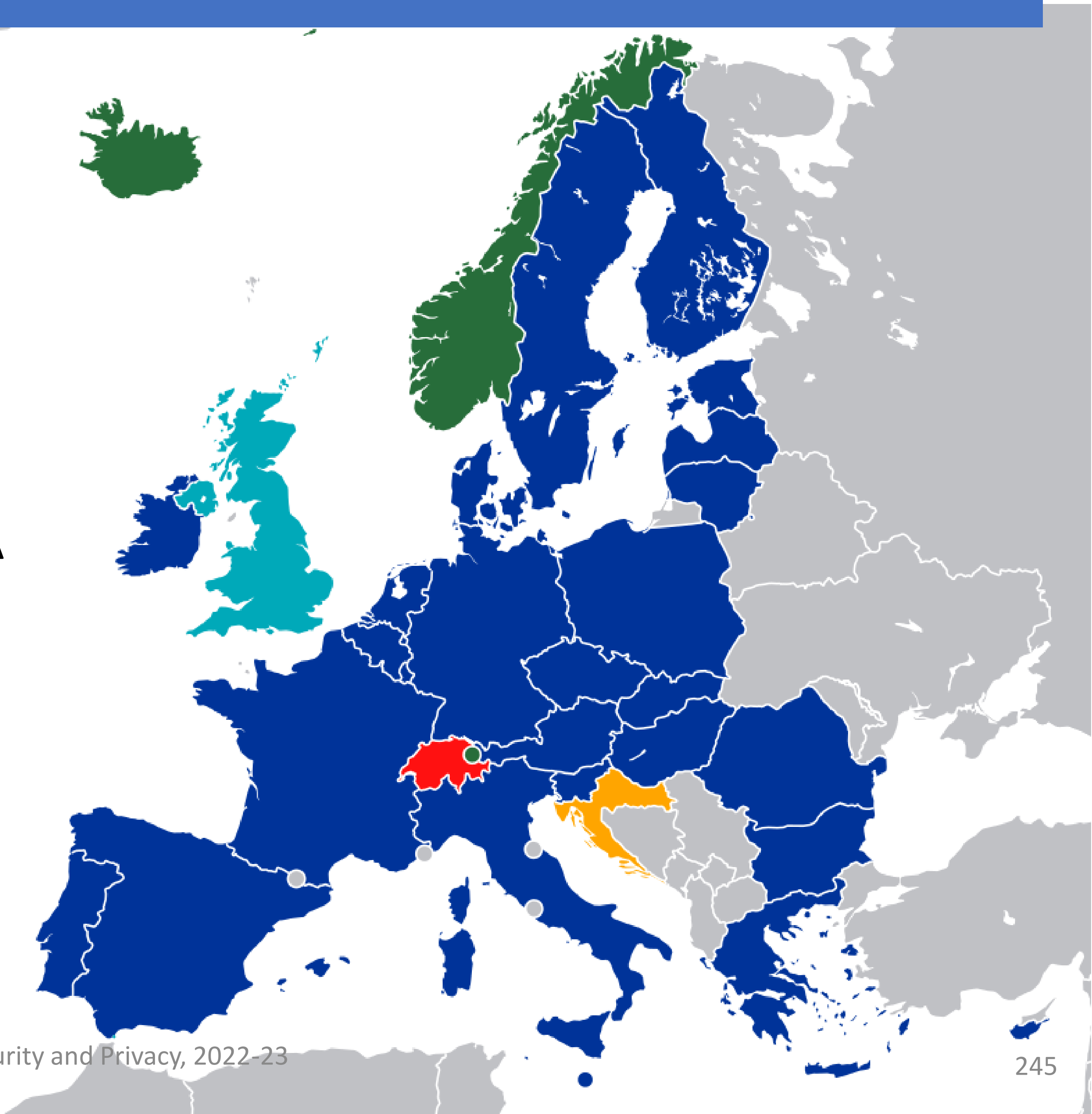
I. INTRODUCTION

IoT (Internet of Thing) is becoming a disruptive technology, especially for city users of metropolitan areas. The pervasiveness of IoT Devices, integrated in common objects, is becoming increasingly deeper. The addresses' space for these devices would be enough to point any sensors of any devices at any moment without restrictions. Diffuse products that implement *Low-Power Wide Area Networks* (LPWAN) technologies for IoT introduced by SigFox and Semtech (LoRa, Long Range) have been gaining interest and have been under intense deployment campaigns worldwide [1]. At the same time, *short range* IoT devices (based on technologies such as IEEE 802.15.4 or Bluetooth Low Energy, BLE, [2]) are sold in increasing quantities and are already able to support scenarios for smart homes, energy metering and industrial automation. On the other hand, the start of the diffusion of *5G devices* and services is creating high expectations in networking IoT technologies, as the killer application of previous technologies in metropolitan areas.

