D2.1
System and dependency analysis (first iteration) - Cybersecurity requirements for local public administrations

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis

Principal author:	Thomas Schaberreiter, University of Vienna Contact: thomas.schaberreiter@univie.ac.at
Co-authors:	Chris Wills, Caris Research Veronika Kupfersberger, University of Vienna Alex Papanikolaou, InnoSec Municipality of Larissa Roma Capitale

Document version:	1.1

Table of Contents

Executive Summary

This deliverable of the CS-AWARE project is the first in an iterative series of three deliverables (D2.1 System and dependency analysis (first iteration) – Cybersecurity requirements for local public administrations, D2.2 System and dependency analysis (second iteration) - Pilot scenario definition and D2.3 System and dependency analysis (third iteration) – Pilot scenario specification and self-healing strategies) that will be delivered throughout the project run time. The first iteration focuses on an overview analysis of cybersecurity related aspects, relevant to CS-AWARE in the context of local public administrations (LPAs). The analysis is based on three thematic focus points: an initial threat assessment for LPAs, an analysis of external information sources that may be relevant to CS-AWARE (for both the system and dependency analysis phase and the monitoring and pattern recognition phase and an analysis of the piloting scenarios based on the first round of soft systems analysis workshops. The results of this deliverable are a substantial input for the CS-AWARE framework (D2.4 - CS-AWARE Framework) as well as the software development and integration of work packages WP3 and WP4.

In the initial threat assessment we have investigated threat assessment reports from relevant network and information security (NIS) authorities, law enforcement authorities and the security industry. We have discussed the most relevant threats and threat actors and identified those threats and threat actors that are relevant for LPAs. Based on this analysis we have created an initial risk assessment. We have identified that the most valued asset in LPAs is the potentially sensitive and/or private citizen and employee data that is managed by LPA systems, and that unauthorized data access, modification and destruction as well as data theft are the most relevant threats towards LPAs. We assess that LPAs are not a high valued target (like for example critical infrastructure or financial institutions are, due to the potentially high pay-off for a threat actor) and therefore assess the risk against LPA data as medium (on a high, medium and low scale). We assess that untargeted large-scale attacks with the goal of extortion, like Ransomware or Distributed Denial of Service (DDoS) attacks carry a higher risk for LPAs. We have identified the cyber-criminal (high) as well as the malicious insider (medium) as the most relevant threat actors. Furthermore, disgruntled citizens, script kiddies and hacktivists are also seen as relevant threat actors, but we assess the risk from those actors to be low due to low potential pay-off for those actors as well as the low expected damages for LPAs.

In the analysis of relevant information sources for CS-AWARE we identified potential information sources in following categories: NIS Competent Authorities, Law Enforcement Agencies, Cyber Intelligence Sources and Information Sharing Tools (both open source and commercial providers), Cybersecurity Intelligence Data Feeds, Malware Analysis, Vulnerability Data, Social Media and Cybersecurity visualizations. We have seen that there are many organizations, commercial providers and open source projects/communities that provide information related to cybersecurity that can potentially be utilized by CS-AWARE to assess the global cybersecurity situation. Some of the identified sources, especially in the categories of "NIS Competent Authorities" and "Law Enforcement Agencies" provide more static information in aggregated form, such as threat assessment reports. Such information can be utilized by CS-AWARE in the system and dependency analysis phase, in order to gain a better overview picture of the global cybersecurity situation and be able to map it to the concrete LPA context. Other information sources provide more dynamic information in structured or unstructured form, like feeds with information about the latest threats or vulnerabilities. Those sources can potentially be utilized by CS-AWARE in the monitoring and pattern recognition phase, to set specific events or security incidents in context with the events or incidents observed in LPA systems. In this deliverable we provide an extensive list of potential information sources, no concrete assessments of which information sources (especially the sources providing dynamic content) are the most relevant to CS-AWARE for data collection have been made.

In the pilot scenario analysis we present a high level overview of the relevant systems and dependencies that we identified in both piloting municipalities of Larissa in Greece and Roma Capitale (RC) in Italy. Our analysis is based on the first round of workshops that were conducted by the CS-AWARE analysts in both municipalities. In those workshops the method of rich pictures

drawn by the administrators of the systems (e.g. technical personal, management or subcontractors) was utilized in order to identify the most critical assets, dependencies and monitoring points present in the LPA systems. This method is part of the analysis according to the soft systems methodology (SSM) that was chosen for CS-AWARE. In CS-AWARE the analysis and identification of assets, dependencies and monitoring points of the existing and organically grown complex socio-technological systems found in all larger organizations - like LPAs - is an integral part of the proposed cybersecurity awareness solution. We argue that in complex systems good cybersecurity awareness can only be provided if the relevant relations between the mission critical aspects of the system are understood, and relevant case specific monitoring points can be utilized. The first round of analysis has only strengthened our argument. In both municipalities, we were able to achieve good analysis results and were able to identify the most mission critical systems and their dependencies, as well as potential monitoring points for CS-AWARE. While the individual set-ups and procedures in the two municipalities are significantly different from each other, especially due to the substantial difference in complexity in the operations of the two very differently sized municipalities, we were able to draw some generalized conclusions that will allow us to develop guidelines and procedures that will help to further simplify future analysis efforts in LPAs. In line with the initial risk assessment we have identified that the potentially sensitive and/or private data managed by LPAs is their most valuable asset. A cybersecurity awareness solution has to monitor the possible data flows in day-to-day operations. We have investigated potential monitoring points at 4 different levels that allow to identify suspicious behaviour related to data operations: The database level, the application/service level, the network level and the security appliance level. On the database level and the application/service level built-in logging and auditing mechanisms can be utilized to monitor relevant data operations, since most modern database systems and applications/services provide good logging and/or auditing capabilities. On the network level, most modern networking products have built-in logging and sometimes even analysis capabilities for monitoring relevant network traffic. Security appliances, like for example firewalls, intrusion detection systems (IDS) or Security Information and Event Management (SIEM) systems are another class of software or hardware based system that can provide relevant information specifically related to security through built-in logging features.
In the second iteration of this deliverable (D2.2 System and dependency analysis (second iteration) - Pilot scenario definition), due in M16, we will focus on substantiating the initial overview analysis and identify 1) those information sources that are most relevant to CS-AWARE and which will be interfaced with CS-AWARE and 2) the concrete piloting scenarios and monitoring points in the municipalities CS-AWARE will interface with. This will allow the project to define the concrete pilot scenarios in preparation for the deployment of the CS-AWARE solution.

1 Introduction

Deliverable *D2.1 System and dependency analysis (first iteration) – Cybersecurity requirements for local public administrations* provides an analysis of cybersecurity requirements in the context of LPAs based on three angles: An initial threat assessment, an analysis of relevant information sources that can be utilized by CS-AWARE as well as an initial analysis of the piloting scenarios in the two piloting municipalities of Larissa and Roma Capitale. Chapter 2 details our initial threat assessment, based on an analysis of relevant threat assessment reports in Section 2.1, leading to our initial threat assessment for local public administrations in Section 2.2. Chapter 3 presents our analysis of information sources relevant to CS-AWARE. Relevant information sources are grouped into NIS Competent Authorities (Section 3.1), Law Enforcement Agencies (Section 3.2), Cyber Intelligence Sources and Information Sharing Tools (Section 3.3) which also includes Commercial Data Providers (Section 3.3.1), Cybersecurity Intelligence Data Feeds (Section 3.4), Malware Analysis (Section 3.5), Vulnerability Data (Section 3.6), Social Media (Section 3.7) with a closer look at potential data from the two social networks Twitter and Reddit (Section 3.7.1), Cybersecurity Visualizations (Section 3.8) and Other Information Sources (Section 3.9). In the analysis of pilot scenarios in Chapter 4 we detail the results of the soft systems workshops conducted so far in the Municipality of Larissa (Section 4.1) and RC (Section 4.2 and Section 4.3) before we conclude our analysis with a discussion of the generalized experiences we gained regarding cybersecurity focused soft systems analysis for LPAs based on the analysis conducted so far (Section 4.4). Annex 1 of this deliverable contains a standardized letter that can be used to ask commercial data providers for access to their data feeds for research purposes in the context of the CS-AWARE project. Annex 2 contains the rich pictures together with detailed descriptions, produced during the one week workshop in the Municipality of Larissa. Annex 3 contains the presentation slides and rich pictures produced during the first one week workshop in RC, and Annex 4 contains the presentation slides and rich pictures with detailed descriptions produced during the second one week workshop in RC.

2 Initial Threat Assessment

In this Chapter we would like to introduce an initial cyber threat assessment for local public administrations, based on general threat assessment reports. We base our assessment on the threat assessment perspectives of NIS competent authorities (ENISA threat Landscape Report 2016 (ENISA, 2016)), law enforcement (The Europol Internet Organized Crime Threat Assessment (IOCTA) report of 2017 (Europol, 2017)) as well as one example for a threat assessment from a commercial security provider (McAfee Labs threats report of June 2017 (McAfee, 2017)).

2.1 Analysis of relevant threat assessment reports

The ENISA threat landscape report 2016, by the time of writing the latest edition, states that the main trend for attackers in 2016 was in gaining efficiency and optimizations in their attacks and the main goal was monetization (mainly through extortion). Profit oriented attacks will be the main trend for the years to come. Attackers are successful in abusing unsecured and Internet facing IT components (especially IoT devices), generating profit through extortion money against commercial organizations, and operating large and resilient malicious infrastructures to launch attacks. As can be seen in Figure 1, the ENISA report lists following relevant cyber threats, in order of relevance:

1. **Malware:** Malicious software installed on a victims device (e.g. via click bait mail or social engineering). Used predominantly for ransomware attacks and information stealing in 2016.
2. **Web-based attacks:** Use web component (web server, browser, extensions, ...) as attack surface. For examples, vulnerabilities in those components can be exploited to breach the network or as a malware installation vector.

3. **Web application attacks:** Similar to web-based attacks against web components, but here the target are vulnerabilities in the applications that run on top of the infrastructure. In 2016 there has been a significant increase in attacks against web applications and they are now considered as the biggest threat to organizational security. This threat is facilitated by the large amount of web application vulnerabilities.
4. **Denial of Service (DoS):** Causing systems to overload or malfunction through continuing cyber-attacks, predominantly to extort money from the owner.
5. **Botnets:** An army of infected hosts (usually through malware attacks) carrying out large scale attacks like DoS.
6. **Phishing:** Try to extort money from victims by engaging them in conversation, usually by "phishing" for an answer through a general spam based mail. CEO fraud, where the conversation seems to be originating from the CEO of a company - asking for help in moving money around - has been the latest very effective phishing technique.
7. **Spam:** Spam mail is still one of the main delivery techniques for malware for infecting computers and malicious URLs and exploiting web service vulnerabilities. Spam itself is usually sent by infected hosts in large spam botnets.
8. **Ransomware:** Ransomware is a growing threat, and one of the main sources of revenue for criminals. It is used to encrypt the hard drive of victim's computers with an ultimate goal to ask for ransom in order to decrypt the content again.
9. **Insider threat:** The malicious insider is still one of the main threats for cybersecurity within organizations. Data theft and espionage are probably the main motivations for a malicious insider.
10. **Physical manipulation, damage, theft and loss:** The physical loss and theft of devices can lead to severe data breaches. - not an attack carried out via cyberspace,
11. **Exploit kits:** Exploiting vulnerabilities on victim's devices to gain device access and potentially install malware.
12. **Data breaches:** Disclosing private or confidential data from organizations or individuals.
13. **Identity theft:** A special case of data breach with the objective to compromise identity information to be used for malicious purposes.
14. **Information leakage:** Gather information about systems or applications, in order to conduct more targeted attacks.
15. **Cyber espionage:** Intelligence gathering via cyber space (either state sponsored or industrial).

The report identifies the following main threat agents that have a motivation to carry out cyber-attacks: Cyber criminals, Insiders, Nation states, Corporations, Hacktivists, Cyber fighters, Cyber terrorists and Script kiddies (low-skilled individuals that use attack tools developed by others, predominantly out of anger or for self-affirmation).
In the context of local public administrations (LPAs), we suggest that the threat agents with the highest motivation to attack LPAs are **cyber criminals** (for monetary gain), **Insiders** (disgruntled or for monetary gain), **Hacktivists** (may have a problem with a policy decision), and **script kiddies** (which could be a bored teenager as well as the disgruntled citizen).
Figure 1, taken from (ENISA, 2016) illustrates which type of threat agent would use which attack. The threats that the identified LPA threat agents would use have been outlined in red, which reveals to us that:

- Malware, Physical manipulation/damage/theft/loss, data breaches and Identity theft would be used by **4 relevant threat agents**
- Web-based attacks, web application attacks, DoS, Botnets, Phishing, Spam, Ransomware and Information leakage would be used by **3 relevant threat agents**
- Spam would be used by **2 relevant threat agents**

- Insider threat, Exploit kits and Cyber espionage would be used by **1 relevant threat agent**

From the listed threats, the following ones have been listed as primary group for at least one LPA relevant threat actor: Malware (3x), Ransomware (2x), Physical manipulation/damage/theft/loss (2x), Web application attacks (1x), Botnets (1x), Phishing (1x), Spam (1x), Data breach (1x), Identity theft (1x), Information leakage (1x) and Cyber espionage (1x).

	THREAT AGENTS							
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓	✓	✓	
Spam	✓	✓	✓	✓				
Ransomware	✓	✓	✓	✓		✓		✓
Insider threat	✓		✓	✓		✓	✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓		✓	✓
Exploit kits	✓		✓	✓		✓		
Data breaches	✓	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓		✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓		✓		

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Figure 1: ENISA threat landscape applied to LPAs

The Europol IOCTA report analyses the threats according to their three main priorities: child sexual exploitation, cyber-dependent crime and payment fraud. We will focus on the cyber-dependent crime

for our analysis. The report states that 2017 has seen attacks on an unprecedented scale. Extortion has been one of the main priorities for the EU law enforcement, with ransomware and distributed denial of service (DDoS) attacks being the most effective attacks in this area. Ransomware, which was already gaining popularity in 2016, has surpassed most other cybercrime threats on a global scale. The most popular malware delivery methods have been spam botnets (sending e.g. click bait mail) and social engineering attacks. Exploit kits have lost popularity for malware delivery purposes. Another key finding of the 2017 IOCTA report was that inadequate IT security for Internet facing devices will continue to result in sensitive data breaches.

The McAfee Labs Threat Report of June 2017 lists, amongst other analysis, threat statistics about cybersecurity relevant aspects on a quarterly basis. From those statistics we can learn that the top targeted sectors for cyber-attacks (based on the number of publicly disclosed incidents) have been the public sector, single individuals, health care, education and online services. Most of those incidents have been observed in the Americas, followed (after a large gap) by Europe and Asia. The top attack vectors for those incidents have been, including a large number of unknown attack vectors, Account Hijacking, DDoS, Targeted attacks, SQL injection, malware, defacement, leak, W-2 scam (a specific phishing attack) and vulnerabilities. From those statistics one can see that while the total number of malware has been steadily rising over the last years, the number of newly discovered malware has been declining in 2016, but is on the rise again in 2017. The same goes for ransomware: the number of total ransomware is steadily increasing, and after a sudden drop in Q4 2017, the number of newly discovered ransomware is raising again in Q1 2017.

2.2 Initial Threat assessment for local public administrations

In this Section we will discuss our initial risk assessment for local public administrations, based on the general threat assessment reports, as well as our initial analysis of the piloting municipalities in Larissa and Rome. We will roughly classify the identified risks in three levels: **low, medium** and **high**. We investigate risks from the angles of relevant threats, relevant threat actors and their motivation.

We have determined that the main asset to be threatened from the cyber domain for local public administrations will most likely be the data that is managed by the administrations, including personal citizen and employee data. The main cybersecurity challenge in local public administrations is assumed to be the prevention of unauthorized data access, modification and destruction of those data. We assess that local public administrations are not a high valued target for potential threat actors, as for example critical infrastructures (potential large-scale disruption of economy) or financial institutions (potential high financial gain) are. However, there is a certain level of risk associated, since there are relevant threat actors that may have a vested interest in gaining unauthorized access to data managed in LPAs. We assume a low to medium level of risk against LPA managed data from the cyber domain.

Our assessment of the relevant threat actors is, as already stated in the above analysis, largely in line with the threat actors that are also relevant to other sectors. The cybercriminal is one of the most relevant threat actors. However, we don't see a large risk of advanced persistent threat attacks since the effort required for those types of attacks may not justify the expected payoff. We see the highest risk from the cybercriminal threat actor to come from large-scale untargeted attacks - like ransomware or DDoS attacks - that may cause service disruptions and/or financial loss for the LPAs. As the second main threat actor in LPAs we classify the malicious insider that would use his knowledge of internal set-ups and procedures, and potentially legitimate access to services and data, to gain a personal advantage, for example by stealing data or extracting knowledge from data that could be sold to interested parties (e.g. data about public bids). The third relevant threat actor may be the disgruntled citizen (e.g. activist or script kiddie). The main motivation of this threat actor will be to disrupt services and operation in LPAs, for example by launching DDoS attacks against LPA systems. While it is less likely that a disgruntled citizen would steal data for financial gain, the malicious alteration

or destruction of data may be a worthwhile goal for the more advanced and maliciously motivated citizen.
We estimate that the most likely motivation of a threat actor to attack an LPA will be extortion and data theft, both will be mainly motivated by financial gain. The most likely extortion attacks will not be targeted attacks against specific LPAs, but large-scale attacks that target common systems or interfaces. The two most notable attacks in this area are ransomware attacks and DDoS attacks. Ransomware attacks usually utilize vulnerabilities in well-known operating systems and services, while DDoS attacks are usually launched against the network infrastructure of a service/organization. The attacker asks for money to stop the attack or restore the system to an operational state. Both attacks can be highly automated and are not specific to LPA systems. The second class of relevant threat is data theft, either for financial gain of the attacker or for shaming the attacked organization for bad security practices. The IOCTA report states in the Section about data breaches and network attacks, that in general, unlawfully acquired data is equally split into financial data and other data (such as intellectual property or personal data), which makes this threat very applicable to LPAs. The main threat actors are the malicious insider selling this data for profit and the cybercriminal that either wants to sell the data for profit or wants to extort money from LPAs for not disclosing the data.
Some threats that do not necessarily threaten the main asset of LPAs (the managed data), but may be the main motivation for some threat actors, are attacks that are aimed at hurting the reputation of an LPA (like web page defacement or denial of service). While those threats are not negligible because potentially highly skilled and motivated threat actors may be behind such attacks, the expected impact of such attacks does not threaten the operation of LPA systems. One notable exception would be if motivated threat actors, like hacktivists, are determined to steal and expose the data managed in LPAs. Due to the nature of the data managed in LPAs, usually citizen/employee data that is private but not highly sensitive[1], this is not seen as a high risk.
Another notable threat against LPAs are malware infections on client machines that make those clients, for example, part of command and control infrastructure of bot nets. While this is a serious threat associated with potentially significant costs (e.g. energy, bandwidth), it does not threaten the main asset of LPAs - the managed data - and is therefore seen as a low to medium risk.

A summary of risks grouped by threat and threat actor, based on initial threat assessment, can be seen in Table 1 and Table 2, respectively.

Table 1: LPA risks grouped by threat

Threat	**Risk level**		
	High	**Medium**	**Low**
Unauthorized data access, modification, destruction		X	
Data theft		X	
Extortion	X		
Advanced Persistent Threat (APT)			X
Ransomware (untargeted)	X		
Ransomware (LPA specific)			X

[1] While data in LPAs can be classified highly sensitive (e.g. religious beliefs), as confirmed by our LPA partners, we still assume this data to be a low to medium valued target.

Distributed Denial of Service - DDoS (untargeted)	X		
Distributed Denial of Service - DDoS (LPA specific)			X
Web page defacement / shaming			X
Malware infection		X	

Table 2: LPA risks grouped by threat actor

Threat actor	**Risk level**		
	High	**Medium**	**Low**
Cyber criminal		X	
Malicious insider	X		
Disgruntled citizen / script kiddie			X
Hacktivist			X

3 Analysis of External Information Sources

In this Chapter we will discuss the initial analysis of different cybersecurity relevant information sources that may be utilized by CS-AWARE in order to better understand the global threat landscape, gather information about possible vulnerabilities and attacks and help to better assess the risks associated to those factors in the LPA context. In general, those information sources may provide "static" information (e.g. in the form of reports) that will help CS-AWARE to build and continuously update its cybersecurity understanding, in a manual or semi-automatic manner. The sources could also provide "dynamic" content related to e.g. ongoing attacks or newly discovered vulnerabilities that will help CS-AWARE to automatically draw conclusions about the risk associated to the specific LPA context.

Our analysis has concluded that the most valuable cybersecurity related information (or cybersecurity intelligence) for CS-AWARE can be found from both official organizations, for example **NIS competent authorities** or **law enforcement organizations**, as well as private efforts, for example **for-profit companies** or **non-profit communities/ projects**. More generalized data, not necessarily provided by the security community, can be found from **social media** or **data visualization** focused data sources. For CS-AWARE we will focus on information that is freely available from either the NIS competent authorities, from companies that provide free data or, probably most relevant, open source intelligence (OSINT) focused communities and projects. However, we will keep the option in mind to ask for-profit companies for access to their cybersecurity intelligence data in the context of this European project, if relevant. A draft contact letter for commercial providers can be found in **Annex 1**.

It should be noted that the analysis provided in this Chapter is a thorough analysis of potential information sources for CS-AWARE (though we do not claim completeness). We do not have the intention to collect information from all of them. In the next step of the project we will identify the most relevant sources that will be interfaced by the CS-AWARE solution.

3.1 NIS Competent Authorities

In this Section we describe possible information sources related to organizations that the European Cybersecurity Strategy (European Commission and High Representative of the European Union, 2013) classifies as one pillar of coordination and information sharing efforts. The pillar, titled "Network and information security" includes organizations like the ENISA, the European Public Private Partnership for Resilience (EP3R) and other national and EU level competent/NIS competent authorities. Furthermore, Computer Emergency Response Teams (CERTs) and the similarly organized Computer Security Incident Response Teams (CSIRTs), are maybe the most relevant information sources for the CS-AWARE project that are classified in this pillar. In this Section we will describe organizations relevant to the CS-AWARE project, and we have conveniently titled them "NIS competent authorities". Besides the European organizations, we have picked several national organizations that we deem relevant for CS-AWARE. Furthermore, we have decided to only list public organizations as NIS competent authorities, private and for-profit organizations or independent non-profit organizations that offer similar services are listed in other categories.

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe[2]. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. ENISA is actively contributing to a high level of network and information security (NIS) within the Union, since it was set up in 2004, to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market.

The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

ENISAs approach includes the following areas:

- Recommendations
- Activities that support policy making and implementation
- 'Hands On' work, where ENISA collaborates directly with operational teams throughout the EU

For CS-AWARE, we are expecting high level policy documents and recommendations to be the main source of information that helps to shape the CS-AWARE solution. No dynamic information sources that can be utilized by CS-AWARE have been identified.

ENISA - European Union Agency for Network and Information Security **P.O. Box 1309,** **710 01 Heraklion, Crete, Greece** **Phone: +30 28 14 40 9710**	**ENISA Athens office** **1 Vasilissis Sofias Str** **Maroussi 151 24** **Attiki, Greece** **Phone: +30 28 14 40 9711**
Email: via contact form https://www.enisa.europa.eu/about-enisa/contact/info **Web: https://www.enisa.europa.eu**	

CERT-EU: In recent years, CERTs have been developed in both private and public sectors, as small teams of cyber-experts connected to the internet that can effectively and efficiently respond to

[2] https://www.enisa.europa.eu/about-enisa

information security incidents and cyber threats, often on a 24 hours a day-7days a week basis. After a pilot phase of one year and a successful assessment by its constituency and its peers, the EU Institutions have decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies on September 11th 2012. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies[3].
On their web page, CERT-EU provides dynamically updating information streams about:

- Product vulnerabilities
- Vulnerabilities
- Threats and Incidents
- Hacking/Techniques

Those information may be relevant to be observed by the CS-AWARE solution. At least some of those streams are provided in RSS format.

Email: cert-eu@ec.europa.eu
Web: https://cert.europa.eu

European Public-private Partnership for Resilience (EP3R): ENISA is currently involved in a key initiative to build closer partnerships between the public and the private sectors[4]. An initial survey of critical information infrastructure protection (CIIP) in Europe revealed that the critical information infrastructures (CII) sector was fragmented both geographically and due to the competition among telecom operators. Increasing the Resilience of those CIIs was generally seen as fundamental within Member States and several National Public-Private Partnerships (PPPs) were already established to enhance preparedness and response to disasters or failures by coordinating the efforts among telecom operators. Cross-border mechanism were set up on an ad hoc basis and soon a need for global approach at a European level arose to respond to both existing and emerging threats.
In March 2009, the European Commission adopted a policy initiative - COM (2009)149 - on Critical Information Infrastructure Protection (CIIP) to address this challenge and a European Public-private Partnership for Resilience (EP3R) was established in order to support such coordination. The objectives of EP3R are fourfold:

- Encourage information sharing and stock-taking of good policy and industrial practices to foster common understanding;
- Discuss public policy priorities, objectives and measures;
- Baseline requirements for the security and resilience in Europe;
- Identify and promote the adoption of good baseline practices for security and resilience.
- EP3R will build upon national PPPs and engage both the public and private sectors in addressing the pan-European dimension of the resilience of critical EU-wide infrastructure. The European Commission requested ENISA to support the EP3R process.

While the EP3R is, like the NIS directive, currently only targeted at critical infrastructures, a direct engagement with the EP3R in the context of LPAs may not be appropriate. However, CS-AWARE may monitor the PP3R progress and try to align interests with this initiative where appropriate.
No dynamically observable information sources in the context of EP3R have been identified to be used by the CS-AWARE solution.

[3] https://cert.europa.eu/cert/plainedition/en/cert_about.html
[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

Contact: N.A. (Probably best to establish contact via ENISA)
Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

List of national CSIRTs by CERT-CC (USA): A list of all national computer security incident response teams (CSIRTs) and computer emergency response teams (CERTs) maintained by the CERT Division of the Software Engineering Institute (SEI) of Carnegie Mellon University[5].
NOTE: This list can be downloaded in .json format for potential further automatic processing. The list includes usually the name, country and contact email. Sample entry for NCSC-FI:

{"longName":"National Cyber Security Centre Finland",
"website":{"description":"Public Website",
"url":"https://www.ncsc.fi"},
"emailAddress":{"description":"cert@ficora.fi",
"address":"cert@ficora.fi"},
"countryCode":"fi",
"shortName":"NCSC-FI",
"country":"Finland"}

No other relevant information streams could be identified from CERT-CC.

CERT Program
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
U.S.A.
Email: info@sei.cmu.edu
Phone: +1 412-268-5800
Web: http://www.cert.org/incident-management/national-csirts/national-csirts.cfm

National cybersecurity center of Finland (NCSC-FI) and CERT-FI: The NCSC-FI is a national information security authority. It develops and monitors the operational reliability and security of communications networks and services. Its CERT duties consist of preventing, detecting and resolving security breaches, as well as of informing of information security threats. The Centre's operations aim at ensuring that public communications networks and communications services are safe and interference-free, as well as securing critical societal functions[6].
NCSC-FI publishes dynamically updating information relating to the following aspects:

- **Information security now!**[7]: Blog style articles about security topics especially relevant to Finnish society and economy.
- **Alerts**[8]: Time-dependent alerts of currently ongoing security incidents and attacks
- **Vulnerabilities**[9]: Very detailed analysis of found vulnerabilities, in general extremely relevant to CS-AWARE.

While those publications are of course geared towards Finnish society and Economy, the global nature of cyberspace makes much of the provided information very relevant to CS-AWARE - especially Alerts and Vulnerability information.

[5] https://www.cert.org/about/
[6] https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices.html
[7] https://www.viestintavirasto.fi/en/cybersecurity/informationsecuritynow.html
[8] https://www.viestintavirasto.fi/en/cybersecurity/alerts.html
[9] https://www.viestintavirasto.fi/en/cybersecurity/vulnerabilities.html

No stream (like RSS) could be identified, but CERT-FI could be contacted if they provide easy access to this information.

The Finnish Communications Regulatory Authority (FICORA)
The National Cyber Security Centre Finland (NCSC-FI)
Itämerenkatu 3 A
P.O. Box 313
FI-00180 HELSINKI
Email:
CERT: cert (at) ficora (dot) fi
Vulnerability coordination: vulncoord (at) ficora (dot) fi
Web: https://www.viestintavirasto.fi/en/cybersecurity.html

CERT Luxembourg/CIRCL Luxembourg: CERT.LU and CIRCL provide the threat sharing platform MISP (Malware Information Sharing Platform)[10]. MISP acts as a platform for sharing threat indicators within private and public sectors. Malware Information Sharing Platform (MISP) allows organizations to share information about malware and their indicators. MISP users benefit from the collaborative knowledge about existing malware or threats. The aim of this trusted platform is to help improving the countermeasures used against targeted attacks and set up preventive actions and detection.
The objective of the CIRCL Malware Information Sharing Platform is to:

- Facilitate the storage of technical and non-technical information about seen malware and attacks
- Create automatically relations between malware and their attributes
- Store data in a structured format (allowing automated use of the database to feed detection systems or forensic tools)
- Generate rules for Network Intrusion Detection System (NIDS) that can be imported on IDS systems (e.g. IP addresses, domain names, hashes of malicious files, pattern in memory)
- Share malware and threat attributes with other parties and trust-groups
- Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works)
- Create a platform of trust - trusted information from trusted partners
- Store locally all information from other instances (ensuring confidentiality on queries)

There is extensive documentation about MISP available at[11]. Information can be accessed via an API. When you connect to the MISP platform, there is a specific menu dedicated to automation and export. CIRCL developed a Python library to access MISP API called PyMISP. The API can be used to feed internal security devices (e.g. IDS, SIEM or alike) in order to improve detection. The PyMISP python library documentation is available.
While the MISP platform development is an open source effort (and will be described separately in a Section further below), access to the information provided by the MISP instance operated by CERT.LU and CIRCL is not public. An organization or an activity based in Luxembourg or an accredited CERT or a trusted security vendor/researcher, can request access to MISP by contacting CIRCL. A feed containing OSINT information can be found at[12].

CIRCL:	**CERT.LU**

[10] https://www.circl.lu/services/misp-malware-information-sharing-platform/
[11] https://www.circl.lu/doc/misp/
[12] https://www.circl.lu/doc/misp/feed-osint/

CIRCL - Computer Incident Response Center Luxembourg **c/o "security made in Lëtzebuerg" (SMILE) g.i.e.** **16, bd d'Avranches** **L-1160 Luxembourg** **Grand-Duchy of Luxembourg** **Email: info@circl.lu** **Web: https://www.cert.lu/**	**CERT.LU c/o SMILE g.i.e.** **41 ave de la gare, L-1611 Luxembourg (Luxembourg)** **Phone: (+352) 274 00 98 601** **Email:info@cert.lu** **Web: https://www.circl.lu**

TF-CSIRT by Géant: TF-CSIRT provides support for the CSIRT community. It provides services like TRANSIT (training for CSIRT personnel), Trusted Introducer (being a trusted third party to introduce those who need to be introduced in the security context) or TF-CSIRT, a task force to promote collaboration and coordination between CSIRTs.
While TF-CSIRT does not provide an information that could be collected by CS-AWARE, the services of TF-CSIRT may be valuable to promote or project in the CSIRT community. Relevant meetings and events are organized that CS-AWARE could take part in later in the project.
Individuals can subscribe to the TF-CSIRT mailing list (https://tf-csirt.org/contacts/)
Above services are coordinated by Géant, a company providing a network for scientific excellence, research, education and innovation.

Amsterdam office **Singel 468 D, 1017 AW, Amsterdam.** **The Netherlands** **Phone: +31(0)20 5304488**	**Cambridge office** **City House, 126-130 Hills Rd, Cambridge** **CB2 1PQ. United Kingdom** **Phone: +44 (0)1223 371 300**
Email: info@geant.org **Web: https://tf-csirt.org/**	

Framework Nazionale per la Cyber Security (Italy): The Cyber Security Report 2015, realized by CIS-Sapienza[13] and by the Cyber Security National Laboratory of the National Interuniversity Consortium for Informatics[14] is included the National Cyber Security Framework. The Framework is based on the NIST Framework for Improving Critical Infrastructure Cybersecurity[15] and is the result of a Public-Private-Partnership. The framework outlines procedures to be adopted and implemented by medium, small or micro businesses (The NIST framework is also taken into account when designing the CS-AWARE framework).
It is not an information source that would provide dynamic content to be harvested by CS-AWARE.

Web: http://www.cybersecurityframework.it/

CERT-PA (Italy): The CERT-PA works within the Agenzia per l'Italia Digitale (AGID) on issues regarding security incidents in the public administration. A news feed with the newest cybersecurity information (e.g. attacks, vulnerabilities) is provided.

[13] http://www.cis.uniroma1.it/en
[14] https://www.consorzio-cini.it/lab-cyber-security
[15] http://www.nist.gov/cyberframework/

Email: cert-pa@cert-pa.it
Web: https://www.cert-pa.it/web/guest/home

CERT nazionale Italia: Part of the Ministry for Economic Development (Sviluppo Economico). Italy's Intelligence System for the Security of the Republic is the collective name given to the authorities and organizations responsible for intelligence policies, intelligence coordination and intelligence operations. The Security Intelligence System includes:

- the President of the Council of Ministers
- the Delegated Authority
- the CISR – Comitato Interministeriale per la Sicurezza della Repubblica (Interministerial Committee for the Security of the Republic)
- the DIS – Dipartimento Informazioni per la Sicurezza (Security Intelligence Department)
- the AISE – Agenzia informazioni e sicurezza esterna (External Intelligence and Security Agency)
- the AISI – Agenzia informazioni e sicurezza interna (Internal Intelligence and Security Agency)

The agency is responsible for the strategic cybersecurity development in Italy (legal framework, cybersecurity strategy, cybersecurity framework). No dynamic content to be harvested by CS-AWARE is provided.

Email: cert@mise.gov.it
Web: https://www.certnazionale.it/

University organized National Cyber Security Laboratory (Italy): The mission of the National laboratory of Cyber Security is to coordinate national cybersecurity related activities and to promote on a national and international level activities

- to help the country deal better with cyber threats
- improve the service continuity of the critical systems
- increase the social awareness
- improve the protection against cyber-attacks directed at the public administration and companies
- and support standardization, definition of processes and methodological national frameworks

Research areas of interest include[16]:

- Enterprise and software Security
- Critical Infrastructure Protection
- Biometrics
- Secure computation
- Protection of cyber-physical and smart complex systems
- Physical-Layer Security
- System and Network security
- Security, privacy and dependability in the cloud
- Risk Analysis
- Privacy for social networks and Big Data
- Machine learning for cyber security
- Holistic approaches for assessment of Dependability and security
- Digital Identity

[16] https://www.consorzio-cini.it/index.php/en/labcs-home/labcs-areas-of-research

- Electronic Voting
- WEB security

Among the various research projects, following projects that may be interesting to CS-AWARE could be identified:

- Trusted Computing for European Embedded Systems TOISE Milan European Project
- Assessing the economic impacts of Terrorist Threats or Attacks following the closing down of public transport systems ATTACS Roma "La Sapienza" European Project

Via Ariosto 25, 00185, Roma, Italy
Email:
Director: Prof. Roberto Baldoni Roma "La Sapienza" **direttore.cybersecurity@consorzio-cini.it**
Dott.ssa Gabriella Caramagno **segreteria.cybersecurity@consorzio-cini.it**
Prof. Arturo Di Corinto **comunicazione.cybersecurity@consorzio-cini.it**
Web: **https://www.consorzio-cini.it/index.php/it/labcs-home**
Phone: +39 0677274024

Il sistema di informazione per la sicurezza della Repubblica (Italy): Italy's **Intelligence System for the Security of the Republic** is the collective name given to the authorities and organizations responsible for intelligence policies, intelligence coordination and intelligence operations. Nato published an article in English summarizing the whole system as of 2015[17].
The Security Intelligence System includes[18]:

- **President of the Council of Ministers** (Prime Minister)
- **Delegated Authority** (often an under-secretary)
- **CISR** – Comitato Interministeriale per la Sicurezza della Repubblica (Interministerial Committee for the Security of the Republic)
- **DIS** – Dipartimento Informazioni per la Sicurezza (Security Intelligence Department)
- **AISE** – Agenzia informazioni e sicurezza esterna (External Intelligence and Security Agency)
- **AISI** – Agenzia informazioni e sicurezza interna (Internal Intelligence and Security Agency)

Contact: dott.ssa Lucrezia Pagano
Email: **info@sicurezzanazionale.gov.it**
Web: **http://www.sicurezzanazionale.gov.it/**

Aristotle University of Thessaloniki (AUTH) CERT (Greece): The incident response team security AUTH (AUTH-CERT), operated by the Network Operation Center (NOC), has been created to inform the academic community in security and computer networks. It also aims to address security threats to computers and networks. Initially the AUTH-CERT team started off by recording incidents that had to do mainly with virus attacks and security breaches, created by them. The main objective was the handling of complaints made to the AUTh and was originally called Network Abuse Handling Team. After a while the team changed forming a Computer Emergency Response Team (C.E.R.T.), responding to security related issues brought forth by all entities comprising the AUTh Community[19].
AUTH-CERT provides an RSS feed of security announcements in both English and Greek language. The information in those feeds is mostly vulnerability and patch information.

[17] https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ITALY_032015_0.pdf
[18] http://www.sicurezzanazionale.gov.it/sisr.nsf/english/about-us.html
[19] http://cert.auth.gr/index.php/en/

Email: cert@auth.gr
Web: http://cert.auth.gr/index.php/el/

Greek National Intelligence Service: The Greek National Intelligence Service operates the Greek national CERT. The mission of the National Authority Against Electronic Attacks is to attend to the prevention as well as the passive and active encounter of electronic attacks against communication networks, data storage facilities and IT systems. In addition, the Authority is responsible for processing the data and notifying the competent authorities. The responsibilities of the Greek National CERT are[20]:

- The National Authority Against Electronic Attacks is the agency responsible for encountering-protecting mainly the Public Sector along with the Critical National Infrastructures as established by Bill 3469/2008 and Presidential Decree 126/2009.
- The Authority utilizes the appropriate equipment and is staffed by the scientific personnel necessary for its operation, the implementation of the strategic policy decisions pertaining to the encountering of threats and/or attacks and finally the collection, processing and dissemination of the relevant information.
- In order to fulfil its mission more effectively, the National Authority Against Electronic Attacks cooperates with foreign national or other CERT authorities and relevant agencies but with in-country government services, as well.

The information provided on their public web page is rather basic, the news feeds have not been updated in many years. For CS-AWARE it may be interesting to establish contact with the Greek national CERT at some point, but no data that can be collected is provided to the public by this source.

NATIONAL AUTHORITY AGAINST ELECTRONIC ATTACKS
4 P. Kanellopoulou,
Athens 101 77,
Greece

Email: cert@nis.gr
Phone: +30 210 6973541
Web:
http://www.cert.gov.gr
http://www.nis.gr/portal/page/portal/NIS/NCERT

Greek School Network CERT: A CERT similar to the AUTH-CERT described above, but in the context of schools. The RSS information feed in English and Greek seems to be identical to the AUTH-CERT feed.

Email: cert@sch.gr
Web: http://cert.sch.gr/index.php/en/

3.2 Law Enforcement Agencies

The second pillar of organizations from the European Cyber Security Strategy (European Commission and High Representative of the European Union, 2013) is law enforcement. While the CS-AWARE project does not expect as much cooperation with law enforcement as with NIS

[20] http://www.nis.gr/portal/page/portal/NIS/NCERT

competent authorities due to the higher requirements for protecting information relating to cybercrime, we have identified several organizations that may be able to provide relevant information for CS-AWARE.

Europol / EC3: At Europol, generating cyber intelligence involves collecting information on cybercrime from a wide array of public, private and open sources, and then processing and analysing that information[21]. The objective is to enrich and expand the store of law-enforcement data and thus help make the fight against cybercrime as effective as possible. To this end, Europol has developed a number of cyber-intelligence products:

- Cyber Bits: short intelligence notifications on cyber-related topics
- The Open-Source Intelligence (OSINT) Dashboard, which aims to capture the most important events from the passing week in a broadly understood cyber domain
- The Common Taxonomy for the National Network of Computer Security Incident Response Teams (CSIRTs).

These notifications are designed to raise awareness and trigger discussions on further actions. Most are aimed at a broad audience, while a few are intended only for law enforcement authorities. Rather than providing a detailed assessment, they bring important news quickly to the attention of the law enforcement in Member States. Notifications fall into four categories:

- Trends: updates on emerging patterns and on new modi operandi, tools and techniques that cyber criminals use
- Knowledge: guidance on different aspects of cybercrime such as infrastructure, tools and modus operandi
- Technology: news on technical developments that could have an impact on the work of law enforcement authorities, and that can spawn more in-depth reports if it is felt that the initial findings warrant this
- Tools: news on tools that have been developed at the request of a focal point within Europol, a Member State or a European Cybercrime Centre (EC3) stakeholder.

The most relevant information source for CS-AWARE has been identified to be the OSINT Dashboard, which is an accessible weekly update, highlighting for Europol's stakeholders the most important events in cyber security and cybercrime, with a focus on the work of EC3.
It could not be established at this point what the criteria are to get access to the OSINT Dashboard. Furthermore, no publicly available information about the technological basis for the OSINT Dashboard could be found.
Another interesting development is the above mentioned common taxonomy for law enforcement in the context of information sharing with CSIRTs. The current version 1.3 of the taxonomy[22] details how incidents relating to crime can be shared with CSIRTs, including details of the incident as well as the legislative framework relating to it. For CS-AWARE this taxonomy may be relevant in relation to the projects information sharing efforts.

Europol
P.O. Box 908 50
2509 LW The Hague
The Netherlands
Web: https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence

[21] https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence
[22] https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts

Interpol: INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled crimes. Most cybercrimes are transnational in nature, therefore INTERPOL is the natural partner for any law enforcement agency looking to investigate these crimes on a cooperative level. By working with private industry, INTERPOL is able to provide local law enforcement with focused cyber intelligence, derived from combining inputs on a global scale. Their main initiatives in cybercrime focus on:

- Operational and investigative support
- Cyber intelligence and analysis
- Digital forensics
- Innovation and research
- Capacity building
- National Cyber Reviews

No information sharing activities with the public have been identified. However, their web page contains a fairly active news feed that may contain interesting information for CS-AWARE.

INTERPOL General Secretariat
200, quai Charles de Gaulle
69006 Lyon
France

Fax: +33 4 72 44 71 63
Web: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Italian Postal and Communication Police (Part of the Italian State Police): Began as a service of the State Policy to protect post offices and vehicles transporting money. In 1999 it was transferred to the Interior Ministry to oversee the security and continuity of telecommunications in Italy. It is charged with monitoring and investigating criminal and administrative offenses relating to communications: postal fraud, counterfeiting and illicit use of stamps, criminal activities on the Internet, and in general cybercrime.
Caries out investigations relating to computer crime, cybercrime, social engineering, and for all criminal cases that being implemented with the help of the latest technology. Police activities include criminal offenses (including chat-lines, newsgroups, social nets, etc.) regarding: hacking, online paedophilia, e-commerce, scams, money laundering, credit card fraud, terrorism, narcotics, weapons, prostitution; in other words, whenever the crime has involved the use of digital instruments..
In general this police force is charged with guaranteeing the functioning of all IT networks (in particular, the protection of critical IT infrastructures in Italy), the prevention of attacks against strategic national structures. In addition they monitor the security and functioning of telecommunications and efforts to counter pedopornographic activity on line.

Web:
http://www.poliziadistato.it/articolo/23393
http://www.commissariatodips.it/profilo/presentazione.html

3.3 Cyber Intelligence Sources and Information Sharing Tools

In this Section we will detail open source data sources as well as different open source information sharing tools that can be utilized for open source data intelligence, as well as commercial data

providers. For the open source data providers, we focus on sources that provide loosely structured information without a dedicated feed or data format, or if they provide a feed the provided data is usually utilized by aggregated data providers (like the ones described in the next Section). The information sharing tools discussed are mainly community efforts to provide mechanisms for data aggregation. While data aggregation is already covered in the CS-AWARE solution, it is worth looking at those tools to see if it would help us to further simplify the data aggregation effort in CS-AWARE. One resource found during the research on open source data providers was a comprehensive list on collected cyber threat intelligence[23] and was found very useful for our analysis. This github repository not only lists multiple open source data sources but also frameworks and data formats that are mostly up to date and highly relevant. At the end of this Section we focus on commercial data providers, which are usually providing high quality threat intelligence, but at a significant cost.

Shadowserver: The Shadowserver Foundation gathers intelligence on the darker side of the internet. They are comprised of volunteer security professionals from around the world. Their mission is to understand and help put a stop to high stakes cybercrime in the information age. The foundation uses various techniques and gathers, tracks, and reports on malicious software, botnet activity, and electronic fraud, and shares this information with relevant authorities. The information is not open to the public, but information that is relevant to specific networks is shared, if one can prove that one owns and controls this network. The foundation works with national CERTs to share information on a national level. The foundation also works with other sources like abuse.ch or Spamhaus, and recommends to use their blocklists. Another service provided is binary test[24], which allows testing of an executable file against a list of known software applications. Can be used for identifying infected software executables.
They provide a mailing list on which they send out a variety of public statistics and reports. This is also an open discussion list for anything security related[25]. This list may be an interesting information source for CS-AWARE. While Shadowserver is an interesting project, we cannot directly get information from them. Other information providers that collaborate with them may already provide enough relevant and public information. It may be a good idea to contact the Shadowserver project and introduce the CS-AWARE project - we may be granted access to their data.

Email: freed0 (Richard) - freed0*AT*shadowserver.org (Project leader)
Web: https://www.shadowserver.org/wiki/

Abuse.ch: Abuse.ch is a well-known data source in the security community, and both private companies as well as public and government institutions support and rely on this source. Abuse.ch is a free and non-profit organization "operated by a random Swiss guy"[26]. The 4 information sources currently provided are:

- Zeus tracker[27]: ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and an IP-blocklist. Text file based list containing known bad IPs, Domains and URLs can be downloaded.
- Feodo tracker[28]: Feodo (also known as Cridex or Bugat) is a Trojan used to commit e-banking fraud and steal sensitive information from the victim's computer, such as credit card details or credentials. For each IP the Feodo tracker lists, following info is provided: (Firstseen

[23] https://github.com/hslatman/awesome-threat-intelligence
[24] http://bin-test.shadowserver.org/
[25] https://mail.shadowserver.org/mailman/listinfo/public
[26] https://abuse.ch/
[27] https://zeustracker.abuse.ch/
[28] https://feodotracker.abuse.ch/

(UTC), Version, Feodo C&C, Status, SBL, ASN, Country, Lastseen, (UTC)). The list can be accessed as RSS feed.

- Ransomware tracker[29]: Ransomware Tracker tracks and monitors the status of domain names, IP addresses and URLs that are associated with Ransomware, such as Botnet C&C servers, distribution sites and payment sites. By using data provided by Ransomware Tracker, hosting- and internet service provider (ISPs), as well as national CERTs/CSIRTs, law enforcement agencies (LEA) and security researchers can receive an overview on infrastructure used by Ransomware and whether these are actively being used by miscreant to commit fraud. Ransomware Tracker offers various blocklists. These blocklists allows enterprises to block malicious traffic towards known Ransomware infrastructure at the network edge, e.g. by blocking them on the corporate firewall, web proxy or in the local DNS server. As any data provided by Ransomware Tracker are being offered for free (incl. the blocklists), antivirus vendors and vendors of security solutions may also implement Ransomware Tracker blocklists within their products. Ransomware tracker provides text based lists with bad domains.
- SSL blacklist[30]: The goal of SSL blacklist is to provide a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on SHA1 fingerprints of malicious SSL certificates and offers various blacklists. The information can be downloaded as simple text file, or as RSS feed.