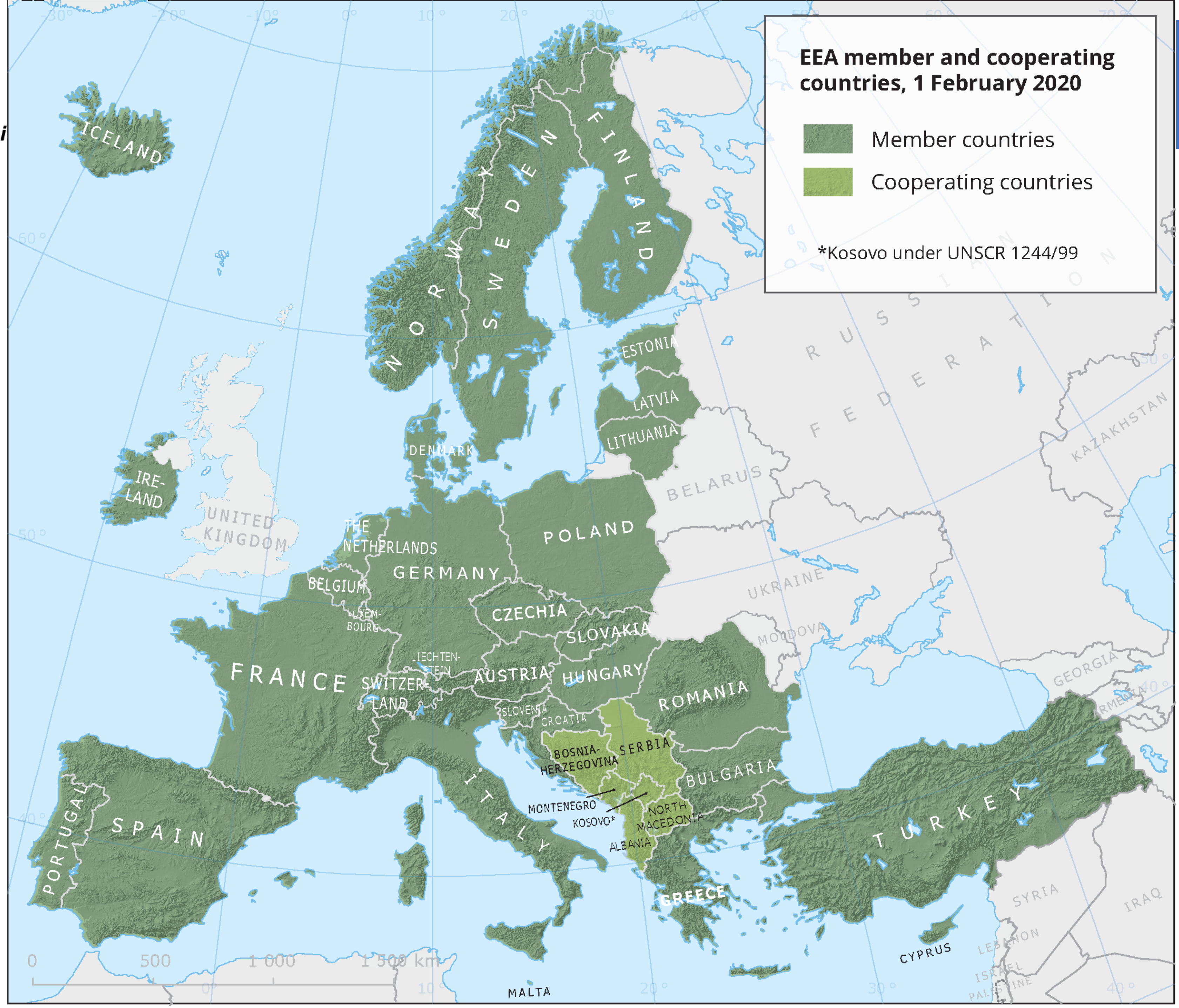
The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

General Data Protection Regulation (1)

- GDPR is:
  - a regulation (not a directive)
    - Regulation is a law, while a directive is a recommendation
  - proposed by the European Union
  - on data protection and privacy
  - for all individuals within EU+EEA (European Economic Area)
    - EFTA: Iceland, Swiss, Norway, Liechtenstein
  - + export of personal data outside the EU and EEA areas
  - Adopted 2016, April 27th
  - Operative since 2018, May 25th



🟦 EU states which form part of the EEA
🟩 EFTA states which form part of the EEA
🟨 EU state which forms part of the EEA through the provisional application of an accession agreement
🟥 EFTA state which signed the EEA agreement but did not join
🟦 Former EU state which has withdrawn from the EEA


EEA member and cooperating countries, 1 February 2020
🟩 Member countries
🟩 Cooperating countries
*Kosovo under UNSCR 1244/99
ICELAND
NORWAY
SWEDEN
FINLAND
ESTONIA
LATVIA
LITHUANIA
DENMARK
IRE-LAND
UNITED KINGDOM
THE NETHERLANDS
BELGIUM
LUXEM-BOURG
GERMANY
POLAND
CZECHIA
SLOVAKIA
LIECHTEN-STEIN
AUSTRIA
HUNGARY
FRANCE
SWITZER-LAND
SLOVENIA
CROATIA
ROMANIA
BOSNIA-HERZEGOVINA
SERBIA
BULGARIA
MONTENEGRO
KOSOVO*
NORTH MACEDONIA
ALBANIA
ITALY
PORTUGAL
SPAIN
GREECE
TURKEY
CYPRUS
MALTA
RUSSIAN FEDERATION
BELARUS
UKRAINE
MOLDOVA
KAZAKHSTAN
GEORGIA
ARMENIA
SYRIA
IRAQ
LEBANON
ISRAEL
PALESTINE
0
500
1 000
1 500 km

General Data Protection Regulation (2)

- It Substitutes
  - Europe → Directive 95/46/CE
  - Italy → d. lgs. n. 196/2003 (codice per la protezione dei dati personali)

- The following cases are not covered by the regulation:
  - Lawful interception, national security, military, police, justice
  - *Public interest statistical and scientific analysis*
  - Deceased persons (national legislation, consent)
  - Employer-employee (dedicated law, human dignity)
  - Purely personal nature or household activity

Reception/Impact

- Thousands of amendments were proposed in the process of definition
- The total cost for EU companies is estimated at around *€200 billion* while for US companies the estimate is for *$41.7 billion*

- *Research indicates that approximately 25% of software vulnerabilities have GDPR implications (emphasizes breaches, not bugs)*
- After the implementation of the GDPR, the US state of California passed a similar bill called The California Consumer Privacy Act (CCPA, 2018)
- Moreover, The New York Privacy Act (NYPA, 2019), plat to give residents there more control over their data than in any other US state. by 2021

- 12 months after the Regulation took effect, an Egress report found that 52% of organizations weren't fully complying with the GDPR.