The information provided by abuse.ch is very relevant to the CS-AWARE project. Especially the Zeus tracker, Ransomware tracker and SSL blacklist. Note: Abuse.ch is one of the information providers for the Hailataxii service described further below.

Email: coSntacPtAmeM@abuse.ch (remove all capital letters)
Web: https://abuse.ch/

Spamhaus: The Spamhaus Project is an international non-profit organization that tracks spam and related cyber threats such as phishing, malware and botnets, provides real-time actionable and highly accurate threat intelligence to the Internet's major networks, corporations and security vendors, and works with law enforcement agencies to identify and pursue spam and malware sources worldwide. Founded in 1998, Spamhaus is based in Geneva, Switzerland and London, UK and is run by a dedicated staff of 38 investigators, forensics specialists and network engineers located in 10 nations. Spamhaus real-time threat and reputation blocklists currently protect over 3 Billion user mailboxes and are responsible for blocking the vast majority of spam and malware sent out on the Internet. Spamhaus data is today used by the majority of the Internet's ISPs, email service providers, corporations, universities, governments and military networks. Spamhaus provides several publicly available blocklists:

- **The Spamhaus Block List ("SBL") Advisory[31]** is a database of IP addresses from which Spamhaus does not recommend the acceptance of electronic mail. The SBL is queriable in real-time by mail systems throughout the Internet, allowing mail server administrators to identify, tag or block incoming connections from IP addresses which Spamhaus deems to be involved in the sending, hosting or origination of Unsolicited Bulk Email (aka "Spam").
- **The Spamhaus Exploits Block List (XBL)[32]** is a real-time database of IP addresses of hijacked PCs infected by illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, wingate, etc.), worms/viruses with built-in spam engines, and other types of trojan-horse exploits. XBL is a list of spam sources due to exploited computers or other devices. It

[29] https://ransomwaretracker.abuse.ch/
[30] https://sslbl.abuse.ch/
[31] https://www.spamhaus.org/sbl/
[32] https://www.spamhaus.org/xbl/

is mostly composed of--as well as the primary distribution zone for--CBL data (cbl.abuseat.org). It may also include other lists of spam sources due to exploited computers and other devices.

- **The Spamhaus Policy Block List (PBL)**[33] is a DNSBL database of end-user IP address ranges, which should not be delivering unauthenticated SMTP email to any Internet mail server - except those provided for specifically by an ISP for that customer's use. The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges. PBL IP address ranges are added and maintained by each network participating in the PBL project, working in conjunction with the Spamhaus PBL team, to help apply their outbound email policies.
- **The Spamhaus Domain Block List (DBL)**[34] is a real-time database of domains with low reputations. Mail server software capable of scanning email message body contents for URIs can use the DBL to identify, classify or reject spam containing DBL-listed domains. The DBL is queriable in real-time by mail systems throughout the Internet, allowing mail server administrators to identify, tag or block incoming email containing domains which Spamhaus deems to be involved in the sending, hosting or origination of Unsolicited Bulk Email (aka "Spam"). The DBL is managed as a near zero false positive list, safe to use by production mail systems to reject emails that are flagged by it. The DBL includes URIs (domains/hostnames) which are used in spam including phishing, fraud/"419" or domains sending or hosting malware/viruses.

Email: cert-ch-shhq@spamhaus.org (Organization Admin & Industry Liaison)
Web: https://www.spamhaus.org/

SANS Internet Storm Center: The Internet Storm Center is an open source data collection and threat detection platform initiated after the successful detection of the Li0n worm in 2001 and has dedicated itself to protect and forewarn the online community. It relies on volunteers analysing collected data and detecting anomalies as well as funding from the SANS Institute in the United States. The ISC bases its intelligence on millions of intrusion detection logs they gather daily. While most data is only available to members, the membership is easily obtainable. Nevertheless, some information is available to guests of the website:

- IP blocklist[35]
- RSS feeds: Curated Security News Feed[36], Handlers's Diary[37]

One of the most commonly used channels of the ISC are podcasts, which can be found on their website[38] or on any of the major podcast platforms. Furthermore, a twitter channel is provided (@sans_isc) that will be covered in the social media sources further below.

Email: via contact form (https://isc.sans.edu/contact.html)
Web: https://isc.sans.edu

[33] https://www.spamhaus.org/pbl/
[34] https://www.spamhaus.org/dbl/
[35] https://isc.sans.edu/block.txt
[36] https://isc.sans.edu/newssummary.xml
[37] https://isc.sans.edu/rssfeed_full.xml
[38] https://isc.sans.edu/podcast.html

Eurosint - The European Open Source Intelligence Forum: The Eurosint is a European association dedicated to the prevention of attacks and detection of risks. The forum has a few major points they focus on to ensure the best possible threat intelligence usage in Europe some of which are:

- Improve Open Source Intelligence of its members and their communication about it
- Think tank to improve usage of OSINT in the EU
- Include industry partners and increase their interest in OSINT

While the Forum is aiming to improve the utilisation of OSINT in cyber threat intelligence, they themselves do not provide any such data. They act as a platform and facilitator to connect interested parties and guide them towards a joint goal.

Axel Dyèvre (Delegate General Manager)
Martin de Maupeou (Assistant)
EUROSINT FORUM asbl
Boulevard Charlemagne, 42
1000 Brussels
Belgium
Web: https://www.eurosint.eu/

STAXX by Anomali: While Anomali focuses on selling and distributing their products, such as Threatstream, they offer a free UI that automatically downloads the most current threat information and makes it available to its clients. Although the service is desktop based, there is the option to access the data via the Limo service the company offers, which allows you to download past threat information. This could potentially be interesting for the definition of patterns by using historic data of threats. The data provided by Anomali is in STIX format and exchanged via TAXII.

Email: info@anomali.com
Web: https://www.anomali.com/platform

MISP - Malware Information Sharing Platform: This open source platform focuses on the sharing of cyber security intelligence information, but also covers the collection, analysis and storage of the data. The identification of threats is based on taxonomies MISP extracts from existing classifications from trustworthy sources[39]. Since information on the type of sources included and used in the platform can neither be found on the website nor in the github repository, this platform should be downloaded and tested. Also it is questionable if the platform offers some sort of API CS-AWARE can use to collect information or if the final list of feeds MISP uses will lead to external feeds which CS-AWARE can integrate as well. Different communities that provide MISP based cyber intelligence are listed here[40].

Email: info@misp-project.org
Web: http://www.misp-project.org/index.html

[39] http://www.misp-project.org/datamodels/#misp-taxonomies
[40] http://www.misp-project.org/communities/

Threat-intelligence.eu: A community that intends to support threat intelligence analysis by raising awareness of the right standards, tools and methodologies. While this is a relatively new community, they provide a list of the most relevant methodologies and standards relating to threat intelligence.

Web: http://threat-intelligence.eu

Abuse.io: abuse.io is an open source tool that supports "*receive, process and correlate abuse reports*"[41]. It unites efforts by users to automate and enhance response processes of detected attacks. Additionally, abuse.io includes multiple external sources such as, but not limited to: ShadowServer, SpamCop, Netcraft, Google Safe Browsing, IP Echelon, C-SIRT, Project Honey Pot, Abuse-IX[42].

Email: dev@abuse.io **(developer mailing list)**
Web: https://abuse.io

Ifas.io: IFAS is an Information Feed Analysis System developed by HKCERT (Hong Kong Computer Emergency Response Team Coordination Centre) and CSIRT Foundry. It collects security event logs from multiple public sources - allowing analysis and search of events. Its architecture is a combination of Abusehelper, Logstash, Elasticsearch, Kibana and the IFAS reporter[43].

Email: ifas@ifas.io
Web: http://www.irtools.io/ifas/index.html

GCA - Global Cyber Alliance: Global Cyber Alliance is an international community that aims to prevent and fight cybercrime on a cross-sectoral basis. While they do not offer a data feed, they have created two open source tools that can be installed to avert fraud or visiting malicious sites.

- DMARC - domain based message authentication, reporting and conformance[44]
- quad9 - routes DNS queries through secure network of servers and if the website you're trying to reach is infected, it blocks the site

Additionally GCA has the goal to enhance sharing of information and improve global cyber security[45].

Email: info@globalcyberalliance.org
Web: https://www.globalcyberalliance.org

Collaborative Research into Threat: This open source threat and malware repository released by MITRE, a US non-profit research company with federal funding. The principal idea is to allow sharing of threat intelligence information and communicate with others in the field. Since there was no information to be found on the list of sources the company includes in their tool, only stating that in the user interface it is possible to add/delete sources to the account, a test of this source must be

[41] https://abuse.io
[42] https://abuse.io/abuseio/features/
[43] http://www.irtools.io/ifas/index.html
[44] https://dmarc.globalcyberalliance.org
[45] https://quad9.net/#/

conducted before potentially integrating it to CS-AWARE. The software consists of a browser UI which uses an analysis engine to detect attack and/or malware indicators in the data.

Web:
https://crits.github.io
https://github.com/crits/crits

Collective Intelligence Framework: This open source tool, which was created by the US company CSIRTGadgets, combines data from multiple sources, detects and alerts users and mitigates attacks. This cyber threat intelligence management tool mostly uses IP addresses, domains and urls and supports users in parsing, normalising, storing, post processing, querying, sharing and producing resulting data sets[46].

Web: https://github.com/csirtgadgets/massive-octo-spice/wiki/Introduction

3.3.1 Commercial Data Providers

The cyber threat intelligence related data sources listed above are, even if some of them are backed by commercial companies, providing free of charge data. The sources listed below are commercial companies that provide threat intelligence as their business. While CS-AWARE will try to rely solely on free and open source data, it is worth investigating which commercial data sources exist in case the free and open source data is not available. We may try to ask some of those companies for free access to their data in the context of this European research project, based on the letter template available in **Annex 1**.

Flashpoint: Besides their Flashpoint Intelligence Platform, the company offers an API with access to their selected dataset. Next to gathering data from Risk Intelligence Datasets, they observe Deep & Dark web data.

Email: via contact form (http://go.flashpoint-intel.com/contact/partnerships)
Web: https://www.flashpoint-intel.com/solutions/
Country: United States

CheckPoint: Checkpoint not only offers solutions for companies, clouds and databased but also for individuals and government institutions. Additionally, they undertake research and provide insights to the threat intelligence community. On their website they have listed an Advisory Archive, in which all detected threat are listed[47].

Vienna office
Check Point Software Technologies GmbH
Vienna Twin Tower A1625
Wienerbergstraße 11
A-1100 Wien
Austria

International Headquarter

[46] https://github.com/csirtgadgets/massive-octo-spice/wiki/Introduction
[47] https://www.checkpoint.com/advisories/

Check Point Software Technologies Ltd.
5 Ha'Solelim Street
Tel Aviv 67897, Israel

Web: https://www.checkpoint.com/

Country: Israel

Fox-IT: FOX-IT is a cybersecurity company that has four main areas of expertise: High Assurance, Web & Mobile Analytics, the FoxAcademy and of course Cyber Threat Management. While the first three are more about conceptualizing and managing IT security for specific clients' needs, the last covers cyber intelligence regarding threats. The company offers multiple products that cover various aspects of cyber threat management; from analysis of the current state to the emergency response by its internal CERT. One of the offered services of FOX-IT is the Managed Intelligence Service where analysts gather and evaluate data on attacks to prevent their clients from being victimized by new threats. According to the company's website the information collection is automated and compared to an individually designed client profile, which might trigger an alert. If this occurs, an analyst assesses the threat individually. FOX-IT declares the usage of open source data for their threat assessment.

Fox-IT
P.O. box 638
2600 AP Delft
the Netherlands

Email: fox@fox-it.com
Phone: +31 (0)15 284 79 99
Web: https://www.fox-it.com/

Country: The Netherlands

TrendMicro: While trendmicro focuses on the prevention of attacks that are targeting their customers, they also provide research on identified malware and aim to detect attacks while they are occurring. This company, although not typically associated with cyber security intelligence data, most definitely has a unique view into possible attacks in real-time, given their market distribution.

Trend Micro Deutschland GmbH
Zeppelinstraße 1
85399 Hallbergmoos
Germany
Phone: +49 (0)811 88990-700
Web: http://www.trendmicro.de/

Country: Japan

Mnemonic: This Norwegian company has focused on Threat Intelligence and distributing existing defence products developed by other companies. The mnemonic threat intelligence feed is fed by information actively collected by analysts and provides real-time data and all available additional

information on threats. The idea of the Argus Threat feed is to be integrated with other solutions such as firewalls, proxies, endpoint solutions or SIEMs.

mnemonic as
Wergelandsveien 25
0167 Oslo
Norway

Email: contact@mnemonic.no
Phone: (+47) 2320 4700
Web: https://www.mnemonic.no/

Country: Norway

S21Sec: S21Sec is a European cybersecurity company that has developed the lookwise software products to support their customers in the areas of information security management, security regulatory compliance and critical systems protection. Additionally, they created Sigma21, which is their designated cyber threat intelligence service suite. One of its capabilities are Cyber Security Alerts, which are sent out to clients based on their company profile. They work closely not only with technology partners, but also innovation and research partners.

S21Sec
MADRID
Valgrande, 6
28108
Alcobendas

Phone: +34 902 222 521
Web: https://www.s21sec.com/en/

Country: Spain

CrowdStrike: Next to providing typical antivirus software to their customers, crowdstrike also offers threat intelligence tools to aid their clients' security staff in detecting and/or preventing attacks. Their Falcon threat intelligence solutions selling points are proactive security and information instead of overwhelming data. Among the data gathering strategies used are: open source intelligence networks, dark web data and signals intelligence. Nevertheless, collected data is analysed by their analysts and final conclusions are human drawn from the data.

Email: info@crowdstrike.com
Web: https://www.crowdstrike.com/

Country: United States

DCU Microsoft: The Microsoft Digital Crimes Unit is an international team founded by Microsoft which focuses on the detection of online crimes. The most recent focus lies on the identification of tech support scammers and their prosecution. Not much information could be found on the DCU.

Email: via Microsoft media relations (rrt@microsoft.com)
Web: https://news.microsoft.com/presskits/dcu/

Country: United States

ThreatConnect: ThreatConnect offers four different software suites to its clients: TC Analyse, TC Manage, TC Identify and a complete version with the combination of the three. TC offers to find threat, evaluate risk and mitigate harm. TC Identify covers the threat intelligence discovery and data collection as well as the connection to TCs in-house analysts. TC Manage allows the security staff to improve efficiency by automating threat intelligence responses both directly in the defensive tools and/or prompting the responsible staff member to action. The TC Analyse platform is the final component of the software suite and analyses the collected data in an intelligent and company relevant way.

ThreatConnect EMEA Office
107-111 Fleet Street
London, EC4A 2AB
United Kingdom

Phone: +44.20.793.69101
Web: https://www.threatconnect.com/

AbuseSA/ClarifiedNetworks: AbuseSA, an open source platform mainly developed by ClarifiedNetworks (part of Synopsys), provides automated data collection and analysis, as well as actionable advice to its customers. Additionally, it sets up its customers business with response mechanisms and processes should an abuse be detected. Among the data used by AbuseSA for their real time analysis are network incidents, non-profit and commercial organizations, Cyber defence organisations, ISPs and Citizens.

Web: https://www.clarifiednetworks.com

Country: Finland/USA

Additional Threat Intelligence Companies: Following companies were identified as being relevant to CS-AWARE, but were not investigated in detail since they do not, as far as we can tell, have an office within the European Union: ThreatQuotient (https://www.threatq.com), ThreatTrack (https://www.threattrack.com), PerchSecurity (https://perchsecurity.com), paloalto network (https://live.paloaltonetworks.com/t5/MineMeld/ct-p/MineMeld), Norse (http://www.norse-corp.com) and LastLine (https://www.lastline.com).

3.4 Cybersecurity Intelligence Data Feeds

In this Section we detail the most relevant cybersecurity/threat intelligence data feeds we identified. Each of the sources listed in this Section provides a data feed in a structured form, based on common and well known data formats (like STIX/TAXII, JSON, RSS, CSV, XML, ...). Some of the listed feeds provide information to a single cybersecurity related issue, while others act as data aggregators collecting information from many of the sources listed in this document and provide them to the interested audience via one feed in one specific data format. While most data formats used are common feed formats and will not be described further in this document, it is worth noting the

STIX/TAXII formats. The STIX (Structured Threat Information Expression) and TAXII (Trusted Automated eXchange of Indicator Information)[48] are open source protocols specifically developed for cybersecurity related threat information exchange, with a strong community support. Most of the aggregating information providers listed in this Section rely on those protocols.
Overall, it seems that the sources listed in this Section provide up-to-date information, at least in the cases where the refresh time interval was stated explicitly or was easily verifiable (e.g. by accompanying timestamps). For retrieving data from the sources listed in this Section some demo prototypes are available (mainly implemented in Python and Java), which were used by CS-AWARE partners for evaluation and testing the provided feeds. The sources that support communication via STIX/TAXII were successfully queried using the Python library cabby, which supported all TAXII 1.x versions. Similarly, JSON data feeds were very easily handled by the Python library json and RSS feeds were handled by the Python library feedparser. However, the respective Java libraries that were available (e.g. java-taxii) proved to be quite problematic. In particular, the available demo prototypes were not successful in communicating with the various TAXII servers (perhaps due to protocol implementation discrepancies) and also there was no support for TAXII 1.1.1 or later.

Advanced Cyber Defence Centre: Started in February 2013, the European Advanced Cyber Defence Centre (ACDC) aims to create a community of stakeholders joining forces to fight botnets[49]. ACDC provides a complete set of solutions accessible online to mitigate on-going attacks and targeted both to end-users and to network operators. It also consolidates the data provided by various stakeholders into a pool of knowledge, accessible through the ACDC central clearing house. ACDC reaches out to users across Europe through 8 national relay centres. ACDC currently operates as a 30 months EU-supported pilot project, ending in July 2015 and aims to continue as a self-sustained infrastructure beyond the end of the project. Initiated by 28 partners from 14 countries, ACDC is open to stakeholders from industry, public authorities and academia across Member States.

Email:
peter.meyer@eco.de (Coordinator)
outreach@mail.acdc-project.eu
Web: https://www.acdc-project.eu/

Access: Free (10/2017: Due to large scale system update, access cannot be granted at this time)
Data formats: TAXII / STIX, JSON, IODEF, IDMEF, X-ARF

AlienVault OTX: Alienvault OTX threat intelligence has more than 65,000 participants in 140 countries, who contribute over 14 million threat indicators daily. Cyberthreat intelligence is provided via the so-called "pulses". An OTX pulse consists of one or more indicators of compromise (IOCs) that constitute a threat or define a sequence of actions that could be used to carry out attacks on networks devices and computers. In particular, IOCs include information such as IP addresses, domains, hostnames (subdomains), email, URL, URI, file hashes (MD5, SHA1, SHA256, PEHASH, IMPHASH), CIDR rules, file paths, MUTEX name and CVE number. The said data is made available via the STIX/TAXII 1.1.1 protocol and one such example is shown in the snippet that follows:

<stix:STIX_Header>
<stix:Title>OTX Pulse (5a0b0b46fee07f41c7a21123)</stix:Title>

[48] https://oasis-open.github.io/cti-documentation/
[49] https://www.acdc-project.eu/

<stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators</stix:Package_Intent>
<stix:Description>Ongoing reporting by ClearSky</stix:Description>
<stix:Short_Description>https://otx.alienvault.com/pulse/5a0b0b46fee07f41c7a21123</stix:Short_Description>
<stix:Information_Source>
<stixCommon:Description>Alienvault OTX - https://otx.alienvault.com/</stixCommon:Description>
<stixCommon:Identity>
<stixCommon:Name>Alienvault OTX</stixCommon:Name>
</stixCommon:Identity>
<stixCommon:Time>
<cyboxCommon:Produced_Time>2017-11-14T15:27:02.520000</cyboxCommon:Produced_Time>
</stixCommon:Time>
</stix:Information_Source>
</stix:STIX_Header>

Email: hello@alienvault.com
Web: https://otx.alienvault.com/

Access: Free (Registration required)
Data formats: TAXII / STIX 1.1.1

Facebook ThreatExchange: Most threat intelligence solutions suffer because the data is too hard to standardize and verify. Facebook created the ThreatExchange platform so that participating organizations can share threat data using a convenient, structured, and easy-to-use API that provides privacy controls to enable sharing with only desired groups[50]. Individuals can apply for the beta program of the Facebook threat exchange. The application for participation in the beta version can take 2-7 days until it gets approved. Only one app is required per participating entity (e.g. company).

Web: https://developers.facebook.com/products/threat-exchange/

Access: Free (Registration required as a FB apps developer)
Data formats: JSON

Hail a Taxii: Hail-a-Taxii is a service from Soltra hosting open source threat intelligence that is mapped into STIX 1.1.1 and can be accessed by any TAXII 1.1 client. It contains more than 900,000 threat indicators and provides regular updates from multiple feeds (abuse.ch, cybercrime-tracker.net, malwaredomains.lehigh.edu, malwaredomainlist.com, torstatus.blutmagie.de, dshield.org and phsihtank.com). There is the option to get combined data from all feeds for the past 7 days or from a given feed without any temporal limitations. A sample of Hail-a-Taxii STIX data is presented below:

<cybox:Title>IP: 84.179.193.99</cybox:Title>
<cybox:Description>IPv4: 84.179.193.99 | isSource: True | </cybox:Description>
<cybox:Object id="opensource:Address-bf60b009-160d-451b-b183-945e1da9f729">
<cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr" is_source="true">

[50] https://developers.facebook.com/docs/threat-exchange/v2.11

<AddressObj:Address_Value condition="Equals">84.179.193.99</AddressObj:Address_Value>

Email: info@hailataxii.com
Web: http://hailataxii.com

Access: Free
Data formats: TAXII / STIX 1.1.1

HoneyDB: HoneyDB provides real-time data of honeypot activity collected from honeypots deployed on the Internet using the HoneyPy honeypot, which is a low interaction honeypot. The data is made available in JSON format and contains information about malicious IP addresses, number of connections made to the honeypot and the last time each malicious IP address attempted a connection to the honeypot. A sample of the said data in JSON format is presented below:

{"remote_host":"38.122.220.1","count":"8757","last_seen":"2017-11-22"}
{"remote_host":"149.3.181.65","count":"6670","last_seen":"2017-11-21"}
{"remote_host":"124.116.176.142","count":"5870","last_seen":"2017-11-21"}
{"remote_host":"64.208.110.246","count":"5004","last_seen":"2017-11-21"}

Furthermore, participating honeypots tweet their activity via @HoneyPyLog

Email: via contact form (https://docs.google.com/forms/d/e/1FAIpQLSe4IgaMllsrYfNlTO10-JgAOn4rqrtM2F7HbbGhr-GJrNT_Ig/viewform)
Web: https://riskdiscovery.com/honeydb/

Access: Free (Registration required)
Data formats: JSON

Malc0de Database Feed: Malc0de Database contains information about domains hosting malicious executables, including the latest malware samples found in the wild. The information is provided in RSS format and contains Domains, IP addresses, Dates, Autonomous System Numbers, Country Codes and MD5 Hashes of the malicious files. A sample of the said data in RSS format is shown below:

<item>
<title>christaminiatures.nl</title>
<link>http://malc0de.com/database/index.php?search=christaminiatures.nl</link>
<description>URL: christaminiatures.nl/JHgd3Dees, IP Address: 37.97.139.59, Country: NL, ASN: 20857, MD5: 8ac7c66efdeefceea010123faa515cdf</description>
</item>

Web:
http://malc0de.com/
http://malc0de.com/rss/
Access: free
Data format: RSS

OpenPhish - Phishing Intelligence Feeds: OpenPhish is a service that provides information about phishing URLs. A free community feed is available, offered in TXT format that essentially comprises a list of Phishing URLs. The community feed is offered in TXT format and essentially comprises a list of Phishing URLs. The academic feed (offered in JSON) contains additional information. OpenPhish was contacted in 10/2017 to explore the possibility of offering the academic feed for the purposes of CS-AWARE, but there hasn't been an answer since. It is not clear how fresh the URL list is (community feed). The visualisation page (Global Phishing Activity) gets updated every 5 minutes, but there is no reference as to whether and how it relates to the community feed.

Email: contact@openphish.com
Web: https://openphish.com/

Access: Free (Community and academic feeds)
Data formats: TXT, JSON

PhishTank: PhishTank is a free community site where one can submit, verify, track and share phishing data. PhishTank data is distributed in JSON format. However, their feeds can be considered as redundant, since "Hail a TAXII" provides the PhishTank data in STIX format.

Email: via contact form (https://www.phishtank.com/contact.php)
Web: https://www.phishtank.com/

Access: Free (Registration required)
Data formats: JSON, XML, CSV

AutoShun: It provides a list of malicious IP addresses, the number of which gets limited to at most 2000 at any given time. It seems to re-use information from sites like malwaredomains.com[51].

Email: info (at) autoshun.org
Web: https://www.autoshun.org

Access: Free
Data formats: CSV, HTML

BOTVRIJ.EU: BOTVRIJ.EU provides a list of email addresses, SHA1 file hashes (from the respective malware files), IP addresses and domain names as Indicators of Compromise. Each data type is in a separate text file containing an IoC in each line. They claim that the provided data is updated regularly and timely.

Web: http://www.botvrij.eu/

Access: free
Data formats: TXT

BruteForceBlocker: BruteForceBlocker provides information about IP addresses that made SSH login attempts via brute force. The said information includes a timestamp of when they were last seen

[51] http://malwaredomains.com/

and the total number of such attempts they have made. Seems to be updated regularly, as there are several entries for the past few months.

Email: danger@rulez.sk
Web: http://danger.rulez.sk/

Access: free
Data formats: TXT

C&C Tracker: C&C Tracker is a feed of active botnet command and control (C&C) servers. It provides the server IP address, botnet name and description, as well as the date it was added to this list. The list seems to be updated daily.

Web: http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.tx

Access: free
Data formats: TXT

CI Army List: CI Army List is a list of IPs that are not currently present on other threat lists.

Email: cins@sentinelips.com
Web: http://cinsscore.com/list/ci-badguys.txt

Access: free
Data formats: TXT

C1fApp: C1fApp is a threat feed aggregation application, providing a single feed, both open source and private. User account must first be approved to check the feeds. A temporary API key was obtained.

Web: https://www.c1fapp.com/

Access: Paid
Data formats: JSON

Cymon: Cymon is a service by commercial company Esentire and provides a list of IP addresses and domains associated with malware, spam, phishing etc., along with domain and IP information. The data can be downloaded via the offered API in JSON format. The current API version (v1) does not offer any feeds. This functionality is supported by v2, which is supposed to be made available soon (according to information on their website, as checked on 04-01-2018).

Esentire Global Headquarters
278 Pinebush Road, Suite 101
Cambridge, ON N1T 1Z6
+1 (519) 651-2200
Web: https://www.cymon.io/

Access: free (currently no feeds available)
Data formats: JSON

FireHOL IP List: FireHOL offers more than 400 IP feeds that offer various information about an IP address such as its evolution, geo-map, its age, retention policy etc. Furthermore, IP address blacklist and whitelists (graphs etc) are also offered in feed form. They don't offer any API interface to access this data, but they make a large number of files available via their GitHub account, mostly in JSON format (there are very few instances of CSV and XML files). Based on the timestamps of the uploaded files, it seems that update is performed on a daily basis.

Web: http://iplists.firehol.org/

Access: free
Data formats: JSON, CSV, XML

MalShare.com: A free Malware repository providing researchers access to samples, malicious feeds, and Yara results. The information provided includes MD5 hash, file type, date and source information for each malware. The data is made available in JSON, HTML and RAW format.

Web: http://www.malshare.com/

Access: free
Data formats: JSON, HTML, RAW

Metadefender.com: Service provided by Opswat. Offers information regarding malware in JSON format (e.g. including MD5 / SHA-256 hashes, threat name, date it was published). Free registration is required to obtain an API key so as to be able to access the feeds.

Email: via contact form (https://metadefender.opswat.com/contact-us)
Web: https://www.metadefender.com/threat-intelligence-feeds

Access: free
Data formats: JSON

Netlab OpenData Project: Botnet C&C Tracker. They currently provide multiple data feeds, including DGA, EK, MalCon, Mirai C2, Mirai-Scanner, Hajime-Scanner and DRDoS Reflector. According to information on their website, for getting access to the data you need to contact them by e-mail and be "a qualified security researcher". Our contact from 12/2017 has not been answered yet.

Email: netlab@360.cn
Web: http://data.netlab.360.com/

Access: free (on request)
Data formats: n.a.

NormShield Services: Provided by NormShield company. NormShield Services provides information about domains that could be the origin of phishing attacks against another domain. It can also notify users if your information is part of a breach. It also has a blacklist service. Data is given in JSON format through their API. It is worth pointing out that the JSON feeds contain STIX v2.0 fields and therefore conversion to STIX can be performed very easily.

Web: https://services.normshield.com/

Access: free
Data formats: JSON

Rutgers Blacklisted IPs: Part of a US educational institution. Provides a set SSH brute force blacklisted IP addresses comprising their local block rules and entries from badip.com and blocklist.de. The update interval is reasonable (approximately 2 hours). No API is offered for obtaining the data, but the webpage format can be parsed without too much effort.

Web: https://report.cs.rutgers.edu/mrtg/drop/dropstat.cgi

Access: free
Data formats: HTML

ThreatMiner: ThreatMiner is a data aggregator which collects a number of open source data feeds and enriches their results. Information provided is up-to-date and includes both domains and malware samples (MD5 hash, filename, file type, etc). Some of the sources it uses are CIRCL, VirusTotal, Malwr.com, AlienVault OTX, ipinfo, Robtex, CleanMX, VirusShare and Sinica data. Although no API is provided, not much effort is required for extracting threat intelligence from their webpage.

Email: michael.yip.apps@gmail.com
Web: https://www.threatminer.org/

Access: free
Data formats: HTML

3.4.1 Rejected Cybersecurity Data Sources and Feeds

While the initial analysis produced a listing of the above sources, that does not mean that all of them are suitable for utilization by CS-AWARE. Several cybersecurity relevant sources have been identified and have eventually been rejected. Table 3 lists those sources and the reasoning of why they have been rejected.

Table 3: Rejected Cybersecurity Data Sources and Feeds

Source	Reason for rejection
Alexa Top 1 Million sites (http://s3.amazonaws.com/alexa-static/top-1m.csv.zip)	Does not offer any threat-related data, but rather just the top 1.000.000 websites, so as to create whitelists. In CS-AWARE

Source	Reason for rejection
	we do not want to rely on whitelists to grant or deny access to web pages.
APT Groups and Operations (https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtm)	A Google doc containing information on many APT groups, operation and targets. The reliability of this source could not be verified.
Botnet Tracker (https://intel.malwaretech.com/)	The CCSS Forum Malware Certs offers a list of digital certificates that have been reported in the CCSS Forum as possibly being associated with malware. The information provided includes the certificate subscriber and issuer, the certificate serial number, validity period, date reported and date revoked. There are no APIs for this service and therefore web scraping is needed. Under maintenance as of 12-01-2017. Their website replies with the message “Back Soon”.
Cisco Umbrella (http://s3-us-west-1.amazonaws.com/umbrella-static/index.html)	Cisco Umbrella offers a whitelist of the top 1 million sites resolved by Cisco Umbrella. In CS-AWARE we do not want to rely on whitelists to grant or deny access to web pages.
Critical Stack Intel (https://intel.criticalstack.com)	Critical Stack Intel offers free threat intelligence in Bro format. It can be parsed and processed using the Python brothonlibrary. It seems to require sufficient effort to convert into STIX format and may not be worth it given the data volume.
Malware Domain List (https://www.malwaredomainlist.com/)	The data offered is part of Hail-a-Taxii
MalwareDomains.com (http://www.malwaredomains.com/)	The data offered is covered by OpenPhish
Minotaur (https://minotr.net/)	The Minotaur Project was built as a hub for security professionals, researchers and enthusiasts to discover new threats and discuss mitigations. It is a combination of 3rd-party open-source software, local datasets, new analysis tools, and more. It provides malware dates, MD5s, VT score, VT Results along with outputs from many open-source tools. No API is available and the data structure is significantly difficult to parse.

Source	Reason for rejection
NoThink! (http://www.nothink.org/honeypots.php)	The data it provides comes from honeypots and includes blacklisted IP addresses that performed SNMP, SSH, and telnet connections. It seems that the site is no longer maintained and/or updated since 2017-06-28.
SANS ICS Suspicious Domains (https://isc.sans.edu/suspicious_domains.html)	The data offered is covered by Hail a Taxii
WSTNPHX Malware Email (https://raw.githubusercontent.com/WSTNPHX/scripts-n-tools/master/malware-email-addresses.txt)	Offered information is not very rich and therefore doubtful if it is usable.
VirusShare (https://virusshare.com/)	VirusShare is a repository of malware samples to be used by security researchers. No feed or API is offered. Although they claim that access to the site is granted via invitation only, we requested access via e-mail and we were granted it. Offered information is not very rich.
Yara-Rules (https://github.com/Yara-Rules/rules)	Offers a collection of Yara Rules for the respective firewall. he offered data is not very useful and it also does not seem to be updated regularly.
Exploitalert (http://www.exploitalert.com/)	Listing of latest exploits released, mostly affecting CMS, it provides a JSON API. Information provided is not very detailed and therefore not very useful. For example, the first record of a response could be*: [{"id":"19952","date":"2014-10-10","name":"WordPress Google Calendar Events 2.0.1 Cross Site Scripting"}, ...]*

3.5 Malware Analysis

The idea of malware analysis tools is to be able to get a detailed report, listing the behaviour of a suspicious executable in a controlled environment (e.g. sandbox). There are several commercial malware analysis providers available offering those services for a substantial subscription fee. In this Section we will focus on the describing services that offer malware analysis results in a free and open manner.

Hybrid Analysis: A malware analysis service provided by Payload Security[52]. They develop VxStream Sandbox, an automated malware analysis system for enterprises, governments, universities, SOCs and IR teams. At the core of their product is Hybrid Analysis, a unique technology implementing in-depth memory analysis extracting more malicious indicators than comparable products. Hybrid-analysis.com is a free demo version of their services for the community. Hybrid analysis uses a combination of

- Network Inspection

[52] https://www.payload-security.com/

- Open Source Intelligence
- Whitelists
- Multiscanner integration

to achieve its analysis results. Analysis results for each submitted sample include[53]:

- An incident response/risk assessment
- Identified malicious indicators
- Network behaviour
- Process/Memory behaviour

This analysis is very relevant to the CS-AWARE solution in order to identify malicious executables.

Email: via contact form on the web page
Web: https://www.hybrid-analysis.com/

VirusBay: A community that offers analyst-to-analyst type of collaboration. Experts may take a look at malicious samples on a per-case basis if they get interested in the specific case. While this type of semi-automatic analysis, heavily supervised and depended on experts, is not the main interest of CS-AWARE, it might still be interesting for the project to monitor this community. A beta version of virus information platform is available at[54], with the following mission:

"VirusBay is a web-based, collaboration platform that connects security operations center (SOC) professionals with relevant malware researchers. Created as an independent project by Ido Naor, a Senior Security Researcher at Kaspersky Lab, VirusBay is designed to help organizations effectively respond to and recover from an IT security incident when it is not possible for an external expert to visit their facility. VirusBay enables an affected enterprise to collaborate with malware researchers on Indicators of Compromise and the creation of an incident report, among other things. In return, the researcher gains access to malware samples for analysis to improve detection for all. The ultimate goal of VirusBay is to build a community of expertise and data sharing. The project platform is ready for beta-sharing and is currently being presented to the research community for feedback and expressions of interest."

If this platform matures, it may be a valuable information source for CS-AWARE. It may be a good idea to request to join the community.

Web:
https://twitter.com/virusbay_io?lang=en
https://beta.virusbay.io/

VirusTotal: VirusTotal, a subsidiary of Google, is a free online service that analyses files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners. VirusTotal's mission is to help in improving the antivirus and security industry and make the internet a safer place through the development of free tools and services[55]. The most important rule governing VirusTotal's

[53] https://www.hybrid-analysis.com/recent-submissions
[54] https://beta.virusbay.io/
[55] https://www.virustotal.com/en/about/

usage is that none of its publicly offered services/applications should be used in commercial products, commercial services or for any commercial purpose. In the same way, none of the services should be used as a substitute for security products. This is particularly critical and of utmost importance when dealing with the public API.
While VirusTotal does not offer access to analysis results of files submitted by others, it offers a public API that allows automated submission of suspicious files/URLs and receiving of analysis results.

Email: **contact@virustotal.com**
Web: **https://www.virustotal.com/en/**

Malwr: Uses Cuckoo open source Sandbox[56] to analyse submitted malware samples. An independent and non-commercial project. NOTE: 1/2018: Service is down at the moment!

Web: **https://malwr.com/analysis/MWFjZTNjYzk2MjI4NDQwYWE1ZGNjMTY3MWM0OGQ0MTM/**

3.6 Vulnerability Data

While one of the main public data sources provided by NIS competent authorities like CERTs is about vulnerabilities, it is still a good idea to have a look at the most well-known vulnerability trackers. For many years, the CVE list provides a standardized way of enumerating software vulnerabilities. Many new services for sharing vulnerability data are based upon and synced with the CVE list.

CVE list: Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities. Use of CVE Identifiers, or "CVE IDs," which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation[57]. CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for public download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and numerous products and services that include CVE

CVE was launched in 1999 when most cybersecurity tools used their own databases with their own names for security vulnerabilities. At that time, there was significant variation among products and no easy way to determine when different databases were referring to the same problem. The consequences were potential gaps in security coverage and no effective interoperability among the disparate databases and tools. In addition, each tool vendor used different metrics to state the number of vulnerabilities or exposures they detected, which meant there was no standardized basis for

[56] https://cuckoosandbox.org/
[57] https://cve.mitre.org/about/

evaluation among the tools. CVE's common, standardized identifiers provided the solution to these problems. CVE is now the industry standard for vulnerability and exposure identifiers. CVE IDs — also called "CVE numbers," "CVE names," and "CVEs" by the community — provide reference points for data exchange so that cyber security products and services can speak with each other. CVE IDs also provides a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security. The CVE list can be accessed via several ways[58], like downloading the data in several formats (e.g. text, XML, CSV, ...) or as a twitter data feed[59].

MITRE corporation
Massachusetts
202 Burlington Road
Bedford, MA 01730-1420
(781) 271-2000
Virginia
7515 Colshire Drive
McLean, VA 22102-7539
(703) 983-6000

Email: cve@mitre.org
Web: https://cve.mitre.org/cve/cna.html

Access: free
Data formats: TXT, XML, CSV, ...

The national vulnerability database (NVD): NVD is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division. The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. Originally created in 2000 (called Internet - Categorization of Attacks Toolkit or ICAT), the NVD has undergone multiple iterations and improvements and will continue to do so to deliver its services. The NVD is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division. The NVD performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs by aggregating data points from the description, references supplied and any supplemental data that can be found publicly at the time. This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing, relying on vendors, third party security researchers and vulnerability coordinators to provide information that is then used to assign these attributes. As additional information becomes available CVSS scores, CWEs, and applicability statements are subject to change. The NVD endeavours to re-analyse CVEs

[58] https://cve.mitre.org/data/downloads/index.html
[59] https://twitter.com/CVEnew/

that have been amended as time and resources allow to ensure that the information offered is up to date[60]. Data feeds in many different formats are available[61].

Email: nvd@nist.gov
Web: https://nvd.nist.gov/

Access: free
Data formats: JSON, RSS, XML, ...

CVE-SEARCH: cve-search project is a set of tools to import CVE (Common Vulnerabilities and Exposures) and CPE (Common Platform Enumeration) to facilitate search and processing of CVEs[62]. The main objective of the software is to avoid doing direct and public lookup into the public CVE databases. This is usually faster to do local lookups and limits your sensitive queries via the Internet. cve-search includes a back-end to store vulnerabilities and related information, an intuitive web interface for search and managing vulnerabilities, a series of tools to query the system and a web API interface.

Email: project. info(AT)cve-search.org
Web: https://www.cve-search.org/

3.7 Social Media

In this Section we will evaluate different social media sources for their relevance to OSINT in the context of CS-AWARE and local public administrations. While the first part of this Section will identify different social media platforms, the second part of the Section will discuss the two most promising platforms in more detail: Reddit and Twitter. Based on our analysis we expect the most relevant information that can be accessed without restrictions from those two sources. In general we expect to collect fast but not in-depth reactions to currently ongoing security incidents from social media sources. While this information may lack the level of depth we expect from more security focused information sources, information collected from social media may help CS-AWARE to react to quickly evolving incidents.

Xing: Xing is the largest German speaking social platform for professionals and can be compared to Linkedin. Xing only offers access to their data by allowing companies to integrate their services on their websites or in their applications. There is no possibility to query comments or posts in groups or on walls posted by Xing users.

Web: https://www.xing.com/

Access: non-free
Data formats: JSON

Linkedin: LinkedIn differentiates between applications and developers when dealing with request limits per day. Following data can be accessed, only if the publisher or user set his/her settings accordingly: data on member profile, company profile, geography, languages, currency, industry,

[60] https://nvd.nist.gov/general
[61] https://nvd.nist.gov/vuln/data-feeds
[62] https://www.cve-search.org/about/

company size, seniority, job function. Similarly to Xing, LinkedIn also does not offer data from posts and/or comments[63].

Web: https://www.linkedin.com/

Access: non-free
Data formats: JSON, XML

Reddit: Reddit, a social news aggregator, allows access to all data on their site. Users can either add comments or links to subreddits, of which each covers a select topic. There is a limitation of 60 requests per minute, per user. Exemplary information available: up/downvotes, title, body, subreddit, link. Since all information on Reddit can be queried, they provide an extensive wiki on how the JSON files they return are structured and which information is included[64].
Since the API is not yet being tested, the analysis of the potential results is based on results from search queries on the website. Overall, the results for initial keyword based analysis (detailed in the next Section) indicate that there is an extensive amount of data available. It is essential to focus on specific subreddits related to the security community. While not all potentially relevant data can be guaranteed to be posted in one of the chosen subreddits, it is most likely as the user community is quite strict with adhering to the set user guidelines. In general, one of the compelling arguments for Reddit data is the self-governing nature of the platform. This is due to the moderator system, meaning each subreddit creator can select moderators individually among registered users.

Web: https://www.reddit.com/

Access: free
Data formats: JSON

Facebook: GraphAPI is the current query language used by Facebook and can be read via HTTP GET requests[65]. To usefully extract data from Facebook, the preselection of informative users and/or pages is necessary. Regarding request limits, following information could be found: 200 calls per hour, per user. Facebook does provide a public feed API but this is only accessible by a set of media publishers and requires approval by Facebook, which cannot be applied for currently.
Additionally, facebook provides a new threatexchange API which is currently in beta version and can be applied for[66]. The Facebook threat exchange is covered in more detail in the Section relating to cyber threat intelligence sources.

Web: https://www.facebook.com/

Access: non-free
Data formats: JSON

Twitter: Twitter's search API focuses on relevance and not completeness – it returns queries against indices of recent or popular tweets. The standard search API is limited to the last 7 days of published

[63] https://developer.linkedin.com/
[64] https://github.com/reddit/reddit/wiki/JSON
[65] https://developers.facebook.com/docs/graph-api/using-graph-api
[66] https://developers.facebook.com/docs/threat-exchange/v2.11

tweets. The request limits of this API are 180 per user or 450 per app in 15 minutes[67]. There is also the possibility of real-time streaming of tweets, limited to 400 keywords, 5000 users IDs and 25 location boxes[68].

Web: https://twitter.com/

Access: free (with restrictions)
Data formats: JSON

Google+: The Google+ API provides following information to its users: activities - notes users post to their stream, comments - replies to activities, people - users. The limit depends on the account type[69].

Web: https://plus.google.com/

Access: non-free
Data formats: JSON

3.7.1 A closer analysis of Twitter and Reddit

At this time our assessment is that the most promising social media sources to be used in CS-AWARE are Twitter and Reddit. In order to properly assess the possible information that can be collected from each social media website, the following keywords were chosen:

- firewall
- malware
- ddos
- virus
- phishing
- spyware
- ransomware
- vulnerability

In Twitter some of these keywords resulted in a limited number of tweets - less when searching for *#'keyword'* than just the word alone, such as firewall, ddos, virus, phishing, spyware and vulnerability. Out of these especially non-specific words such as vulnerability and virus, which can be used in different contexts, result in tweets with no relevance to CS-AWARE. It will be crucial to filter out such irrelevant information before extracting and storing the data. Other keywords had a great amount of tweet-output which definitely would yield some valuable information. Malware and ransomware yielded a high amount of on-point tweets. The actual relevance to detect attacks would need to be evaluated in real-time. Additionally, a list of interesting users was selected to be analysed in more detail:

- Shadowserver
- sans_isc
- EC3Europol

[67] https://developer.twitter.com/en/docs/tweets/search/overview
[68] https://developer.twitter.com/en/docs/tweets/filter-realtime/overview
[69] https://developers.google.com/+/web/api/rest/latest/comments

- IntelSecurity
- INTERPOL_Cyber
- HoneyPyLog

While these users offer great input and information on cyber security risks and threats, there is the need for further, more detailed research into analysts and good Samaritans supporting the public cause, by openly warning when attacks occur. Not all public institutions would immediately go public with information they detect, it is therefore more likely to find valuable information quicker on individuals' feeds. On Reddit all keywords yield a much higher output, in this case it will be vital to research and define relevant subreddits on which to focus the data extraction. Further, there might be individual users on the platform that prove themselves to be particularly engaged and informative. For example, the following two screenshots, seen in Figure 3 and Figure 2, show an overview of the top results for the keyword "malware" on both social media platforms and should illustrate cybersecurity related information is available on social media that should be investigated further for its relevance to CS-AWARE.