Main concepts

The six main principles

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality

The seventh principles

- Controller–processor contracts;
- Relevant policies and procedures;
- Privacy notices;
- Staff training records;
- Security monitoring and event logging records;
- Data breach records; and
- Data protection impact assessments.

TOP

GDPR analysis

Content

- The GDPR consists of 99 *articles*, grouped into 11 chapters, and an additional 173 *recitals* with explanatory remarks. Italian version is 88 pages long.
- Chapters' headings:

I - General provisions

II - Principles

III - Rights of the data subject

IV - Controller and processor

V - Transfers of personal data to third countries or international organizations

VI - Independent supervisory authorities

VII - Cooperation and consistency

VIII - Remedies, liability and penalties

IX - Provisions relating to specific processing situations

X - Delegated acts and implementing acts

XI - Final provisions

I - Disposizioni generali

II - Principi

III - Diritti dell'interessato

IV - Titolare del trattamento e responsabile del trattamento

V - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

VI - Autorità di controllo indipendenti

VII - Cooperazione e coerenza

VIII - Mezzi di ricorso, responsabilità e sanzioni

IX - Disposizioni relative a specifiche situazioni di trattamento

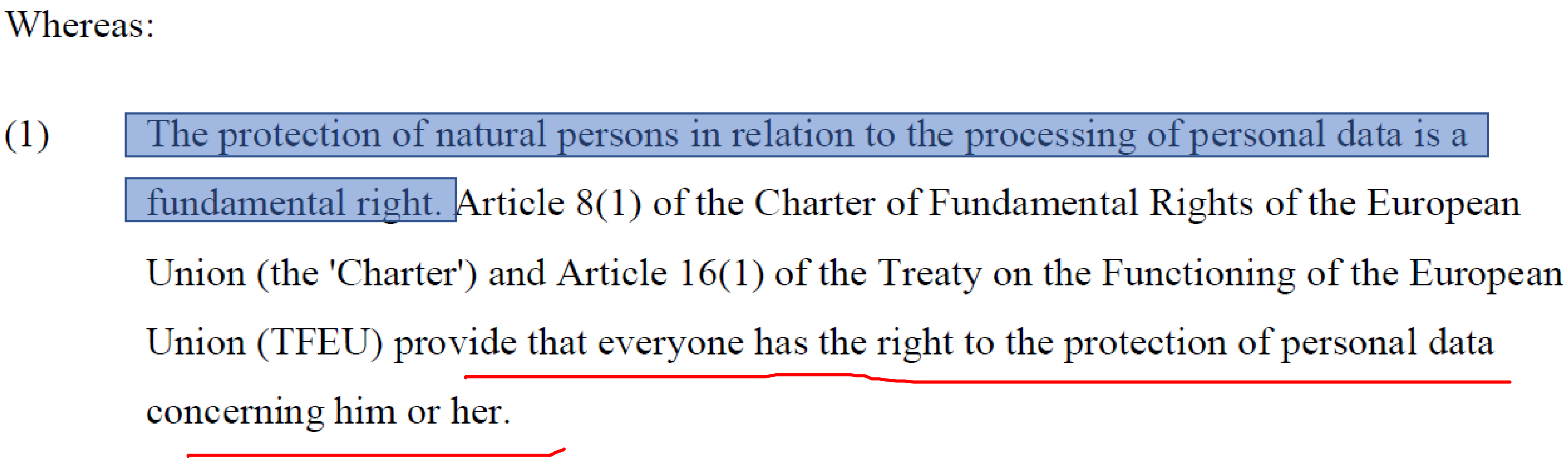
X - Atti delegati e atti di esecuzione

XI - Disposizioni finali

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725

Recitals - 1

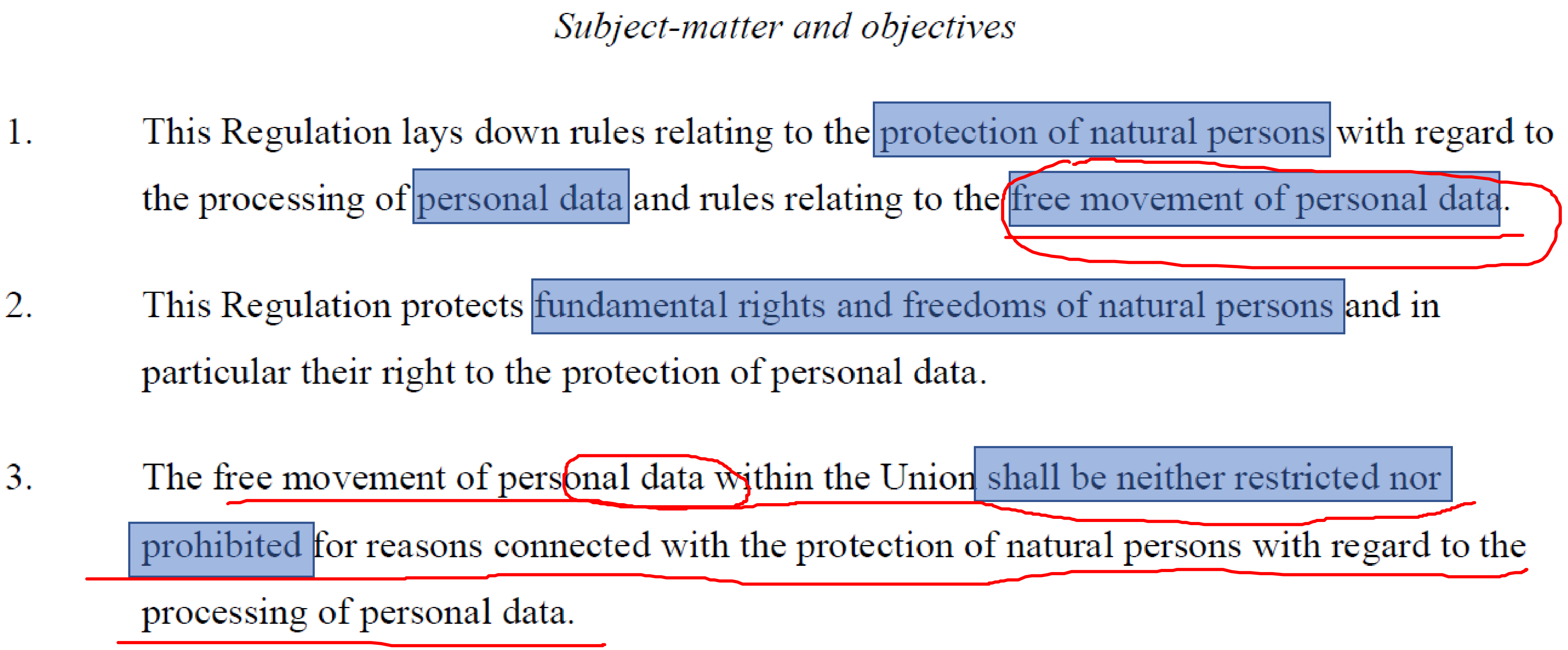
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4374552



Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

Article - 1



Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Scope (1)

- The regulation applies if the **data controller** (an organization that collects data from EU residents), or **processor** (an organization that processes data on behalf of a data controller – cloud provides), or the **data subject** (person) is based in the EU.

- The regulation also applies to organizations based outside the EU if they collect or process personal data of **individuals located inside the EU**.

- **Data Protection Officer (DPO)** employed in the organization, has responsibilities for advising on GDPR regulation

Scope (2)

- DPO appointment is **mandatory** for
  - Public bodies (excepts courts) and
  - Data controllers and data processors that, as a core activity, monitor individuals *systematically* and on a large scale, or that process *sensitive* data on large scale
- Appointment, position and tasks of DPO are set out in GDPR
  - Expert knowledge of *data protection law* and practice
  - Be involved in *all data protection issues*
  - Report directly to *highest* level of management
  - Operational independence, no conflicts of interest, confidentiality
  - Inform and advice; monitor compliance; point of contact for individuals

Personal Data

- Any information relating to an **individual**, whether it relates to his or her private, professional or public life.
- It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."
- The precise definitions of terms such as "personal data", "processing", "data subject", "controller" and "processor", are stated in Article 4 of the Regulation
- any data that are not personal data are outside the scope of the proposed Regulation.

Lawful basis for processing (1)

- **Unless** a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so. According to Article 6, the lawful purposes are:
  - If the data subject has **given consent** to the processing of his or her personal data
    - Consent by default is not valid anymore (EXPLICIT consent)
    - Can be removed and controller cannot refuse
  - To fulfill **contractual obligations** with a data subject;
  - To comply with a data controller's **legal obligations**;
  - To protect the **vital interests** of a data subject or another individual;
  - To perform a task in the **public interest** or in **official authority**;
  - For the **legitimate interests of a data controller** or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the **Charter of Fundamental Rights** (especially in the case of children – 16years old).

Lawful basis for processing (2)

- Public Task: you can process personal data, without consent, to carry out your official functions or a task in the **public interest** - and where you have a **legal basic** for the processing
- **Legitimate Interest**: you can process personal data, without consent, if you have a genuine and legitimate reason to do so
  - Legitimate interest can be for **commercial** benefit
  - GDPR recitals – direct marketing could be a legitimate interest
  - BUT exception if your interests are outweighed by harm to the individual's right and interest (balance it against the individual's interests, rights and freedoms)

Lawful basis for processing (3)

- Consent may be required if you are:
  - Marketing
  - Selling information
  - Transferring data outside EU/EEA
- Consent will NOT be appropriate:
  - Consent is a pre-condition of using the service
  - You would still process personal data using different basis even if consent was withdrawn
- GDPR sets a higher standard for obtaining consent

Lawful basis for processing (4)

- Consent – Practical changes
  - Identify basis of processing
  - Clear and plain language
  - Keep records
  - Drive Withdrawal
- Don't use informed consent… for example
  - Don't bundle consent
  - Blanket consent
  - Don't use pre-ticked boxes
  - Penalize withdrawal

Responsibility and accountability

- **Compliance** with the GDPR: the *data controller* must implement measures which meet the principles of **data protection by design and by default**.
- Data protection by design and by default (Article 25) require data protection measures to be designed for products and services.
  - i.e. pseudonymizing personal data, by the controller, as soon as possible (Recital 78).
  - responsibility of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller (Recital 74)
  - inform the user about collection
  - **data protection impact assessments** (DPIA, Article 35)
    - identify and minimize the data protection risks of a project

Data protection by design and by default

- (Article 25) requires **data protection to be designed into the development of business processes** for products and services (At the beginning, for the root → easy task for new process, but what about old process?)
- by default: **Privacy settings at a highest level**
- implement mechanisms to ensure that personal data is not processed **unless necessary** for each specific purpose (touch lesser is better)

- encryption and decryption operations must be carried out **locally**, not by remote service (because of keys) and data must remain in the power of the data owner if any privacy is to be achieved.
- outsourced data storage on remote clouds is practical and relatively safe if only the **data owner**, not the cloud service, holds the decryption keys.