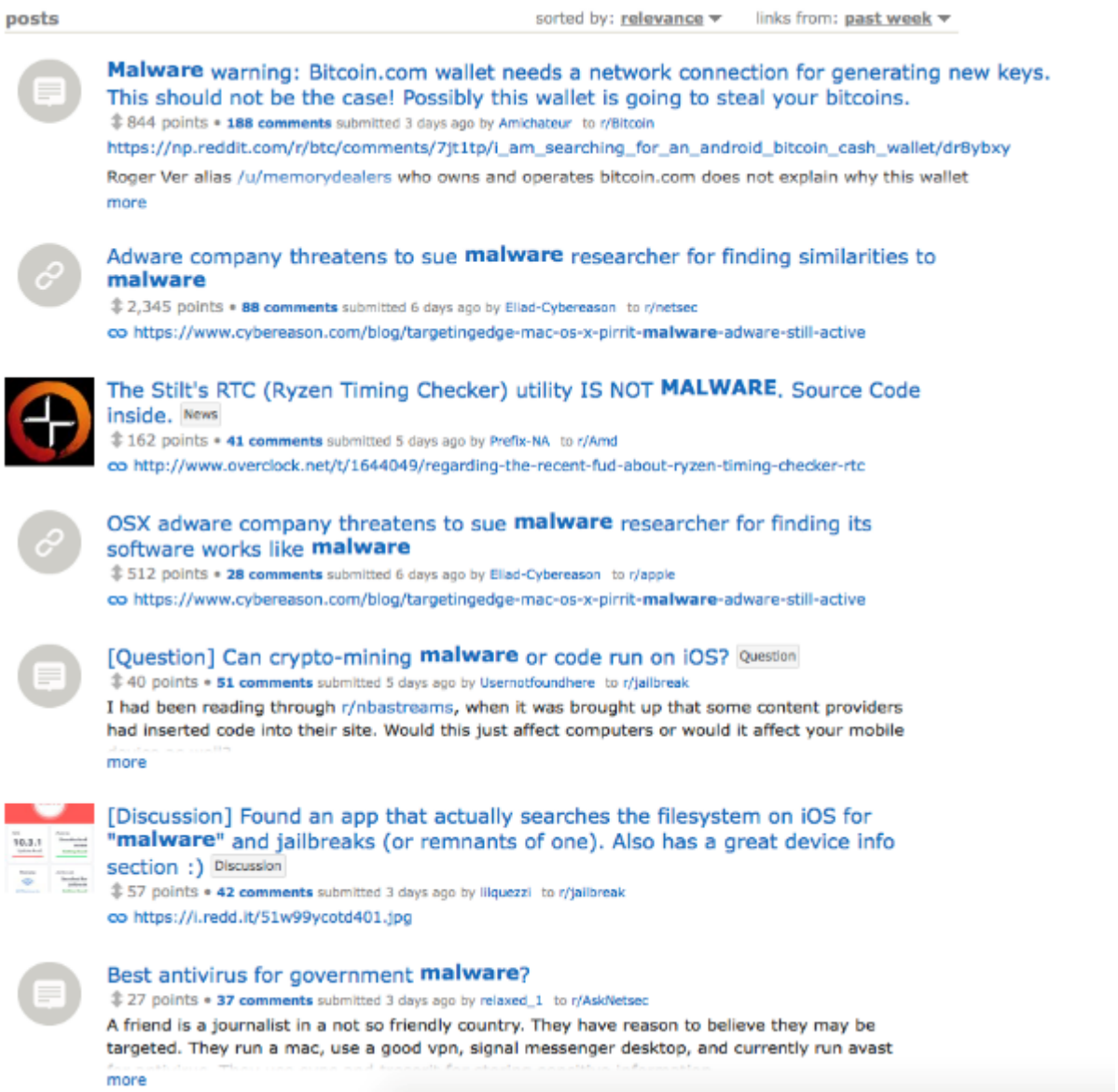


Figure 2: Social media example – Reddit

Figure 3: Social media example - Twitter

3.8 Cybersecurity Visualizations

Good examples of cybersecurity related visualizations can be beneficial in two ways to the CS-AWARE project: We may get an inspiration for the visualization of the cybersecurity situational awareness component of the project and the data sets used for publicly available visualizations may be a potential information source for CS-AWARE. The report on Metaphors on Cybersecurity by the Sandia National Laboratories (Karas, Moore, & Parrott, 2008) provides interesting insights in the topic of cybersecurity related visualization.

Information is Beautiful: Information is Beautiful is a well-known blog by David McCandless, a London-based author, writer and designer. He and a small team behind him are out to distil the world's data, information and knowledge into beautiful and useful graphics & diagrams. Their goal is always to help everyone make better, clearer, more informed decisions about the world. They are visualizing data on a broad variety of different topics - They base all their graphics & visualisations on facts & data. They illustrate multiple perspectives (even if they don't agree with them). And, because knowledge is evolving and data is updated, they constantly revise and revision their work[70]. One visualization and data set that may be of interest to CS-AWARE is about the world's biggest data breaches and hacks[71,72].

Email: via contact form on web page
Web: http://www.informationisbeautiful.net/

Digital Attack Map: Digital Attack Map offers a visualisation of real-time DDoS attacks worldwide. Historical data is also available and can give users insights into patterns and trends. The tool is produced by Google Ideas and Arbor Networks, the latter providing the data for the graphical representation[73]. As metaphors have impact on the awareness process, the linguistic usage should be examined in order to use the visuals contained in the metaphors relating to cyber security.

Web: http://www.digitalattackmap.com

Log analytics by Fastly: Real-time insights are critical for understanding how your web and mobile traffic is performing. With Fastly you can stream 100% of your logo data in real time to Google BigQuery and use Looker to visualize and analyse your data[74].

Looker Data Sciences
Headquarters
101 Church Street
Santa Cruz, CA 95060

Web: https://looker.com/platform/blocks/source/log-analytics-by-fastly

[70] http://www.informationisbeautiful.net/about/
[71] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[72] https://docs.google.com/spreadsheets/d/1sJW1mbc-44xCNwRRGns5UuqhUSB8iZ8o2-TrgQu4kJQ/edit?single=true&gid=2&range=A1:W400#gid=1640918774
[73] http://www.digitalattackmap.com/faq/
[74] https://looker.com/platform/blocks/source/log-analytics-by-fastly

The works of Edward Tufte and Graphic Press: Edward Tufte is a renowned visualisation expert. His homepage contains much inspiration in the included notebook entries regarding visualisation.

Web: https://www.edwardtufte.com/tufte/

3.9 Other Information Sources

In this Section we list classes of Information that were considered during analysis, but turned out to be less relevant than expected and will most likely not be information considered for CS-AWARE.

Software version check: The idea would be to see what version of a software is installed and check what would be the latest up-to-date version, in order to discover outdated and potentially vulnerable software. A list of popular software and its latest version could not be found. However, one option would be to identify the most critical software within the pilot systems, and identify where to find information about the latest version on a per-case basis (e.g. the manufacturer's web page).

Leaked Data: One class of information sources could be leaked data. While leaked data, like for example the WikiLeaks Vault7 leak[75], has proven to be a valuable source of cybersecurity related information in the past years, CS-AWARE will not consider such information as information source due to its unreliability and substantial legal grey areas.

4 Analysis of Pilot Scenarios

In this Chapter we will focus on the description of our initial analysis of the systems of the CS-AWARE piloting partners, the Municipality of Larissa, Greece and the Municipality of Roma Capitale (RC), Italy. In CS-AWARE, the system and dependency analysis of local public administrations is an integral part of the solution, and a pre-condition for the eventual deployment of the CS-AWARE cybersecurity awareness tools. Since each municipality is different, without an individual analysis of the specific assets and dependencies among them, cybersecurity awareness will always be incomplete. However, we have already seen during our initial analysis, and backed by our initial threat analysis in Chapter 1, that there are fundamental similarities in the general duties and procedures of LPAs that will allow us to derive general guidelines and procedures that may simplify the analysis for future administrations and potential customers of the CS-AWARE solution.

The end result of the pilot specific system and dependency analysis, will be to identify the critical assets within local public administrations, the dependencies among them and how those assets can be best run-time monitored to gain an understanding of the cybersecurity situation. The main goal for this round of analysis was to gain an initial understanding of the complexities within LPAs and identify realistic and meaningful piloting scenario that can be managed with the resources available for this project. During the analysis we have met and even exceeded the expectations we set for our first round of analysis. In both piloting scenarios we have now a clear understanding of the critical assets and their dependencies to other critical assets that need to be taken into account, and we have identified how those assets can be monitored. We have set the basis for the next round of system and dependency analysis, which will focus on building and finalizing the dependency model based on our results, how the relevant data can be extracted for on-line monitoring, and if this data potentially contains personal identifiers that need special handling (permissions from the relevant data protection authorities as well as anonymization at source).

To conduct the system and dependency analysis we utilized the soft systems methodology (SSM) (Checkland, Systems Thinking, Systems Practice, 1981) (Checkland, Soft Systems in Action, 1990), as laid out in the work plan of the CS-AWARE proposal. More specifically we were focusing on the

[75] https://wikileaks.org/ciav7p1/

first two steps of the methodology, "Enter the problem situation" and "Express the problem situation". We organized a one week workshop with each of the piloting partners and utilized and asked them to draw rich pictures relating to their systems and express the problem situation in those pictures. We were able to achieve the level of detail we expected from this round of analysis within one week in the Municipality of Larissa (2.10-6.10 2017), given that Larissa is a medium sized municipality and the system complexity is manageable. We quickly realized that we will not be able to gain a sufficient level of detail during the one week workshop we organized in the Municipality of Roma Capitale (16.10-20.10.2017) due to the socio-technological complexities that are present in a municipality the size of Rome. A second one week workshop was organized (11.12-15.12 2017) in which we were able to achieve similar results than during the workshop in Larissa. The Sections below present the results of those workshops in detail.

4.1 First Soft Systems Workshop in the Municipality of Larissa (2.10-6.10 2017)

The first workshop in Larissa commenced on October 2nd 2017. The workshop ran for three days, but the members of the systems analysis team (the analysts) continued to analyse the output from the workshop until the end of the week to ensure that they had developed an understanding of Larissa's systems and networks. The visiting project team of analyst / facilitators comprised as follows:

Organization	**Participant**
University of Oulu	Christian Wieser
University of Vienna	Thomas Schaberreiter Veronika Kupfersberger
CARIS Research Ltd	Christopher Wills Robin Hirsch
Innosec	Alex Papanikolaou
Larissa	George Kolovou Heleni Drakou Christos Topalidis Thanasis Poultsidis
OTS	Nikos Tsiridis George Apostolopoulos Leonidas Orfanidis

Several weeks prior to the workshop commencing, Larissa was asked to provide an overview of the systems and networks used by Larissa, Elassona and Kileler (while Larissa is a full project partner, the Municipalities of Elassona and Kileler are associated with the project vie a letter of support, and will deploy the CS-AWARE solution if the results in Larissa are promising. In this analysis however, we will focus on the Municipality of Larissa, since we have identified significant similarities in the set-ups). This overview can be found in Annex 2 of this report. It is clear from this overview and as is as depicted in Figure 4, that there is some considerable duplication of systems.

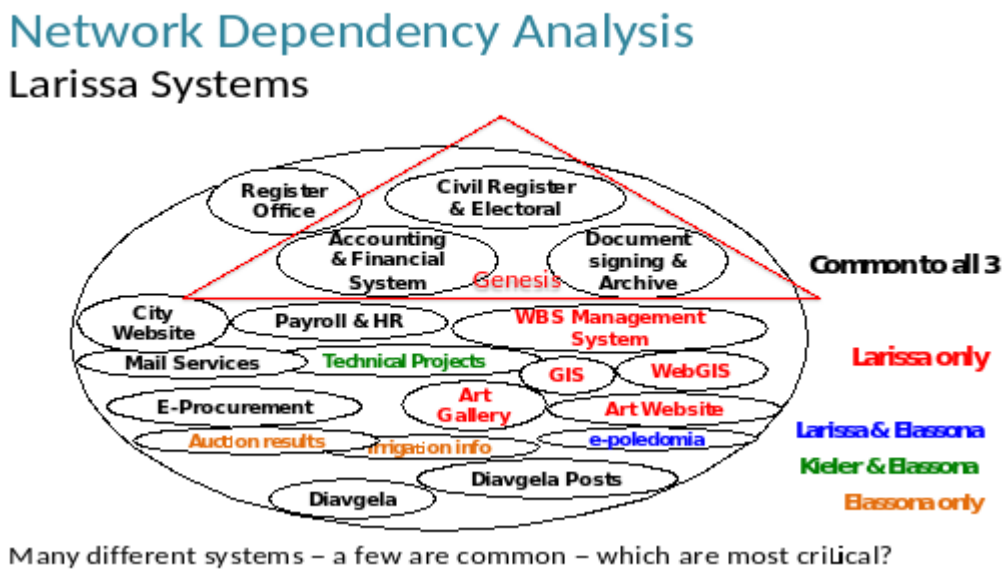


Figure 4: High level system view

Following introduction from The Mayor and Deputy Mayor of the City of Larissa, Thomas Schaberreiter gave a short overview of the CS-AWARE project. Christian Wieser gave a short presentation on the issue of ethics and data protection. Chris Wills gave a short presentation of the Soft Systems Method and answered questions from the Larissa team.

The Larissa team were asked to identify those systems that contained personal or sensitive data, or data that was mission critical to the operation of the City Government. Additionally, they were asked to identify points in the network / systems architecture where it might be possible to collect analytical data such as log files that could be used to identify anomalous events. The analysts emphasised that this was a key problem to be resolved in this first iteration of the systems and dependency analysis. The Larissa team then commenced drawing RP's depicting the City's IT systems and networks.

The analysts expected that a number of RP's of systems and networks would emerge from the process as being of clearly particular significance for informing the design of the CS-Aware pilot system. It is these RP's that will be examined in detail in this first iteration of the systems and dependency analysis, in the main body of this report. However, all of the RP's drawn by the Larissa team, along with the associated descriptions that were formulated by Thanasis Poultsidis and his colleagues from Larissa, can be found in Annex 2 of this report. This is not to say that the RP's contained in Annex 2 are of any less significance or importance than those upon which we concentrate in this report. Far from it, as they have enabled all of the participants in the workshops to begin to develop a thorough, holistic, understanding the systems operating in Larissa and in particular, the interdependencies between the systems and the networks via which, the systems are connected.

4.1.1 Day 1: A high level analysis

The first two RP's drawn on the first day of the workshop depict a high level overview of the City's systems and networks. Day 1 RP 1 gives an overview of the City's network and main services. The only gateway from the City's systems to the Internet and the telephony connection to the outside world is via a router called SYZEFXIS router. SYZEFXIS is a virtual private network that the Greek Government maintains and oversees. It connects all Greek public authorities. The Cities of Larissa, Elassona and Kileler all use a SYZEFXIS router, as does every other LPA in Greece. SYZEFXIS is connected to both the Metropolitan Area Network (MAN) and to the three servers located in the Town Hall. The City does not control the SYZEFXIS router and cannot monitor the traffic running through SYZEFXIS. The R710 hosts Genesis, (the City's ERP system that is used to manage income and expenditure) Genesis handles information about both suppliers and citizens and tax and debt

collection. This system is used for maintaining the civil registry, for the records of document signings and for the cash desk. Additionally the R710 hosts the Human Relations Management System (HRMS) and public applications along with the American Computer Engineering (ACE) ERP and the ECM application that is used to manage public construction works. Genesis and the HRMS run in an Oracle relational database.

The Metropolitan Area Network (MAN) is pictured on Day 1 RP 2 and includes connection to the two hospitals, the police and the fire service. The MAN is owned by the City and is a fibre optic network that includes some wireless bridges. One key question that emerged from the first two RP's was about network level monitoring points that could eventually be used to interface to CS-AWARE. It appeared as if there was no obvious place in the network where traffic could be monitored and where anomalous events could be detected and used as a feed into the proposed CS-AWARE system. At the close of the first day, the Larissa team were asked to think about how and where such a monitoring point might be established.

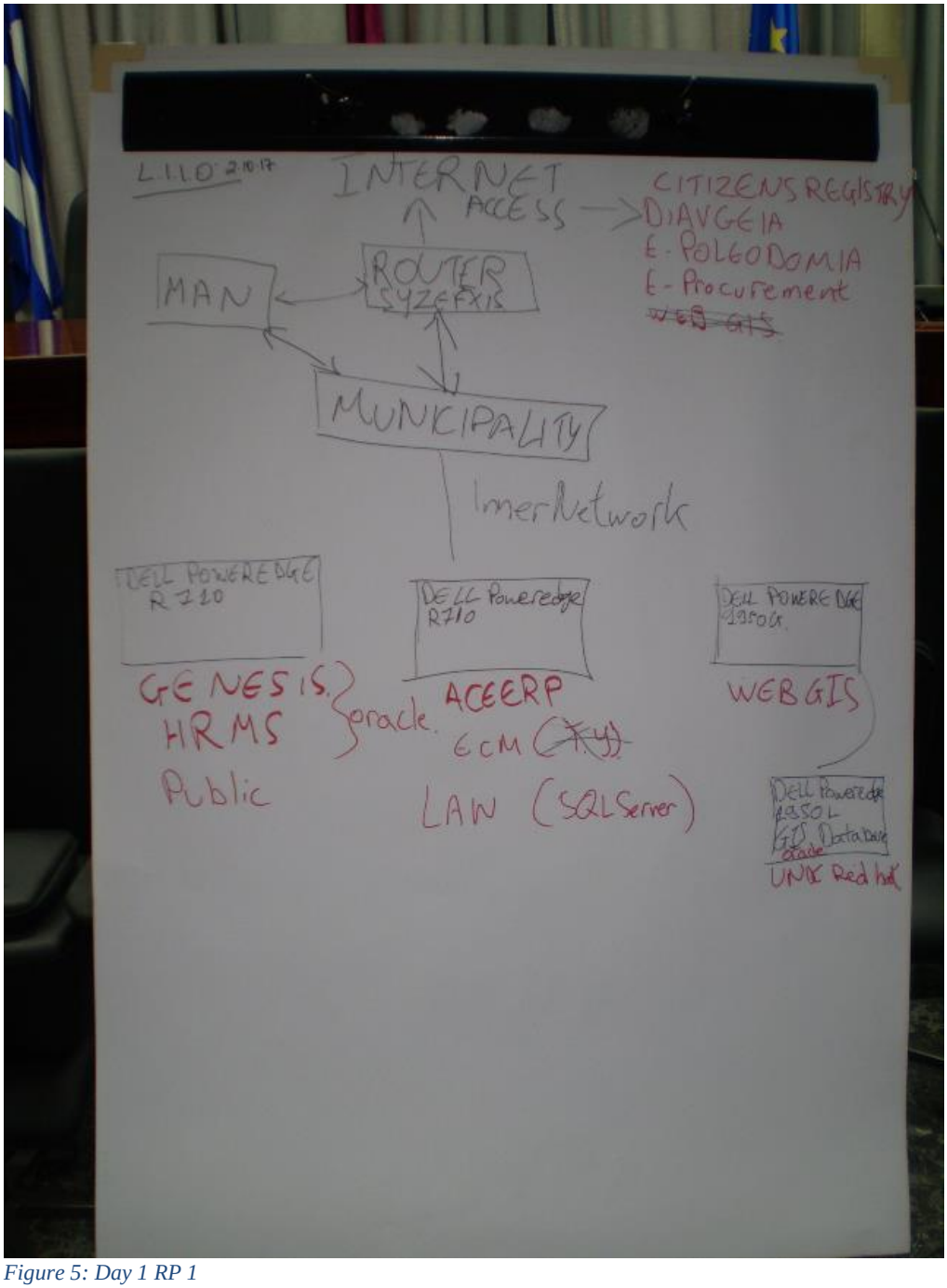


Figure 5: Day 1 RP 1

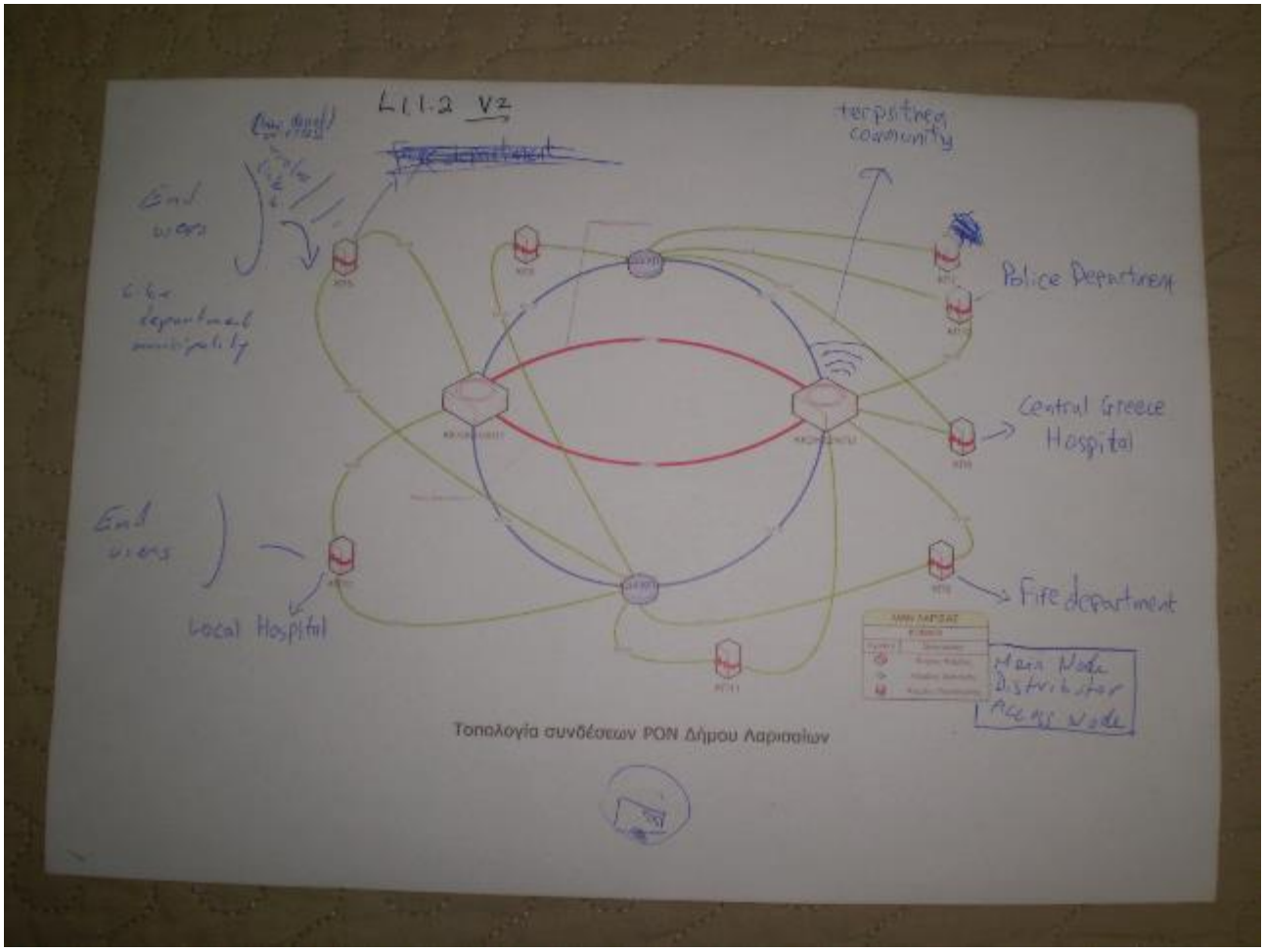


Figure 6: Day 1 RP 2

A further six RP's were drawn on the first day which examined the operation of GENESIS, the apps running on the MAN and its nodes and the HRMS in greater detail, allowing us to understand the dependencies between the network set-up and the service level applications in the Municipality of Larissa managing the most critical data. Day 1 RP5 lists how the MAN nodes interact and depend on different services operated by the Municipality of Larissa. For example, we can understand from this picture that from all the access nodes on the Municipal Area Network, nodes 2, 3, 5, 6 and 12 have connections to Genesis and here are therefore potential attack vectors.

Day 1 RP4 details GENESIS, the City's ERP and as such one of the key systems in Larissa. It is a "mission critical" system in two respects; it handles the City's revenues, tax collection, and tracks invoices and payments. Most importantly, it also stores and processes personal data about citizens and sensitive data about the municipality's operations.

Day 1 RP 7 details HRMS, another critical service operated by the Municipality of Larissa. The Human Resources Management System (HRMS) stores and processes personal and sensitive data about the City's personnel such as employee's educational background, job contract, annual leave and salary, along with taxes and deductions. It also produces reports for all management levels as well as official financial statements. It therefore another "mission critical" system, that will require monitoring.