Pseudonymization (1)

- as a process that is required when data is stored (as an alternative to the other option of complete data anonymization) to transform personal data in such a way that the resulting data **cannot be attributed** to a specific data subject without the use of additional information.
- Encryption: decryption key separately!!!
- Tokenization: replaces sensitive data with non-sensitive substitutes (but still possible to link to original owner)

- Nice to have: The definition of personal data lists a number of factors how a person can be identified, e.g. with reference to identification numbers. Here, a general reference to "any other unique identifier" could be added for ensuring comprehensive coverage.

Pseudonymization (2)

- data minimization is a requirement
  - with pseudonymization the regulation provide no guidance on how or what constitutes an effective data de-identification scheme, with a **grey area** on what would be considered as inadequate pseudonymization subject to Section 5 enforcement actions
- anonymization and pseudonymization are two distinct techniques
  - Recital 26 of the GDPR defines anonymized data as “data rendered anonymous in such a way that the data subject is not or **no longer identifiable**.”
  - By contrast to anonymization, Article 4(5) of the GDPR defines pseudonymization as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of **additional information**.”

Pseudonymization (3)

- The risk of re-identification:
  - The effectiveness (and legality) of both anonymization and pseudonymization hinge on their abilities to protect data subjects from re-identification.
  - In Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are "**reasonably** likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."
  - Whether pseudonymized data is "reasonably likely" to be re-identified is a question of fact that **depends on a number of factors** such as the technique used to pseudonymize the data, where the additional identifiable data is stored in relation to the de-identified data, and the likelihood that non-identifiable data elements may be used together to identify an individual.

Pseudonymization (4)

- ANONYMOUS
  - Not possible to identify the user in any way
  - Data can be used in aggregation

AND

- PSEUDO ANONYMOUS
  - Very difficult to identify
    - With current technology
    - With data from other sources
    - In a reasonable time
  - Not direct linked with user profile
  - --- nothing about incidental findings
  - --- nothing about the identification via cross data deduction
- NON ANONYMOUS
  - Identified and linked with user profile
  - Consent for any data types

Right of access

- More generally: data subject right (Article 15).
  - access their personal data and information about how this personal data is being processed
  - A data controller must provide, **upon request**, an overview of the categories of data that are being processed (Article 15-1b) as well as a copy of the actual data (Article 15-3).
  - Furthermore, the data controller has to inform the data subject on **details about the processing**, such as the *purposes* of the processing (Article 15-1a), with whom the data is shared (Article 15-1c), and *how* it acquired the data (Article 15-1g)
  - be able to **transfer** personal data from one electronic processing system to and into another → data portability and data interoperable
  - **review** the collected data

Art 1, 4

Right to erasure

- Was *right to be forgotten* → became *right of erasure*
- Records of processing activities must be maintained that include purposes of the processing, categories involved and envisaged time limits. The records must be made available to the **supervisory authority** on request (Article 30)

- Supervisory authorities cannot have their eyes on all controllers all the time, so it is crucial **to give data subjects strong rights** for their interactions with controllers.

Data breaches (1)

- the data controller is under a **legal obligation** to notify the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals.
- There is a maximum of **72 hours after becoming aware** of the data breach to make the report (Article 33). **Individuals** have to be notified if adverse impact is determined (Article 34). In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach (Article 33).
- However, the notice to data subjects **is not required** if the data controller has implemented appropriate technical and organizational protection measures that render **the personal data unintelligible** to any person who is not authorized to access it, such as encryption (Article 34).

Data breaches (2)

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data
- Example: Carphone Warehouse
  - Fined £400.000 in January
  - Records for approximately 3.350.000 customers of a number of mobile phone provider
  - Records for 389 customers across two other companies
  - Historical transaction for period March 2010-April 2010
  - Records of approximately 100 employees

Data breaches (3)

- Vulnerability is a weakness which allow an attacker to reduce a system's information assurance. Vulnerabilities are the intersection of the three elements:
  - a system susceptibility of flaw
  - attacker access to the flaw
  - attacker capability to exploit the flaw
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface
- Example: Carphone Warehouse – how did they get in?
  - Vulnerability?
  - Password

Data breaches (4)

- Example: Uber
  - Details of 2.7 million UK drivers and riders
  - Details of 57 million people worldwide
  - Email address and phone numbers
  - US Driver license numbers
- how did they get in?
  - Password stored on GitHub
  - What is GitHub?
  - Cover up!
  - ICO Response
    - «Uber has confirmed its data breach in October 2016 affected approximate 2.7 million user accounts in the UK. Uber has said the breach involved names, mobile phone numbers and email address. On its own this information is unlikely to pose direct threat to citizens, However, its use may make other scams, such as bogus emails or call appear more credible. People should continue to be vigilant and follow the advice from NCSC»

Data breaches (5)

- It’s not only loss of confidentiality or unauthorized processing of personal data
  - It also encompass availability and integrity
- only breaches “likely to affect” data subjects have to be notified to them, and not all breaches
- Nice to have: public register of breaches to educate the public about IT security and provide added insight into trends regarding breaches

Data breaches (6)

- Preventing
  - Vulnerability testing and Penetration testing
  - Password management
    - Risk assess
    - Two Factor Authentication
    - FIDO2 and biometrics
  - Utilized DLP (Data loss prevention) feature on key documents
    - help a network administrator to control what data end users can transfer
  - Data protection training
    - Employers
    - Users

Sanctions (1)

- a **warning** in writing in cases of first and non-intentional noncompliance
- **regular** periodic data protection **audits**
- a fine up to **€10 million or up to 2% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions: (Article 83, Paragraph 5 & 6)
- a fine up to **€20 million or up to 4% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions: (Article 83, Paragraph 4)

Sanctions (2)

- **Data protection Commissioner**
  - Investigative powers
    - Conduct *investigations* and audits
    - *Obtain access to data*, premises and equipment
  - Corrective powers
    - Issue warnings and reprimands
    - *Order* compliance
    - Order communication of a data breach to an individual
    - Impose a temporary/permanent ban on processing
    - Order rectification or erasure of personal data
    - Suspend data transfers to a third country
  - Administrative fines
    - May impose fine (effective, proportionate and dissuasive)

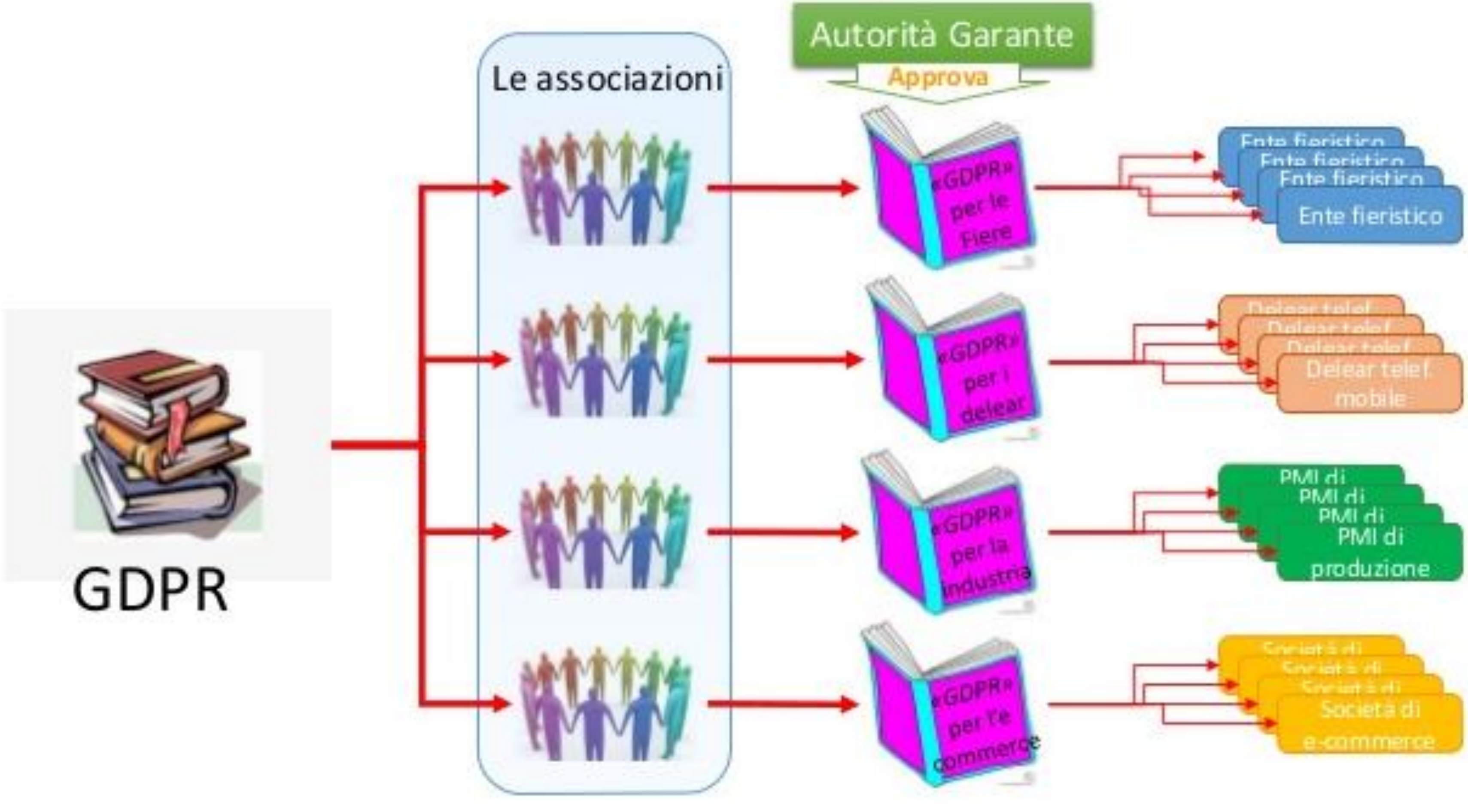
Codes of conduct and certification (section 5, article 40) (1)

- **The Member States, the supervisory authorities**, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the **proper application** of this Regulation, taking account of the specific features of the **various processing sectors** and the specific needs of micro, small and medium-sized enterprises.
  - Involvement authorities
  - Awareness of the problem
- **Associations and other bodies** representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to
  - The association that represent the firms