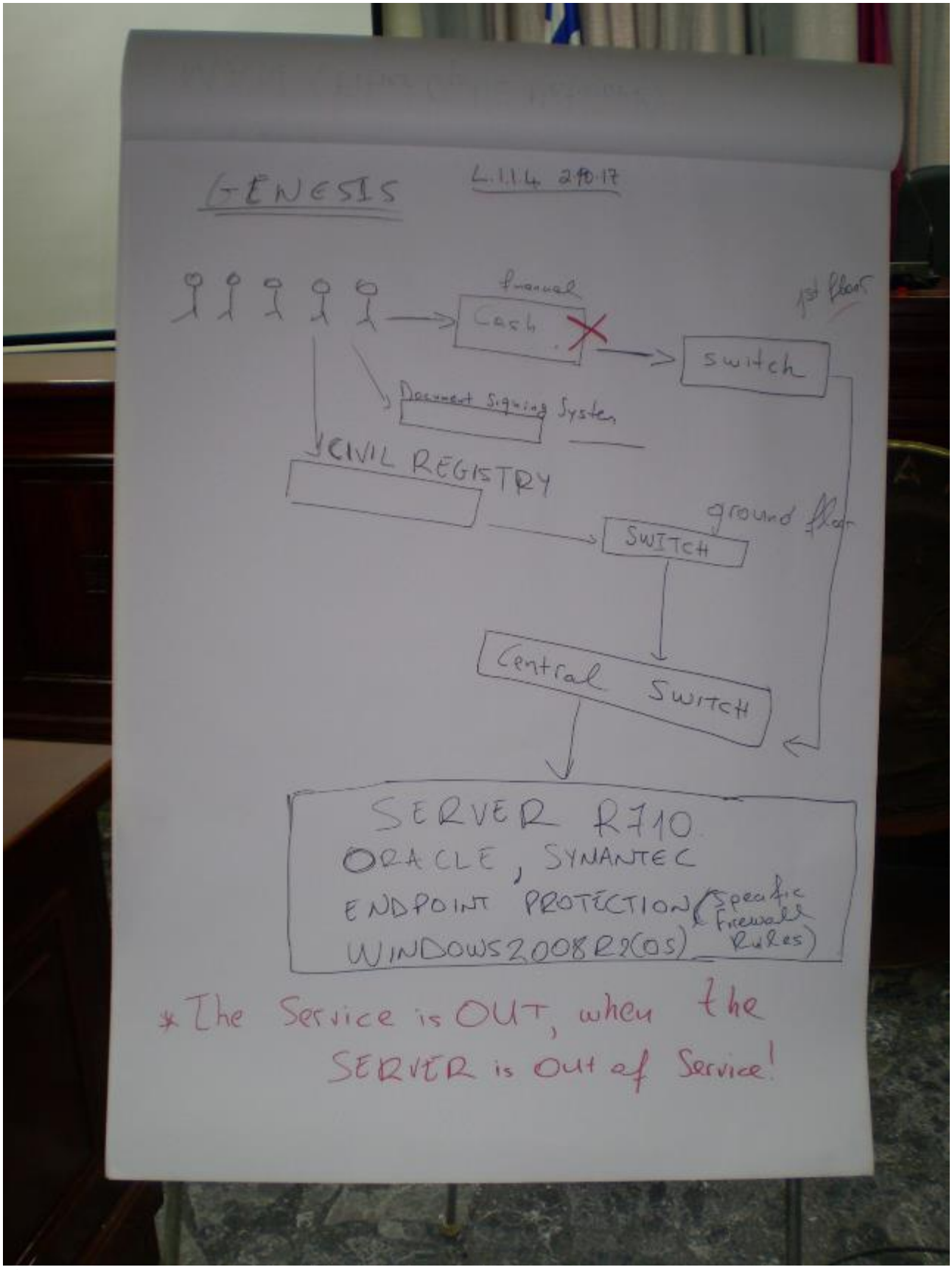


Figure 7: Day 1 RP 4

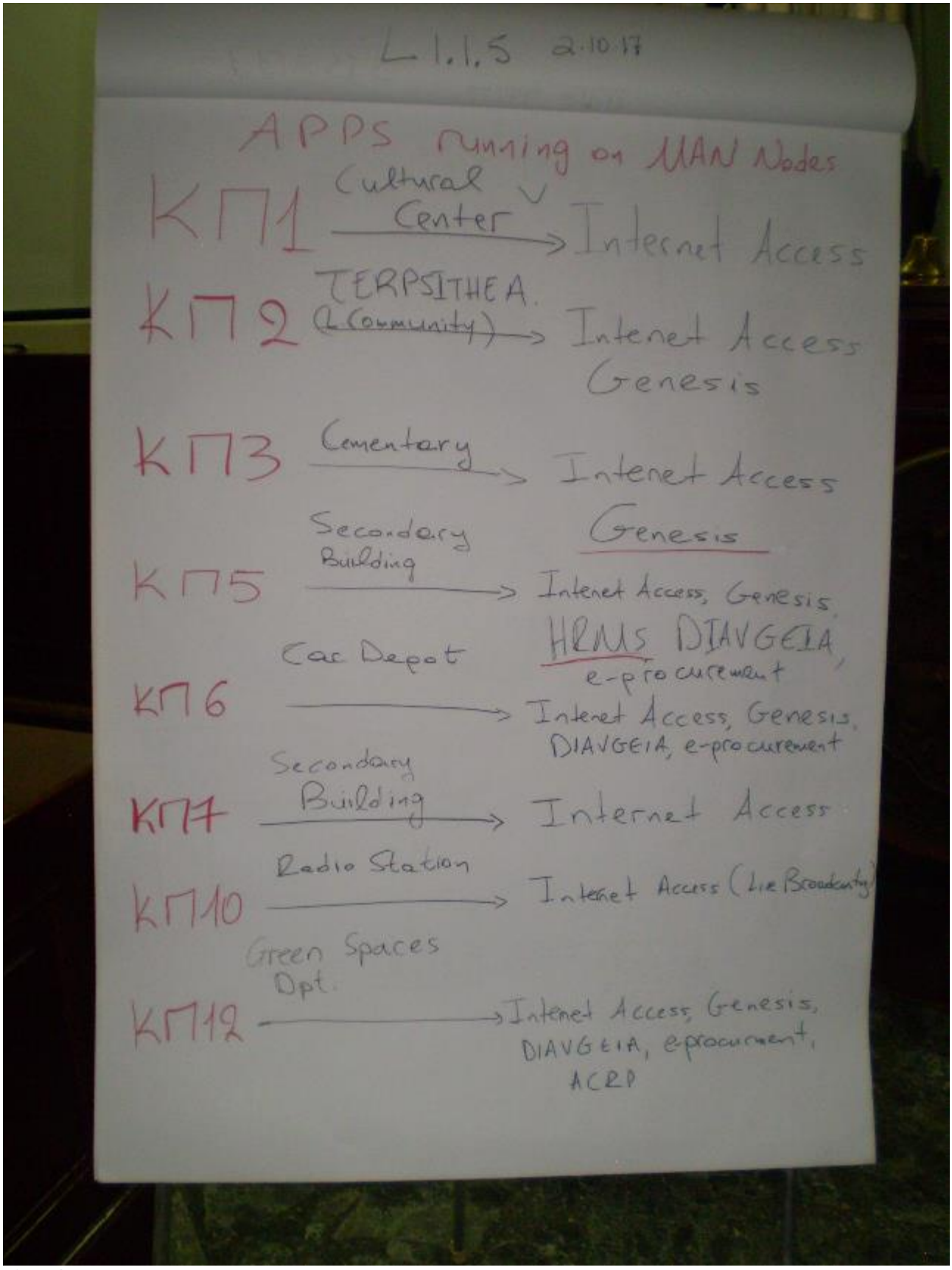


Figure 8: Day 1 RP 5

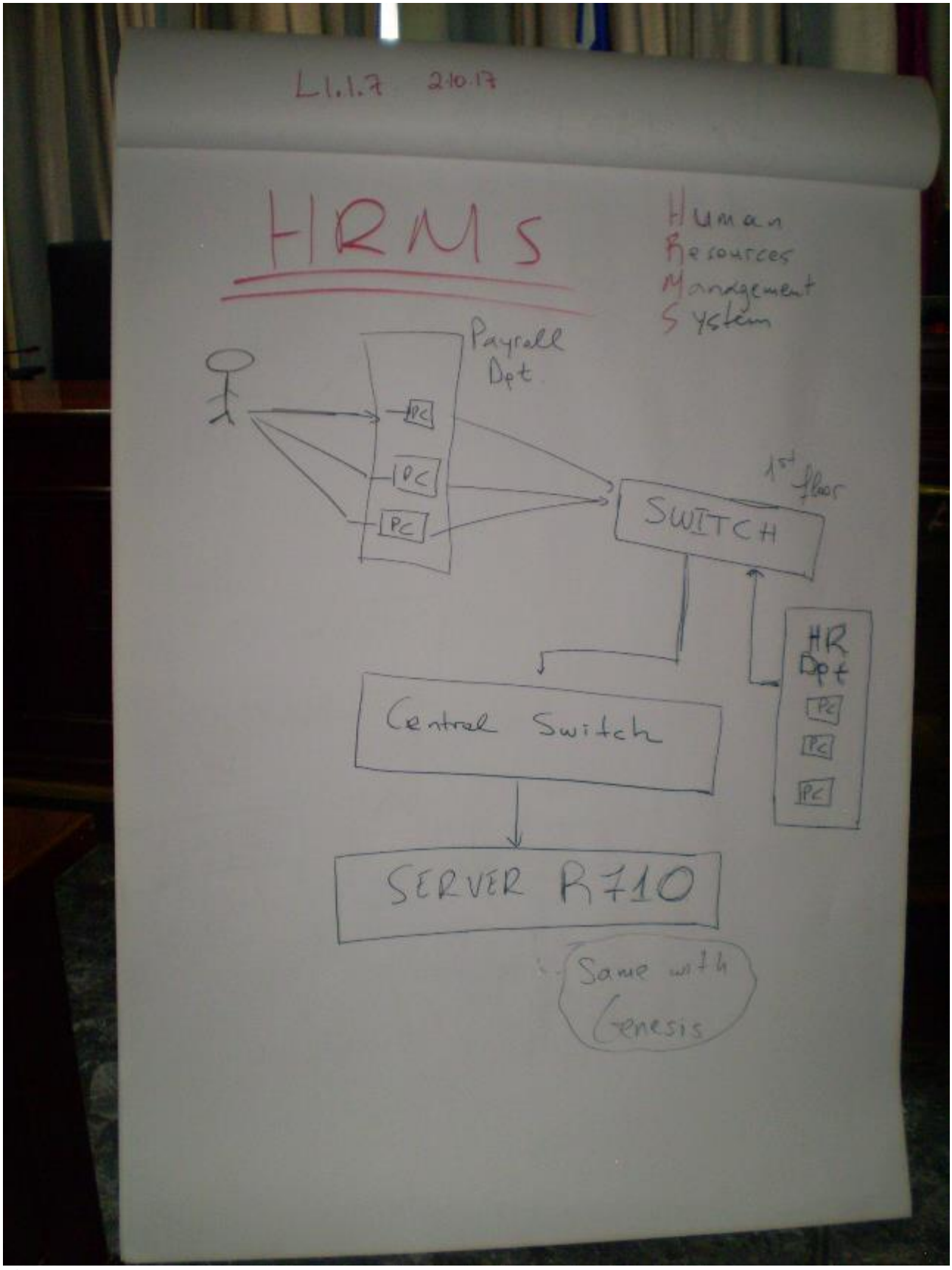


Figure 9: Day 1 RP 7

4.1.2 Day 2: A detailed system analysis

On day 2 an additional 8 rich pictures were produced, which can be found in Annex 2 together with a detailed description of each picture. We focused on a more detailed analysis of the critical systems we had identified during the overview analysis in first day of the workshop. We asked to identify possible flows of critical data in day-to-day operation, on the network level and the service level. Furthermore, we asked for an analysis of the existing security mechanisms and how data from those mechanisms could be potentially used in CS-AWARE.

On the service level, it was established through a series of rich pictures that GENESIS and HRMS are in fact the two most critical services in Larissa, and that both could be potentially monitored with the auditing features of the applications themselves, as well as the built-in auditing mechanisms of the database that manages the data.

On the network level, the Larissa team responded to the request to identify a possible monitoring point in Day 2 RP 1. They had identified a gateway router that had been bypassed when the fibre optic switch was added to the network, but is configured in a way that still all traffic is routed through this now redundant router. It has been identified as an ideal potential monitoring point for CS-AWARE.

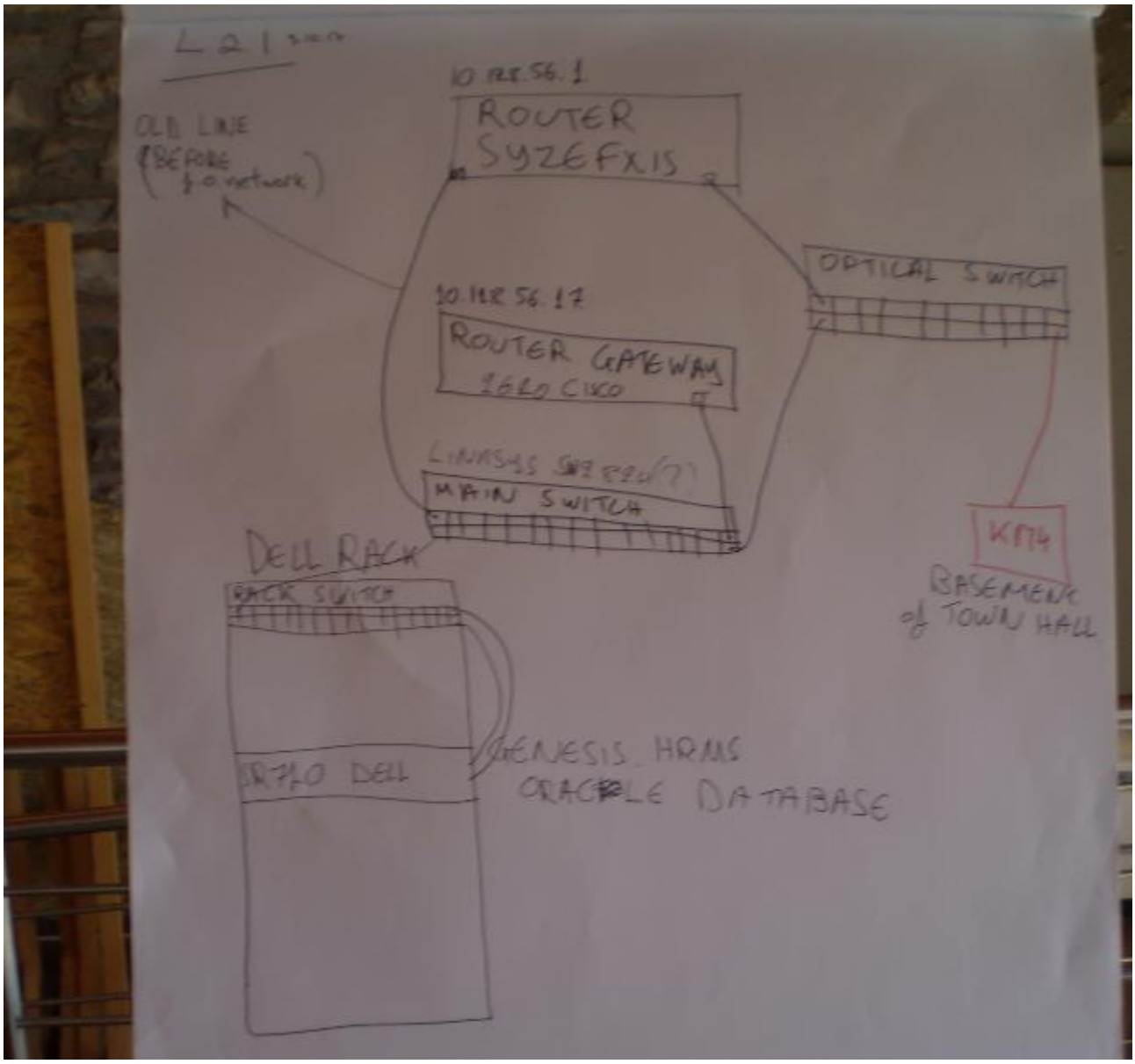


Figure 10: Day 2 RP 1

At the end of day 2 we started looking into existing security mechanisms. As illustrated in Day 2 RP 8, Symantec Endpoint Protection (SEP) is installed as the main security mechanisms on all servers as well as on all clients (with an additional antivirus program on the clients).

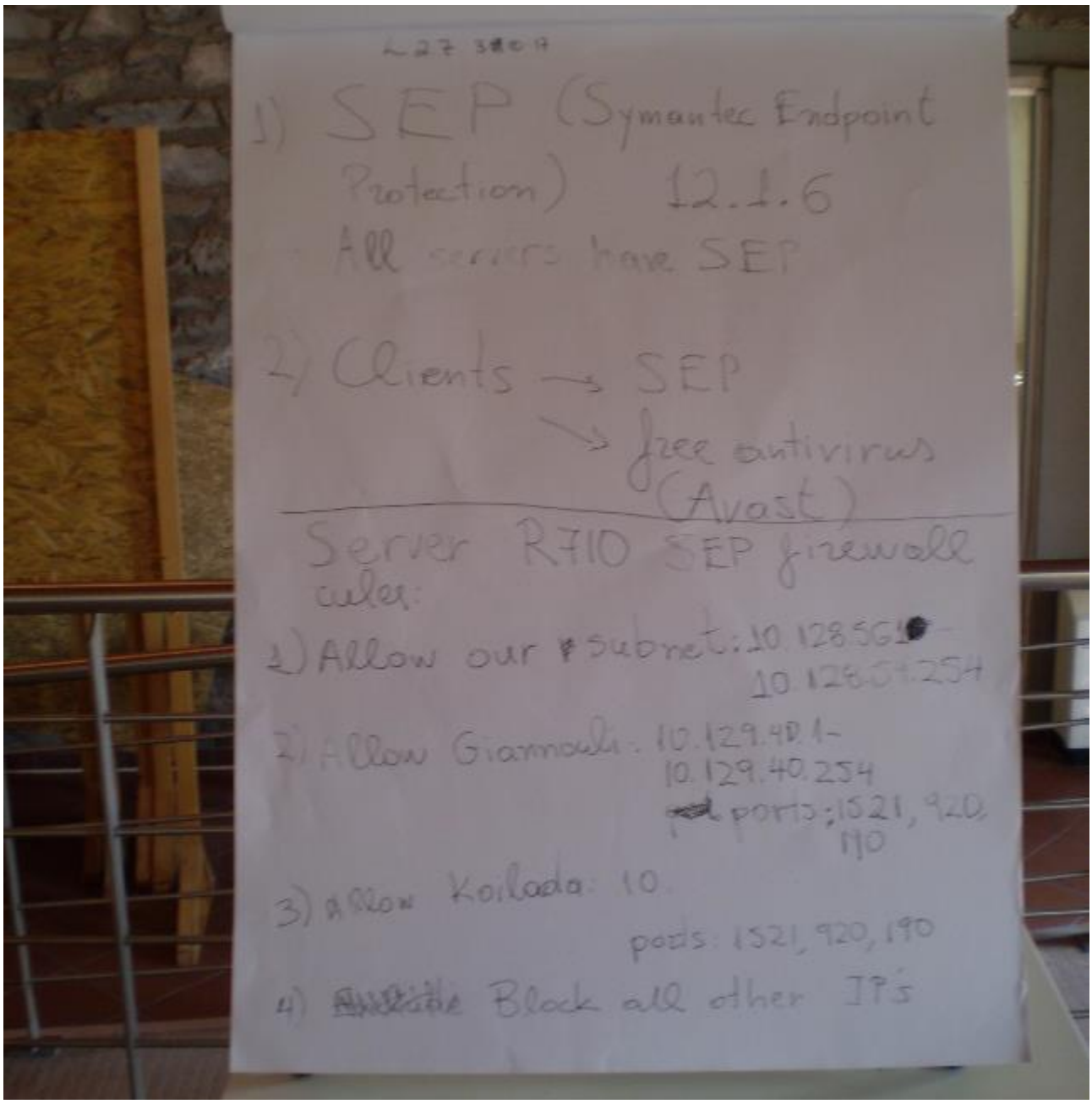


Figure 11: Day 2 RP 8

4.1.3 Day 3-5: Recap of workshop results and wrap-up

On day 3 we continued the discussions started at the end of day 2 about the security mechanisms. It was concluded that data retrieved from SEP logging mechanisms are a relevant potential information source for CS-AWARE. After that, we started to recap the workshop results by going through the main findings and revisiting the relevant rich pictures. After both the analyst team as well as the team from Larissa were satisfied that we achieved the level of analysis results we wanted to achieve during this first workshop, we released the local team from Larissa to return to their day-to-day work. The

analyst team as well as a core team from Larissa continued to process and refine the workshop results for the remainder of the week.

4.1.4 Workshop Results

Mission Critical Systems / Systems containing Sensitive Data: GENESIS, the City's ERP system is "mission critical" in two respects; it handles the City's revenues, tax collection, and tracks invoices and payments. Most importantly, it also stores and processes personal data about citizens and sensitive data about the municipality's operations. HRMS stores and processes personal and sensitive data about the City's personnel such as employee's educational background, job contract, annual leave and salary, along with taxes and deductions. It also produces reports for all management levels as well as official financial statements. These two systems both store and process personal and sensitive data and both are critical to the operation of the City. Therefore, the proposed CS-AWARE solution will seek to monitor these systems and networks.

Conclusion: In general the analyst team was satisfied with the outcome of the workshop, and that the Larissa team could be already released after three days of data gathering, after the required level of analysis detail had been achieved. The two main factors contributing to this result were the manageable complexity of systems in a mid-sized municipality, as well as the excellent preparedness of the team in Larissa. The team had familiarized themselves with the CS-AWARE project ideas as well as with the analysis methodology which allowed the analysis team to quickly achieve excellent results.
As outcomes of the workshop the analysts concluded that the most interesting connection points for CS-AWARE are monitoring on the service level, the network level, as well as monitoring existing security mechanisms. At the service level, the analysts concluded that it was only necessary to concentrate on Genesis and the HRMS. In both cases, it was established that activity could be recorded and saved to the database via built-in auditing mechanisms, meaning SQL queries could be used to capture audit information about data operations (although any personal data will need to be anonymized at source). Furthermore, similar data can be gathered from built-in database auditing mechanisms.
At the network level, the analysts came to following conclusion: Although now redundant, the Cisco 2620 gateway router was still connected to the main Linksys switch and could be used as a monitoring point for network traffic. After further investigation it was established that almost all of the network traffic could be monitored through the Cisco 2620 gateway, and that most likely built-in monitoring mechanisms (like the Cisco NetFlow protocol) can be used to gather this data.
At the level of security mechanisms it was concluded that SEP is the most relevant point of monitoring (most likely only the server deployments), and that built-in logging mechanisms can most likely be utilized to collect the relevant information.

4.2 First Soft Systems Workshop in the Municipality Roma Capitale - first iteration (16.10-20.10 2017)

The first workshop in Roma Capitale (RC) commenced on October 16th 2017. The first workshop ran for four days and due to the sheer size and complexity of the systems and network architectures, began with a series of presentations from the RC Team. These can be found in Annex 3 of this report and comprised:

Title	Content
Network Infrastructure	Overview of data & voice network
System of Public Connectivity	The network that connects Italy's Gov't Agencies

Title	Content
TETRA	RC's secure multi-access radio network
Risk Assessment	Overview of risk assessment and mitigation measures
Disaster Recovery	Overview of recovery measures
RC Data Center	Data & services management and IT security
Main Projects, Services and Contracts	Overview of RC's Department of Technological Innovation & current main projects

The visiting project team of analyst / facilitators comprised as follows:

Organization	Participant
University of Oulu	Christian Wieser
University of Vienna	Thomas Schaberreiter Veronika Kupfersberger
CARIS Research Ltd	Christopher Wills
3rd Place	Matteo Bregonzio
Cloudpartners	Kim Gammelgaard
Ancitel	Giuseppe Clementino John Forrester
Roma Capitale	Antonella Caprioli Raffaella Pullano Arianna Bertollini Giuseppe Bartoli Silvia Guglielmucci Simona Stoklin Massimiliano Rossi Massimiliano Zanchiello Roberto Massimiliani Marco Massari Luca Iezzi

4.2.1 Workshop Results

The presentations given by the RC team were very informative and an excellent summary of the systems and networks in RC. However, the visiting team of analysts were not able to harvest sufficient details from the presentations to enable them to develop a detailed understanding of the RC operation. It became evident that there was an error in the number of person months in the project plan, which had ascribed zero months to Roma Capitale for this phase of the project. This error had resulted in RC failing to appreciate the level of input that would be required of them to this work package. Some discussion took place as to how this error and misunderstanding had arisen and it was agreed that all

of the partners would participate in a telephone conference every week following the workshop, in order to find a solution to this apparent resourcing shortfall. All participants were confident that this issue could be resolved and it was discussed to schedule a second one-week iteration of this workshop in a timely manner, in order to reach the necessary level of analysis required for this phase of the project. The visiting team re-iterated the purpose of the workshop and again explained the methodology that was going to be applied, in order to analyse RC's systems. The visiting team explained that they needed participation by RC personnel in the workshops who had a detailed understanding of each and every critical system used by RC and the participation of external personnel from any external service providers.