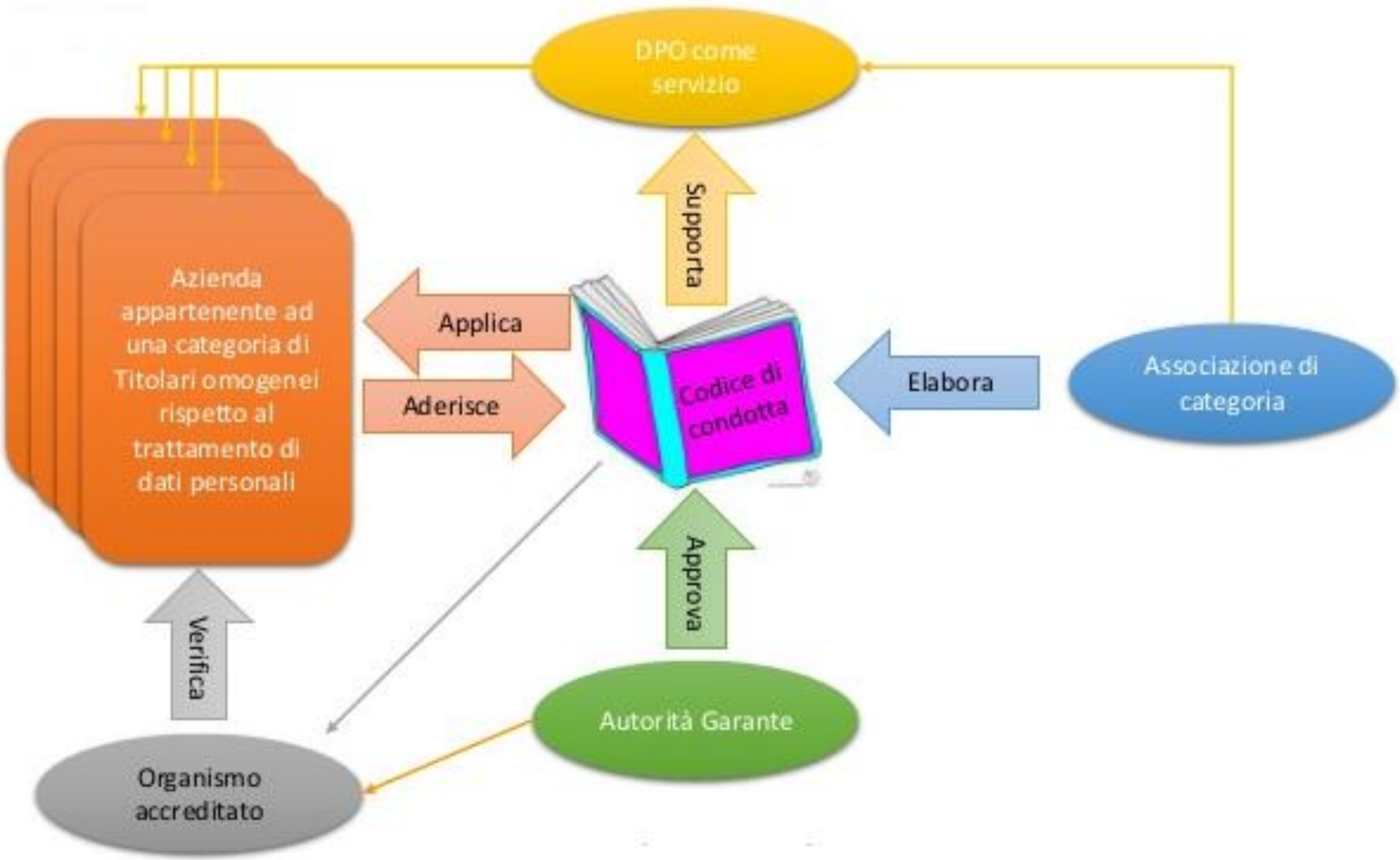
Codes of conduct and certification (section 5, article 40) (2)

- (a) fair and transparent processing;
- (b) the legitimate interests pursued by controllers in specific contexts;
- 5419/16 AV/NT/sr 175 DGD 2 **EN**
- (c) the collection of personal data;
- (d) the pseudonymisation of personal data;
- (e) the **information provided to the public** and to data subjects;
- (f) the exercise of the rights of data subjects;
- (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- (h) the measures and procedures referred to in Articles 24 and 25 and the measures to **ensure security** of processing referred to in Article 32;
- (i) **the notification of personal data breaches** to supervisory authorities and the communication of such personal data breaches to data subjects;
- (j) the transfer of personal data to third countries or international organisations; or
- (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

Codes of conduct and certification (section 5, article 40) (3)



Codes of conduct and certification (section 5, article 40) (4)


DPO come servizio
Supporta
Azienda appartenente ad una categoria di Titolari omogenei rispetto al trattamento di dati personali
Applica
Aderisce
Codice di condotta
Elabora
Associazione di categoria
Approva
Verifica
Autorità Garante
Organismo accreditato

Mapping GDPR to Required Capabilities

- GDPR compliance can be achieved only by applying a combination of controls that can summarized as People, Process, Products:
  - **People** → specific roles, responsibilities and accountability
  - **Processes** → operating principles and business practices
  - **Products** → technologies used for data storage and processing

- Specific set of controls for GDPR:
  - **Discover:** scope data subjects to the regulation
  - **Defend**: implement measure to protect discovered data
  - **Detect**: identify breach against data and remediate security and process gaps

Discover (1)

- *Before* implementing security controls, identify **which** personal data are stored and **how long** the organization is permitted to retain

1. Identification of *IMPACT* to Personal Data: integrate tools that enable controller to quickly and conveniently **review their data content** and to inspect **what additional** data will be captured as new services are under development (Article 35, clause 1)
2. *RETENTION* of Personal Data: capability to **identify personal data**, and **securely erase** once the expiration period has been reached, or an individual specifically requests erasure (Article 13, clause 2a)

- To erase means marking as DELETED
  - for police officer investigation (i.e. 30 days)

Discover (2)

- What ‘personal data’ do you hold and use?
- Why do you need it or use it? What’s the legal basis for processing it?
- How is it processed and shared? How long is it kept for?
- Where is stored and from where is it accessed?
- Identify and understand the data flows (data mapping, data inventory)

Defend (1)

- Implement the controls that will protect data (Article 32, clause 1)

1. *Access Control*: only authorized users can access personal data (Article 25, clause 2 + Article 29). It should be possible to enforce **authentication controls** so that only the clients (users, application, administrations) authorized by the data processor can access the data. The KB should also allow data controllers to define specific *roles, responsibilities and duties* each client can perform against data

Defend (2)

2. *Pseudonymization & Encryption*: in the event of a breach, the **pseudonymization** and **encryption** of data is designed to prevent the identification of any specific individual from compromised data (Clause 28). Pseudonymization via separation of user information from user data + access control. Encryption (Article 32, clause 1 + Article 34 clause 3a) for data *in-transit* using network connections and data *at-rest* using storage and backups
3. *Resilience and Disaster Recovery*: provide system and service + means to restore data in a **timely** fashion + **fault tolerance** to system failures (Article 32)

Defend (3)

4. *Data sovereignty: Data transfer outside of the EU*: To support globally distributed applications, organizations and increasing **distributing data to data centers and cloud facilities** located in multiple countries across the globe, it should be possible to enforce data sovereignty policies by only distributing and storing EU citizen data **to region recognized as complying** with the regulation

Detect

- In the event of a data breach, the organization must be able, in a **timely fashion**, to *detect and report* on the issue, and also to generate a record of what activities had been performed against the data

1. *Monitoring and reporting*: The closer to real-time, the better chance of limiting the impact. The KB should offers managements tools that enable constant monitoring of KB behaviour to proactively mitigate threads and that enable the organization to report any breaches (Article 33, clause 1)
2. *Auditing*: Record activities on KB and present that activities for forensic analysis when requested by controller (Article 25, clause 1 + Article 28, clause 3H)

TOP

GDPR verification

DPIA

- **data protection impact assessments**
- **Struttura DPIA:**
  - Executive Summary
  - Obiettivo del Documento e dell'Azione (scambio/accesso/uso dati)
    - Obiettivi, motivazioni
  - Definizioni
  - Contesto Normativo, Normative e Standard di riferimento
  - Perimetro di Applicazione
  - Ruoli e Responsabilità: Conduttore, DPO
  - Durata del trattamento e detenzione dei dati
  - …..vedi next slide….-→

- **Segue struttura (aspetti tecnici)**
    - Trattamento dati: Misure di Protezione
    - Trattamento dati relativi a Minori e/o categorie protette
    - Trattamento e Piattaforma dati: descrizione tecnologica
    - Dati Trattati: descrizione
    - Obiettivi perseguiti da chi usa i dati, resa per il fornitore dei dati
    - Modalità di trasmissione dati, da fornitore a utilizzatore
    - Modalità di Utilizzo dei dati
        - Chi accede e come, eventuali liste di accesso, concessioni autorizzazioni, etc.
    - Backup e Continuità del servizio (da ambo le parti, se necessario)
        - Su eventuali ritorni dalle elaborazioni, sui servizi correlati se richiesti dal fornitore, etc..
    - Sicurezza: PENtest, vulnerability, TLS, certification, DB encryption, …
    - Impatto e Rischi: perdita dei dati
    - Accesso e Proporzionalità
    - Firme: DPIA resp, DPO, DPIA reviewer

Definizioni

- **Probabilità** [P] valutazione della frequenza di accadimento di una minaccia, in funzione delle vulnerabilità in essere e di eventuali contromisure implementate;
- **Impatto** [I] indicazione della gravità di un incidente che comprometta la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa Privacy;
- **Minaccia** [M] evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'interessato;
- **Vulnerabilità** [V] debolezza intrinseca del sistema informativo o del sistema informatico che, qualora si realizzasse una minaccia che la sfrutti, produrrebbe un danno all'interessato;
- **Rischio Privacy**: combinazione di impatto per l'interessato e della probabilità di accadimento di una minaccia che possa compromettere la riservatezza, l'integrità o la disponibilità di un dato personale ad esso riferito;
- **Contromisure** [C] soluzioni organizzative, procedurali o tecnologiche che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;
- **Soglie di accettazione del rischio** definizione del livello massimo di rischio accettato superato il quale si rende necessaria l'implementazione delle contromisure;
- **Rischio Privacy Residuo**: valore determinato dalla combinazione tra il Rischio Privacy e la Vulnerabilità. Tale valore deve essere tenuto entro i limiti determinati dalle Soglie di accettazione del rischio.

Contesto Normativo

L' Art. 35 c. 7 del GDPR prevede che la valutazione contiene almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al par. 1;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Spetta al titolare garantire l’effettuazione della DPIA (art. 35, paragrafo 2). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all’organismo; tuttavia, la responsabilità ultima dell’adempimento ricade sul titolare del trattamento

TOP

GDPR verification

Checklist

- Legal bases for processing
- Policies and procedure
- Privacy notes
- Appropriate technical and organizational measure
- Documentation and record-keeping
- Staff training
- Dealing with Data Subject Rights
- Security and Data breach
- Data Protection Impact Assessments
- Data Processor and contracts
- Appoint a DPO if required, or at least, a lead person
- Privacy by design and by default

Main concepts

The six main principles

1. Lawfulness, fairness and transparency

2. Purpose limitation

3. Data minimisation

4. Accuracy

5. Storage limitation

6. Integrity and confidentiality

The seventh principles

- Controller–processor contracts;
- Relevant policies and procedures;
- Privacy notices;
- Staff training records;
- Security monitoring and event logging records;
- Data breach records; and
- Data protection impact assessments.

GDPR verfiication on Snap4City

GDPR Compliance Verification Feature	Verif.	Reqs.
Signed consent	UI	R8
User profile management and control	UI	R13
Data Type private as default	UI	R8
Rights to access per element	UI	R9
Rights to transfer per element	UI	R10
Rights to erase per element and total	UI	R13
Rights to revoke/change per Data Type	UI	R10
An interface for Right management for Data Type	UI	R9
Clear Terms of Use and Privacy Policy	UI	--
Auditing Tools for Data Type	UI	R14
Publish as Anonymous	UI	R9
Encrypt personal users’ data	Code	R12
Secure Authentication and Authorization	Code	R3
Data protection by Design	Code	R17
Secure connection	Code	R6
Security Control, data breach control, anonymization, etc.	PEN Test	R15, R16, R18