Aside from the administrative issues discussed, at the end of the workshop six Rich Pictures (RP's) were produced that sought to describe the structure of RC's systems and networks, set against the background of the presentations given by the RC team. These can be found in Annex 3 of this report. However, there was insufficient time for the visiting team of analyst / facilitators to begin to explore the content of these RP's or to have the RC team formulate textual explanations of their RP's. In several cases, the RP's contained information that was not of central relevance to the project. All of the RP's were at very high level and contained unclear and unstructured information, much of which had already been described in the preceding presentations. Some critical services began to be identified, such as the SUET and SUAP services as can be seen in RP1, which are used by citizens for services related to building permissions. Some areas were identified which would require a second workshop in order to look at them in detail, as can be seen in RP6. SUET was seen to be an ideal candidate for CS-AWARE for several reasons: It is a relatively new service that is very well documented and therefore easier to manage in the context of a research project. Furthermore, it does not deal with the most critical data in Roma Capitale (which means that it is easier to work with the service in the context of a research project), it can however be seen as a quite critical service for the operations of Roma Capitale. For example, a substantial amount of financial transactions (fees related to building permissions) is managed by the service and a disruption would cause significant losses. A potential piloting scenario that would be within the scope of CS-AWARE was identified: It was discussed to focus on one service (e.g. SUET), and discuss all parts of Roma Capitale systems that are involved in the day-to-day operations of this service (e.g. network infrastructure, data centre, web portal, identification and authentication management, existing security mechanisms, other software and services - like databases). Furthermore, it was discussed to look closer at the centralized fleet management system that manages certain aspects of a substantial amount of RCs client machines. It was agreed that in the second workshop relevant personal from RC and from its sub-contractors for those parts of RCs systems would be participating.

By then end of the workshop all of the participants had a clear and much improved understanding of how the Soft Systems Methodology was going to be used in the systems dependency analysis, and which piloting scenario would be investigated in more detail. All that remained to be resolved was the emergent resourcing issue. The solution that was agreed was for a change request to be made to the Project Officer (PO) to exchange RC's allocation of hours from another phase of the project. This was agreed by the PO and the project coordinator, and RC produced a list of workshop participants for the second workshop.

4.3 First Soft Systems Workshop in the Municipality Roma Capitale - second iteration (11.12-15.12 2017)

Having resolved the resourcing issue, as is set out in the report on the first workshop, the second workshop in Roma Capitale (RC) commenced on December 11th 2017. The workshop ran for five days. The visiting project team of analysts / facilitators comprised as follows:

Organization	Participant
University of Oulu	Christian Wieser
University of Vienna	Thomas Schaberreiter Veronika Kupfersberger
CARIS Research Ltd	Christopher Wills
Cloudpartners	Kim Gammelgaard
Wise & Munro	Jerry Andriessen (NOTE: not present due to flight cancellation)
Ancitel	Giuseppe Clementino John Forrester

After all of the participants introduced themselves, the RC team gave an overview of SUET (presentation slides attached in Annex 4), the service that we agreed upon before the workshop to investigate closer in CS-AWARE. Chris Wills gave a short presentation about SSM and the purpose of this workshop to those participants that had not been present during the first workshop. Thomas Schaberreiter gave a short introduction to the CS-AWARE project and Christian Wieser explained the ethics and data protection requirements for this project and how personal data that may be discussed during the workshop will be handled by the project.
After the presentation, the workshop participants from RC and the suppliers were initially asked to form six teams, one for each of the following areas agreed upon during the first workshop:

Areas of Expertise	Roma Capitale Expert	External Supplier Expert
Network	Simona Stoklin	Company: Fastweb Andrea Boggio
SUET service	Andrea Quatrini Annalisa Mannucci (part time)	Company: Accenture Antonio La Malfa (other person, if necessary)
Data Center	Luca Iezzi Roberto Massimiliani (part-time)	
Security (network, balancer, security, proxy, firewall)	Massimiliano Rossi Massimiliano Zanchiello	Company: Eidemon Raffaele Conforte
Fleet Management	Ivano Ottaviani	
Web Portal	Ivan Bernabucci Mauro Melella Walter Duca (IAM)	Company: Leonardo NSR Marco Liverani

However, the RC participants decided to combine some areas therefore four teams were formed:

- Team 1 - Networks
- Team 2 - SUET & Web Portal.

- Team 3 - Data Centre and Fleet Management.
- Team 4 - Security

The teams were asked to draw a high level understanding of the systems and dependencies relating to their area of expertise, identifying mission critical systems as well as those parts of the systems that handle sensitive data. This resulted in four initial rich pictures (Team 1 RP1, Team 2 RP1, Team 3 RP1 and Team 4 RP2), all of which can be found in Annex 4 together with detailed descriptions. In the beginning of the second day the teams were asked to present their view on the RC systems, based on their rich pictures. We have seen that each team, while having a unique view on RCs systems, included many aspects of other parts of the systems that other teams had been investigating in more detail. Dependencies that had not been expressed explicitly became obvious during the discussions between the presenting team, the analyst team and the members of the other teams. The complete system overview became much clearer by combining the effort that had been done before in separate teams. This resulted in slight modifications of some of the rich pictures, and the enriched system view was included in the textual descriptions of each rich picture which the teams were asked to produce in the afternoon of the second day.
For the remainder of the workshop an additional 8 rich pictures (as well as several iterations of some of those rich pictures) were produced, detailing several aspects of the systems that the analyst team wanted to gain a deeper understanding of. Each rich picture was presented to the analysts and the members of the other teams, after which a written description of each picture was produced. Towards the end of the week the members of the original four teams combined in such a way that a detailed description of system components could be produced based on different and relevant areas of expertise. Those rich pictures and their detailed descriptions can be found in Annex 4 (Team 1 RP 2, RP IAM (together with Team 2 RP 2), Team 3 RP 2, Team 4 RP 2, Team 4 RP 3, RP Database/Application log, RP DMZ Detail).

4.3.1 Workshop Results

Mission Critical Systems / Systems containing Sensitive Data: In the first workshop in October, The following services were identified as being mission critical, either to the City or to the citizens (Annex 3 RP 6):

- Vehicle Tickets
- Building Construction Services
- Business Online Services for Enterprises (SUAP)
- Tourist Tax

In the second workshop it emerged that SUET carries some of the mission critical systems appearing above and the Identity Access Management system (IAM) (see RP IAM & Team 2 RP 2). In the presentation of the SUET system (attached in Annex 4) it emerged that SUET contains and processes sensitive and personal data, as does SUAP:

- Personal – Demographic - Census
- Urban Development - Map Databases
- Election - Polling – Projection
- Companies – Production Activities
- Local Police Authority
- Financial – Payments – Billing
- Accounting – Human Resources
- Open Data
- The Data Center manages all of RC’s data

- The Data Center provides, for example, the following services on-line Services for citizens, companies and employees
  - Civil Registry
  - Certificates
  - Tax-Related Payments
- The Data Center runs, for example, the following internal applications:
  - Accounting – Financial
  - Human Resources
  - Infrastructure
  - Payment

The above are RC's most important mission critical systems some of which contain and process sensitive and personal data. To achieve a realistic piloting scenario with the resources available to CS-AWARE, it was established that CS-AWARE will for now focus on monitoring the SUET service and it's most critical dependencies which are, as of now, the data centre, the web portal/IAM service, the relevant part of the network and security appliances.

Conclusion: At the end of the workshop the analyst team was satisfied that the required level of analysis detail had been reached. We were able to gain a good understanding of the overall architecture of RC systems and dependencies, and were able to gain a more detailed understanding of the system aspects that are the most relevant to CS-AWARE, identifying possible monitoring points for all relevant parts. As expected, the RC systems are much more complex than those that have been seen in the Municipality of Larissa, due to the extraordinary size of Roma and the number of on-line services that are provided to citizens and employees of RC. Still we were able to identify a piloting scenario that will be possible to manage with the resources available within the CS-AWARE project: It was discussed to focus for now only on one relevant critical service, the SUET service - as well as all systems it depends on. It was identified that the most relevant critical dependencies can be found within the RC data centre (where the application service as well as the relevant application database are running), the web portal together with the identity and access management system (IAM), and several security appliances (like firewalls, proxies and SIEM (Security Information and Event Management) systems) that contain information relevant to SUET operations. After gaining the information during the workshop it was decided that fleet management, while definitely an interesting point of information for CS-AWARE, will not be further investigated in the project since it does not clearly relate to the chosen piloting scenario.
On the network level it was identified that the most relevant systems are located in two parts of the network: The network infrastructure provided and operated by supplier Fastweb (e.g. Team 1 RP2) and the RC datacentre (e.g. RP DMZ Detail). The best points of monitoring any network traffic in the Fastweb infrastructure would be from the various security mechanisms (e.g. Front End Firewall Cluster, Application Server Firewall Cluster, Back End Firewall Cluster, Web Application Firewall) that are part of the network set-up - in CS-AWARE those can be used to monitor the perimeter network traffic. In the RC datacentre, several additional security mechanisms are deployed that can be utilized by CS-AWARE: A SIEM system is used to aggregate, for example, OS level logs from all virtual application servers running in RC, as well as the OS logs from the dedicated database server. Furthermore, an internal datacentre firewall as well as IPS (Intrusion Prevention System) logs can be potential monitoring points for CS-AWARE. On the application level, we gained a better understanding of the IAM system used (RP IAM), as well as how it interacts with the SUET service. The Identity manager, hosted by Fastweb as well as the access manager hosted within RC data centre could both potentially provide interesting authentication audit logs relevant to CS-AWARE. Furthermore, the SUET itself as well as the database relevant for SUET have several logging mechanisms (as shown in RP Database/Application log) that could potentially be monitored by CS-AWARE.

4.4 Discussion of pilot scenario analysis results

Following the first of three rounds of Soft System Workshops planned in CS-AWARE we could take away several generalized findings to help us to better understand LPA operations and, in preparation for deliverable "D2.4 - CS-AWARE Framework" as well as "D2.5 Guidelines and procedures for system and dependency analysis in the context of local public administrations". The first round of workshops focused on gaining an overview understanding of LPA systems and dependencies, and start to identify possible monitoring points for said systems. Based on the chosen case studies in the Municipality of Larissa and the Municipality of Rome, we were able to gain insight in the operations of a medium sized LPA as well as a large LPA. In line with our initial risk analysis we have confirmed that the main assets in LPAs are dealing with data, potentially sensitive and/or private, relating to citizens and LPA employees. While the system set-ups and configurations have been significantly different in Larissa and Rome, we have identified several generalizable aspects of the systems that handle critical data in day-to-day operations, as well as generalizable monitoring points to observe those operations. Relating to the seven OSI model layers (Physical, Data Link, Network, Transport, Session, Presentation and Application), we have found that the most relevant information for CS-AWARE will be found on levels three and four (Network and Transport) as well as on layer seven (Application):

- The database level, in which the critical data is stored. Most modern database systems have built-in monitoring and auditing capabilities that can be utilized to observe all database operations (insert, modify, delete) relating to the data observed by CS-AWARE.
- The application/service level, in which both general application/service logs and/or more specific auditing logs can be utilized to observe application/service behaviour in CS-AWARE.
- The network level, on which relevant connections and data flows can be observed. Most modern network equipment provides excellent auditing and monitoring capabilities that can be utilized by CS-AWARE to observe relevant network activity.
- Security appliances, like for example software/hardware firewalls, intrusion detection systems, SIEM systems. Those systems can provide relevant information that is already actively used to monitor information and cybersecurity related aspects in LPA systems, based on monitoring and analysing specific aspects of the systems. Such appliances usually provide logs about security incidents or suspicious behaviour that can be used by CS-AWARE to further determine the security state of the systems.

In both municipalities we have also evaluated the possibility of observing systems for centralized fleet management, which we thought may be a relevant information source for CS-AWARE (in Rome, for example, centralized fleet management could provide information about potentially 15000 client machines). For different reasons fleet management has been ruled out in both municipalities. The conclusion was that centralized fleet management is not a straight-forward process due to the vastly different set-ups the end users require, and it is still a vastly manual process. We do not see how meaningful conclusions could be derived from such a monitoring point in CS-AWARE.

In conclusion we have seen that, while the system and dependency graph that specifies all the critical assets and dependencies in LPA systems will be strongly case dependent, our initial threat assessment and analysis results strongly suggest that in the LPA context the graph of the most critical systems and dependencies can be derived by looking at the four levels we identified above.

At the end of this Section we would like to discuss our experiences with, and the effectiveness of, the analysis methodology that we have chosen for CS-AWARE: the soft systems methodology. So far we have been concerned with the first phase of the methodology, the information gathering phase that is done mainly by having the users of the system expressing their knowledge about the system and the problems they have with the system in a workshop setting by drawing rich pictures. The discussions among the workshop participants based on the pictures usually provides an environment that gradually, over several workshop sessions, creates a holistic understanding of the systems and

the socio-technological interactions. It is understood that in complex environments this type of analysis is more effective and leads to more accurate analysis results, when compared to classical analysis methods like an analyst trying to gain an understanding based on system documents, presentations and interviews. In CS-AWARE, the system and dependency analysis of each organizational system where the CS-AWARE tool is deployed is an integral part of the solution – CS-AWARE will not work without a good understanding of the socio-technological systems and dependencies, and an understanding of how we can monitor them. Only then we can set the cybersecurity situation of each individual organization in context with the wider world and provide effective cybersecurity situational awareness. One could even say that the system and dependency analysis is what makes and breaks CS-AWARE. We want to make absolutely sure that the information gathering and our holistic understanding of the pilot systems is as accurate as possible.

So how the approach hold up in practice? We have by now conducted the first of three rounds of user workshops at our piloting partners. We have seen that, if the participants of the user workshops have prepared themselves and have understood the added value of system analysis using rich pictures, this method is a powerful tool to quickly gain a common understanding of the systems and interactions, from a high level overview down to a detailed technical understanding. The right composition of participants in the user workshops is crucial. Only if representatives from all relevant organizational levels (such as managers and technicians) are present in the workshops, a complete and holistic understanding of the problem domain will be achieved. We have seen that it is essential to have stable workshop groups – those who decide to be part of the workshop need to be there for the whole duration of the analysis. In a situation where participants come and go based on their conception of when they are needed, two things will happen: First, information will be missing because the right person was not present to contribute their knowledge at the right time and second, information will be reiterated several times because a participant has not been present when something was already discussed. Both slow down the progress of the analysis considerably. We have also noticed that if the workshops are conducted in a cultural setting that does not facilitate participatory workshops, the participants do not necessarily see the benefit of this type of analysis. The willingness to engage and contribute to an interactive analysis that requires constant input and interaction from the participants is restrained. It can go as far as the participants starting to question their role in the workshop and to cease to engage completely, which of course means that the information gathering is not as effective as it could be. However, at some point, the "penny drops" and the participants begin to see that by expressing and sharing each other's tacit knowledge, a far more extensive and detailed understanding of the systems and networks emerges and is developed, than would otherwise be the case. Certainly, this was the experience in the RC second iteration workshop, when the participants began to realise that the workshop had not only enabled them to develop a better understanding of RC's systems and networks than they had before, it had also enabled them to document the entire system and its interdependencies. The final emergent benefit has been that we have arrived at an agreed joint understanding and description of the problem domain - a goal very rarely achieved, if ever, by the use of other systems analysis approaches in such a setting. The analysts have facilitated the RC participants to analyse RC's systems and networks and develop *their own detailed and holistic understanding of RC's IT operations*. The important point here is that the RC participants "own" the analysis and the outcome of it, for it is certain that with their tacit knowledge, they will have developed a much better understanding of RC's operations, than could ever be achieved by external consultants.

In summary, we have been quite happy with the results of the first round of system and dependency analysis workshops. In some aspects we achieved much better results, quicker than we had expected, while in others it took a bit longer than expected to gain a common understanding of the workshop goals, before achieving the expected results. Based on the experiences we have gained so far, we are confident that we have chosen the right approach for CS-AWARE and with some tweaks to accommodate for individual cultural aspects, we expect even better results during the second round of workshops.

Bibliography

Checkland, P. (1981). *Systems Thinking, Systems Practice.* Wiley [rev 1999 ed].

Checkland, P. (1990). *Soft Systems in Action.* Wiley [rev 1999 ed].

ENISA. (2016). *ENISA Threat Landscape Report 2016.* Online. Retrieved 2 2018, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

European Commission and High Representative of the European Union. (2013). *Cybersecurity strategy of the european union: An open, safe and secure cyberspace.* JOIN(2013) 1 final.

Europol. (2017). *Internet Organized Crime Threat Assessment (IOCTA) 2017.* Online. Retrieved 2 2018, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Karas, T. H., Moore, J. H., & Parrott, L. K. (2008). *Metaphors for Cyber Security. Sandia National Laboratories.* Online. Retrieved 2 2018, from http://www.evolutionofcomputing.org/Multicellular/Cyberfest%20Report.pdf

McAfee. (2017). *McAfee Labs Threats Report, June 2017.* Online. Retrieved 2 2018, from https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf

Annex 1

Name Name
Address Address
City, State, Zip Code
Phone
Email

00.00.0000
X
Title
XXCompanyXX
Address
City, State, Zip Code

Cyber Security Awareness Solution CS-AWARE

Dear Mrs./Mr. X,

CS-AWARE is a cyber security awareness tool for local public administrations that is being developed by academic and industry partners within the context of an EU Horizon 2020 project - www.cs-aware.eu.

The tool aims to facilitate the generation of cyber security awareness in the non-expert community. This will be achieved through monitoring each participating organizations' systems. Monitoring will be set both within the context and against the background of various cyber intelligence sources. The outcome of this will be the creation of CS-awareness tool that has the following features:

Automatic incident detection and visualization
Information exchange with, for example, national and EU level NIS authorities
System self-healing mechanisms

The tool will also focus on collecting information from public sources. However, the accuracy of the awareness alerts that are thereby produced would be improved immensely by the contribution of trustworthy professional expertise such as yours. Moreover, such external inputs would also assist in the ability of the tool to recognize emergent patterns in cyber security challenges.

The supplementation of cyber security data with any information relating to cyber-attacks and threats (be they in real-time or historical in nature) that you or your organization could make available to us would be of immense benefit. It would greatly improve our ability to provide as accurate and timely awareness alerts as possible.

Therefore, ***XXSWProductXX*** would make an excellent extension to the current list of information sources. Next to improving our cyber intelligence data, this cooperation would also benefit ***XXCompanyXX*** through additional European partnerships and an opportunity to increase social and academic publicity.

If this first introduction to CS-AWARE has piqued your interest and you require any further information, let us know.

We, the CS-AWARE consortium, are convinced of the mutual advantages of this proposed cooperation. We look forward to receiving what we hope will be your positive response.

Best regards,

Prof. Juha Röning (Coordinator, CS-AWARE)

Annex 2

Systems description for CS-AWARE

The table below contains a system description that was provided to CS-AWARE in preparation for the first user workshop. It contains detailed descriptions of the services present in the Municipalities of Larissa, Elassona and Kileler.

	Unit 1 – General Description
Organization Name	Municipality of Kileler
Details	Total Population (Census 2011): 20.854 Number of employees: 86
Information systems – Applications	**Accounting and Financial Services** **Payroll and HR Management** **Civil Register and Elections Catalogue** **Document Signing and Archiving System** **Diavgeia** **Diavgeia Posts** **Register Office** **Digitized Register Office Actions** **Technical Projects** **E-procurement** **Central repository for financial data reporting** **City's Website**
IT Infrastructure	Local Servers. Windows clients/terminals Syzeyxis VPN network for phone, mail, and Internet services.
	Unit 2 – Description of Information Systems
Accounting and Financial Services	
Description	This is the city's ERP to manage their revenues and expenses. It handles supplier and citizen information, tracks invoices and payments. It organizes tax and debt collection. It produces reports for all management levels as well as official financial statements. ERP operates on the server – client architecture and supports all major RDBMS solutions.
End Users	18
Manufacturer	OTS

Hosting	Self-hosted
Interoperability	ERP interacts with HR, WBS, Diavgeia, Central repository for financial data reporting
Case of systems unavailability	In case of the system's non-availability, citizens and companies are unable to pay fees and taxes, suppliers are unable to get paid for the goods and services they have provided and end users have no access to financial data in any way whatsoever. Administration cannot also report with financial or statistical data as required by Central Government. Systems recovery should have taken place within the following business day. For the duration of no availability, the organization has no failover options and any transactions taking place must be logged in written and then entered to the ERP.
Backup	End customer retains all recent binaries and executables and maintains automated daily backups of their database(s). Database backups are also maintained to a NAS Server for redundancy.
DSR Plan	No DSR
Business Continuity Plan	There is no Business Continuity plan.
Payroll and HR management.	
Description	This is the city's Human Resources Management System. This information system helps the city to manage their personnel. It handles employees' personal information such as educational background, job contracts, leaves, salaries along with taxes and deductions. It also produces reports for all management levels as well as official financial statements. HR operates on the server – client architecture and supports all major RDBMS solutions. Currently it works on the Oracle RDBMS.
End Users	2
Manufacturer	OTS
Hosting	Self-hosted

Interoperability	HR interacts with ERP, the central repository for financial reports and several insurance funds.
Case of systems unavailability	In case of the system's non-availability, end users are unable to enter any kind of information about their employees and cannot calculate payroll, fees and taxes. There is also no access to financial data. Administration cannot also report with financial or statistical data as required by Central Government nor can it send data to insurance funds. Systems recovery should have taken place within the following business day. For the duration of no availability, the organization has no failover options and any transactions taking place must be logged in written and then entered to the HR.
Backup	End customer retains all recent binaries and executables and maintains automated daily backups of their database(s). Database backups are also maintained to a NAS Server for redundancy.
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Civil Register and Elections Catalogue	
Description	This is the city's Civil Register Management System. This information system helps the city to register and maintain their citizens' family status. It handles citizens' personal information such as date of birth, gender, marital status, family members, past marriages and so on. It also produces certificates for official use. Civil register operates on the server – client architecture and supports all major RDBMS solutions. For end customer, it works on the Oracle RDBMS. It also employs an application server within its premises to send data to or receive data from a central database repository that resides on the Interior Ministry. **Elections Catalogue.** The elections catalogue is a subsystem of the Civil Register Management system. It helps end customer to organize lists of citizens that can take part in national and/or local elections.
End Users	10

Manufacturer	OTS
Hosting	Self-hosted
Interoperability	Civil Register interacts with the National Civil Register Information system that collects data from all municipalities across the country.
Case of systems unavailability	In case of the system's non-availability, end users are unable to enter any kind of information about their citizens or update their status. They is also no option of producing official certificates. The system's normal functionality highly depends on the network communication with the Interior Ministry. Any network failures can result to an inconsistent state of data between the local and the central database. Systems recovery should have taken place within the following business day. For the duration of no availability, the organization has no failover options and no transactions can take place. In case of network failures, only local transactions may happen.
Backup	End customer retains all recent binaries and executables and maintains automated daily backups of their database(s). Database backups are also maintained to a NAS Server for redundancy.
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Document Signing and Archiving System	
Description	This Information system's main purpose is to sign and archive all incoming and outgoing documents. It assigns a single number per document for future reference, archives it to an auxiliary database and can optionally digitize the document itself. The system operates on the n – tier architecture and supports all major RDBMS solutions. Currently it works on the Oracle RDBMS. It employs an open source application server within its premises and users operate on their browsers.
End Users	6

Manufacturer	OTS
Hosting	Self-hosted
Interoperability	The system interacts with ERP and Civil Register
Case of systems unavailability	In case of the system's non-availability, end users are unable to sign or archive any documents. No single number can be assigned to certificates issued by Civil registry or documents produced by the ERP. Systems recovery should have taken place within the following business day. For the duration of no availability, the organization has no failover options and no transactions can take place.
Backup	End customer retains all recent binaries and executables and maintains automated daily backups of their database(s). Database backups are also maintained to a NAS Server for redundancy.
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Diavgeia	
Description	Diavgeia is considered one of the backbones of public administration. Each document issued by a public entity that needs to have a legal force must be posted to this information system. It is installed to one of the central government's datacenters and all public entities access it via the internet. End users access the portal with their browsers.
End Users	1
Manufacturer	OTS
Hosting	Centrally Hosted
Interoperability	The system interacts with Diavgeia Posts, ERP
Case of systems unavailability	In case of the system's non-availability or the lack of access to the internet, end users are unable to post documents. Systems recovery, i.e. the internet, should have taken place within the following business day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration related issues syzefxis helpdesk is available via phone or email.

DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Diavgeia Posts	
Description	This IS has been developed by OTS to help end customer to speed their posts to Diavgeia IS. Instead of accessing the portal, end users can upload the document they need via this information system. Systems recovery should have taken place within the day. For the duration of no availability, the organization can access the portal via the internet.
End Users	n/a
Manufacturer	OTS
Hosting	Self-hosted
Interoperability	The system interacts with ERP to have documents uploaded instantly as well as with diavgeia's main site.
Case of systems unavailability	In case of the system's non-availability or the lack of access to the internet, end users are unable to post documents. Systems recovery, i.e. the internet, should have taken place within the following business day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. He also retains all recent binaries and executables and maintains automated daily backups of their database(s). Database backups are also maintained to a NAS Server for redundancy.
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Register Office	
Description	This a nationwide Information System that each municipality uses to register actions, i.e. births, deaths, marriages and dissolution of marriages. It is being maintained by the Interior Ministry and users of the register office access it via the internet.
End Users	7
Manufacturer	Interior Ministry
Hosting	Centrally hosted

Interoperability	Interoperated with public register
Case of systems unavailability	In case of the system's non-availability or the lack of access to the internet, end users are unable to register any actions. Systems recovery, i.e. the internet, should have taken place within the day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration related issues, syzefxis helpdesk is available via phone or email.
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Digitized Register Office Actions	
Description	This a nationwide Information System that each municipality use to reference actions originally registered to books, i.e. births, deaths, marriages and dissolution of marriages. The Interior Ministry are maintaining it. Users of the register office access it via the internet.
End Users	7
Manufacturer	Interior Ministry
Hosting	Centrally hosted
Interoperability	Interoperated with public register
Case of systems unavailability	In case of the system's non-availability or the lack of access to the internet, end users are unable to register any actions. Systems recovery, i.e. the internet, should have taken place within the business day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration related issues, syzefxis helpdesk is available via phone or email.
DSR Plan	No DSR.

Business Continuity Plan	There is no Business Continuity plan.
Technical Projects	
Description	This application operates on the server – client architecture. Data is stored in SQL Server
End Users	5
Manufacturer	ACE HELLAS
Hosting	self-hosted
Interoperability	n/a
Case of systems unavailability	Systems recovery should have taken place within the following business day.
Backup	n/a
DSR Plan	No DSR
Business Continuity Plan	There is no Business Continuity plan.
Central register for e-procurement and e-procurement management system for public sector entities	
Description	This is a centrally managed e-procurement management platform for all public-sector entities. End customer is obliged by law to insert and manage all contracts it signs above a certain monetary value.
End Users	6
Manufacturer	Ministry of Development
Hosting	On the ministry's datacenter
Interoperability	n/a
Case of systems unavailability	In case of the system's non-availability or the lack of access to the internet, end users are unable to register any actions e-procurement. Systems recovery, i.e. the internet, should have taken place within the following business day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration, related issues, syzefxis helpdesk is available via phone or email.

DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
Central repository for financial data reporting	
Description	A centralized information system that operates on the Interior Ministry. End customer prepares its financial data reports (accounting, HR, projects) and uploads them to the central repository for further processing. Alternatively, the Ministry's employees may pull data from municipalities upon request. Data is transferred over the syzefxis VPN network and via an application server which operates within its infrastructure.
End Users	n/a
Manufacturer	Interior Ministry
Hosting	On the ministry's datacenter
Interoperability	None
Case of systems unavailability	In case of the local system's non-availability, that is database and/or the application servers, or the lack of access to the internet, end users are unable to upload financial data reports. Systems recovery, i.e. the internet, should have taken place within the following business day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration related issues, syzefxis helpdesk is available via phone or email. End customer also retains all recent binaries and executables and maintains automated daily backups of their database(s).
DSR Plan	None
Business Continuity Plan	There is no Business Continuity plan.
City's Website	
Description	This is the city's website. It provides information about the city to visitors and citizens. The IS also provides mail services to the city's employees.
End Users	1 site administrator

Manufacturer	Entropia
Hosting	Cloud hosted
Interoperability	n/a
Case of systems unavailability	In case of the system's non-availability, citizens have no access to the municipality's website. Also, the administrator cannot update the website.
Backup	n/a
DSR Plan	No DSR.
Business Continuity Plan	There is no Business Continuity plan.
	Unit 3 – Description of IT infrastructure
Local Servers	
Description	End customer administers a local computer room to support their daily back office operations. Local servers operate the Windows operating system and have both Oracle and SQL server software to store and retrieve data. Open source application server software, such as Jboss, Tomcat and alfresco are also employed to support the n-tier architecture wherever applicable. Hyper-V is the preferred hypervisor for virtualization.
Administrators	1
Case of systems unavailability	In case of the infrastructure's non-availability due to outages or the lack of network access, end users are unable to get access to locally stored data. Infrastructure recovery, i.e. the servers, network, internet, should have taken place within the day. For the duration of no availability, the organization has no failover options.
Backup	End customer maintains copies of their databases backups to a NAS Server. No other Infrastructure related backups are in place.
DSR Plan	No DSR
Business Continuity Plan	There is no Business Continuity plan.
Syzeyxis VPN network	

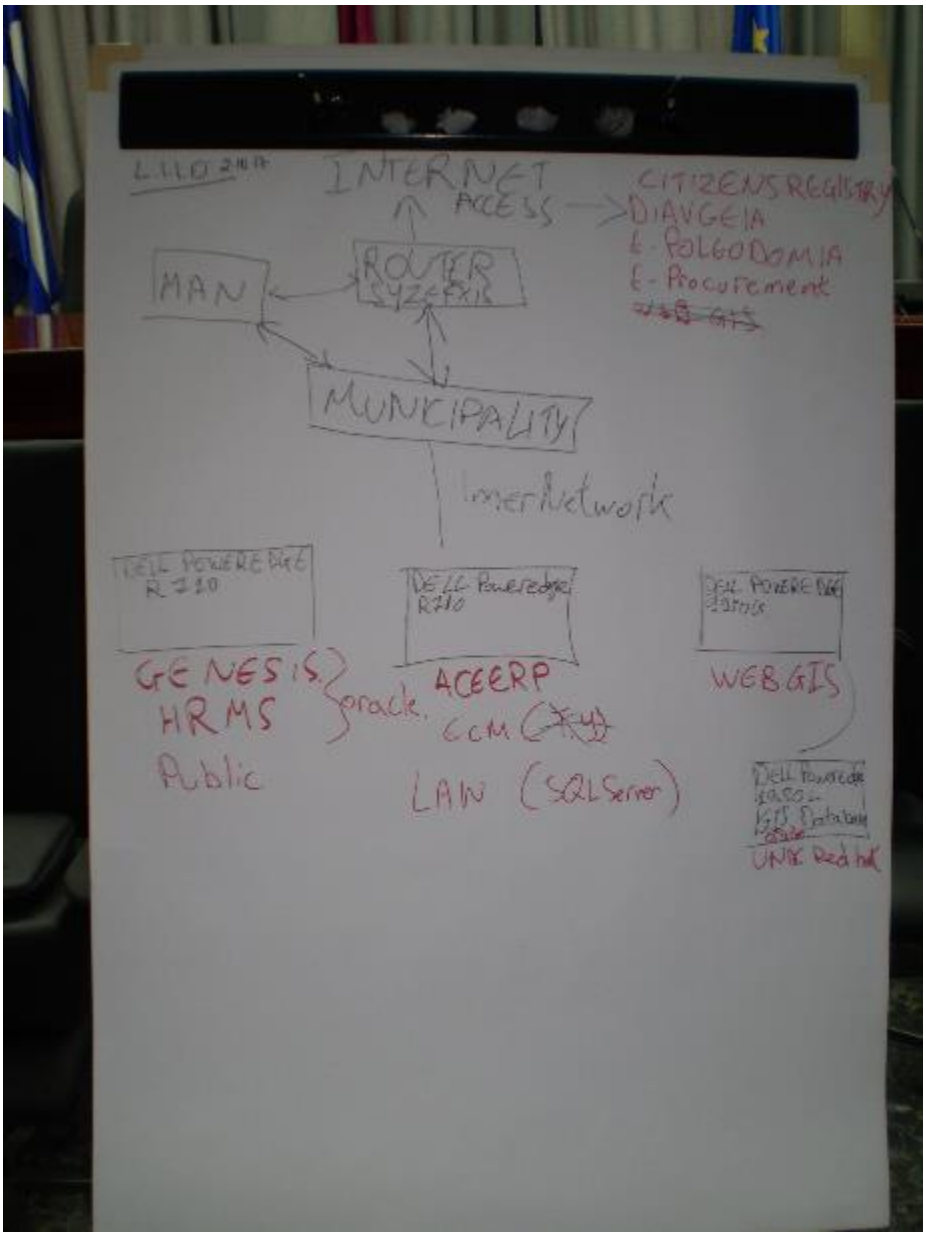
Description	End customer utilizes the Syzeyxis VPN network for its phone, mail and internet services. All levels of local and central government communicate over this VPN network.
Manufacturer	OTE
Administrators	1
Case of systems unavailability	In case of the network's non-availability, end customer has no access to mail, internet and phone services thus its communication is severed. Network recovery should have taken place within the day. For the duration of no availability, the organization has no failover options.
Backup	End customer must ensure that network devices are operating normally and there are available spare parts. For network configuration, related issues, syzefxis helpdesk is available via phone or email.
DSR Plan	No DSR
Business Continuity Plan	There is no Business Continuity plan.

Rich Pictures and Commentary

Day 1 RP1

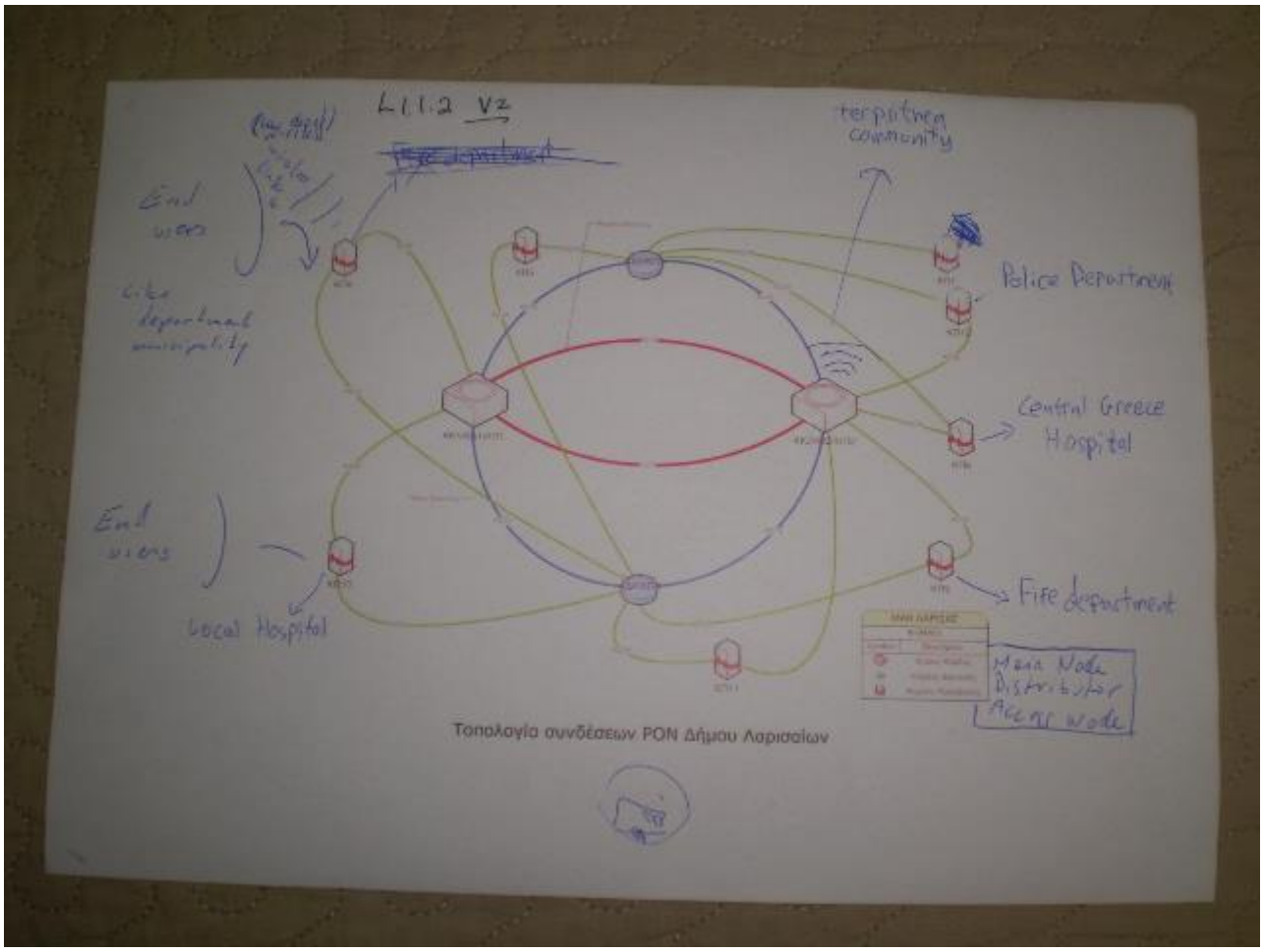
In this picture we see a general presentation of the municipality's network, main servers, and main services. As we see the only route to the Internet is via the main router, the one shown as "Router Syzefxis". This router is connected both to the Metropolitan Area Network (MAN) and the main Town Hall. Inside the Town Hall there are three main servers:

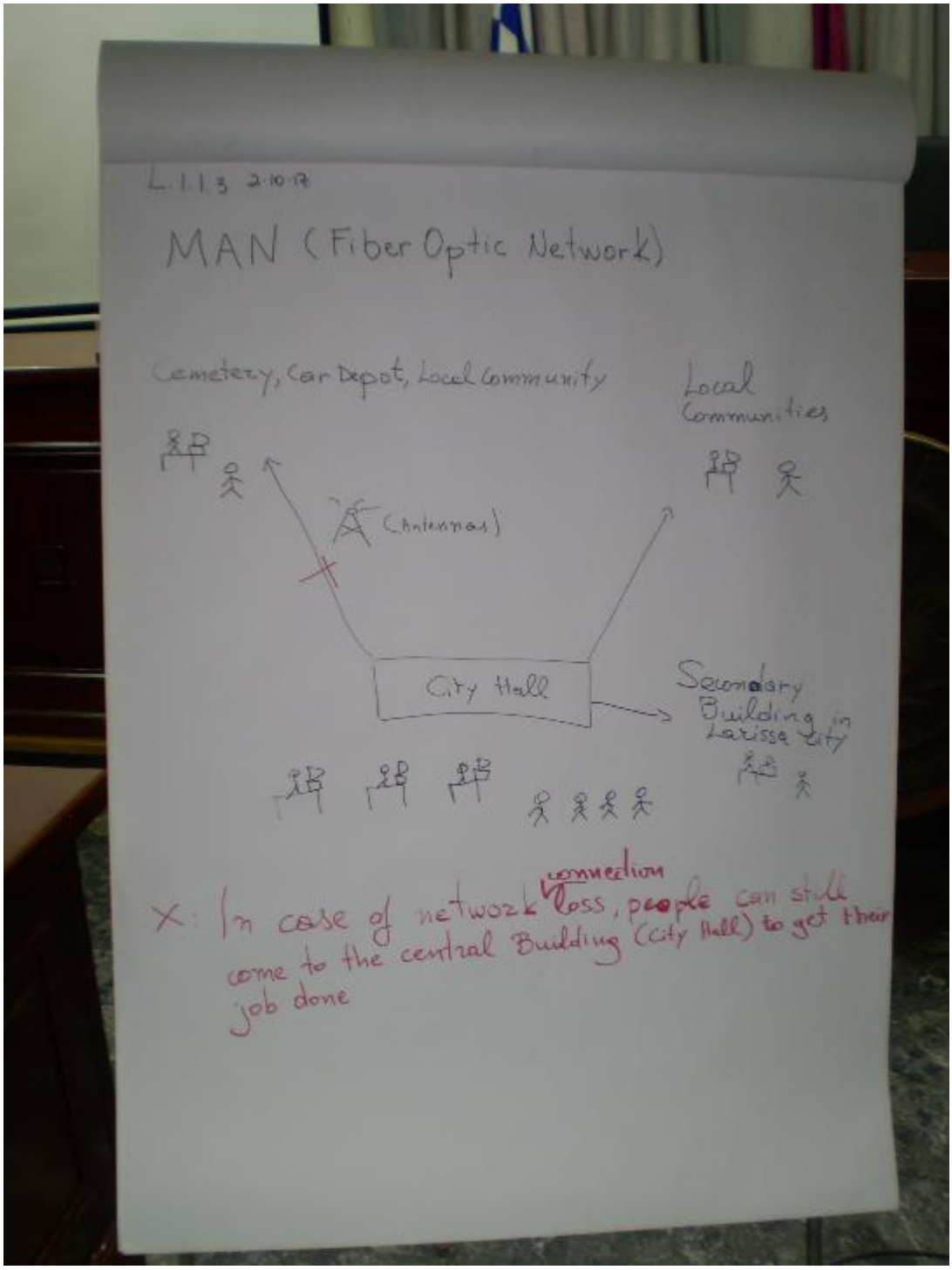
- The R710 that hosts the Genesis, HRMS and Public applications. The Oracle database is set up here to collaborate with Genesis and HRMS
- The R530 that hosts the ACE-ERP, ECM and LAW applications.
- The 2950G that hosts the WebGIS. GIS oracle database is hosted to another server, the 2950L that runs on UNIX red hat. Other services that are shown in the Internet level are provided and hosted by the interior ministry, and they are web based.



Day 1 RP 2 and 3

In RP's 2 & 3 we can see the whole Metropolitan Area Network. The MAN is a fibre optic network with some wireless interconnections. We can see that there are two main nodes, four distributors (two of them hosted in the same room with main nodes) and access nodes. In each access nodes we have end users like a cultural centre or a municipality's secondary building. The MAN belongs to the municipality, although other services are using it (permissions are provided by our department) in order to connect their buildings or connect to their main service. So through the MAN the two hospitals of our city are connected, the fire department is connected with its main service and the police department is connected to other services.



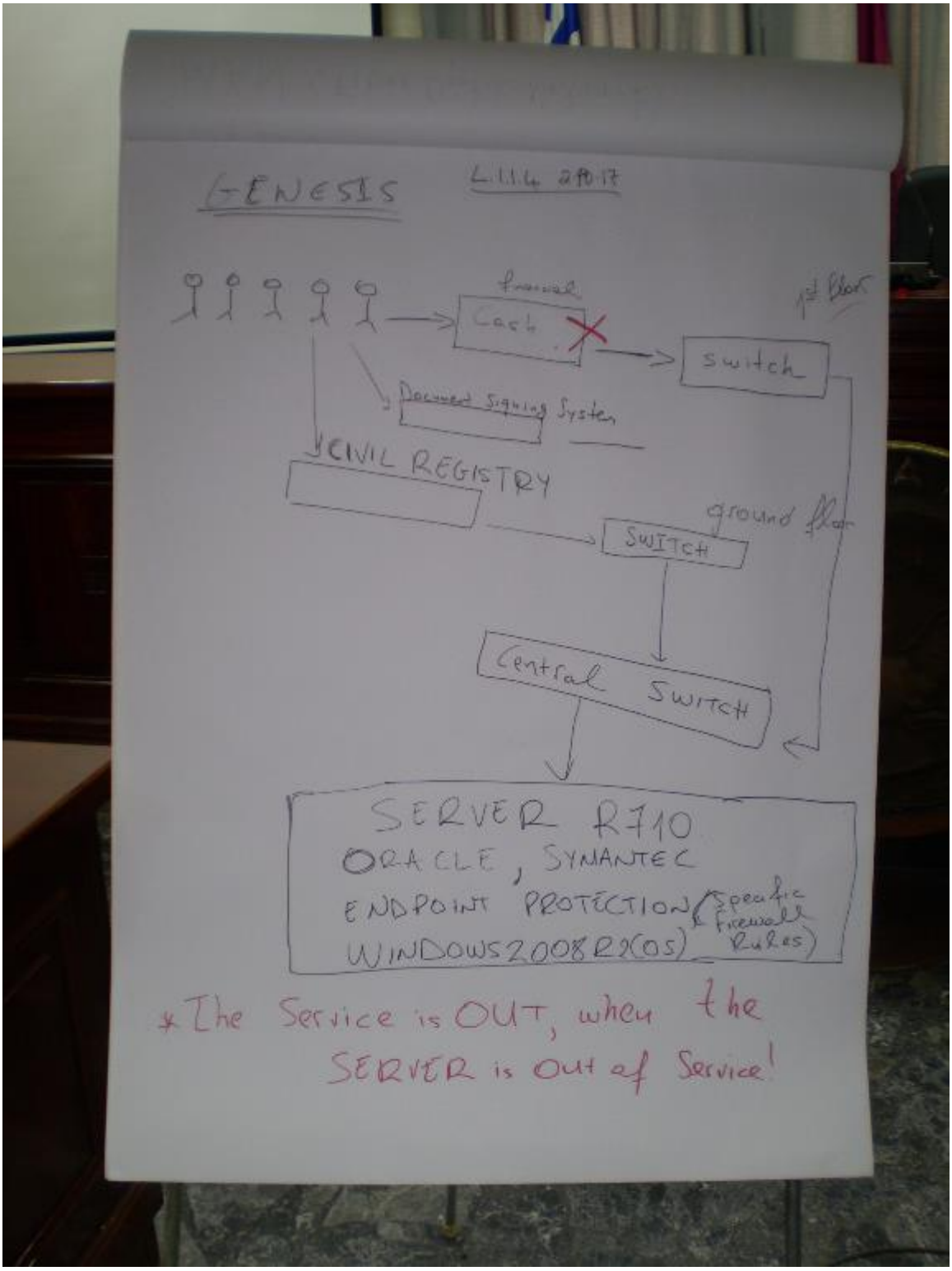

L.I.S 2.10.17
MAN (Fiber Optic Network)
Cemetery, Car Depot, Local Community
Local Communities
(Antennas)
City Hall
Secondary Building in Larissa City
X: In case of network connection loss, people can still come to the central Building (City Hall) to get their job done

Day 1 RP 4

This is the City's ERP to manage municipality's revenues and expenses. It handles supplier and citizen information, tracks invoices and payments. It organizes tax and debt collection. It produces reports for all management levels as well as official financial statements.
Genesis-users are located:

- At the municipality's main building (ACCESS NODE: ΚΠ6)
- At the car depot department (ACCESS NODE: ΚΠ6)
- At the cemetery department (MAN NODE: ΚΠ3)
- At the green spaces department (ACCESS NODE: ΚΠ12)
- At the department of Athletic, Culture and Social Services (ACCESS NODE: ΚΠ5)
- At the local communities' buildings (Terpsithea (ACCESS NODE: ΚΠ2), Giannouli- Falani (through Government VPN), Koilada (through Government VPN))

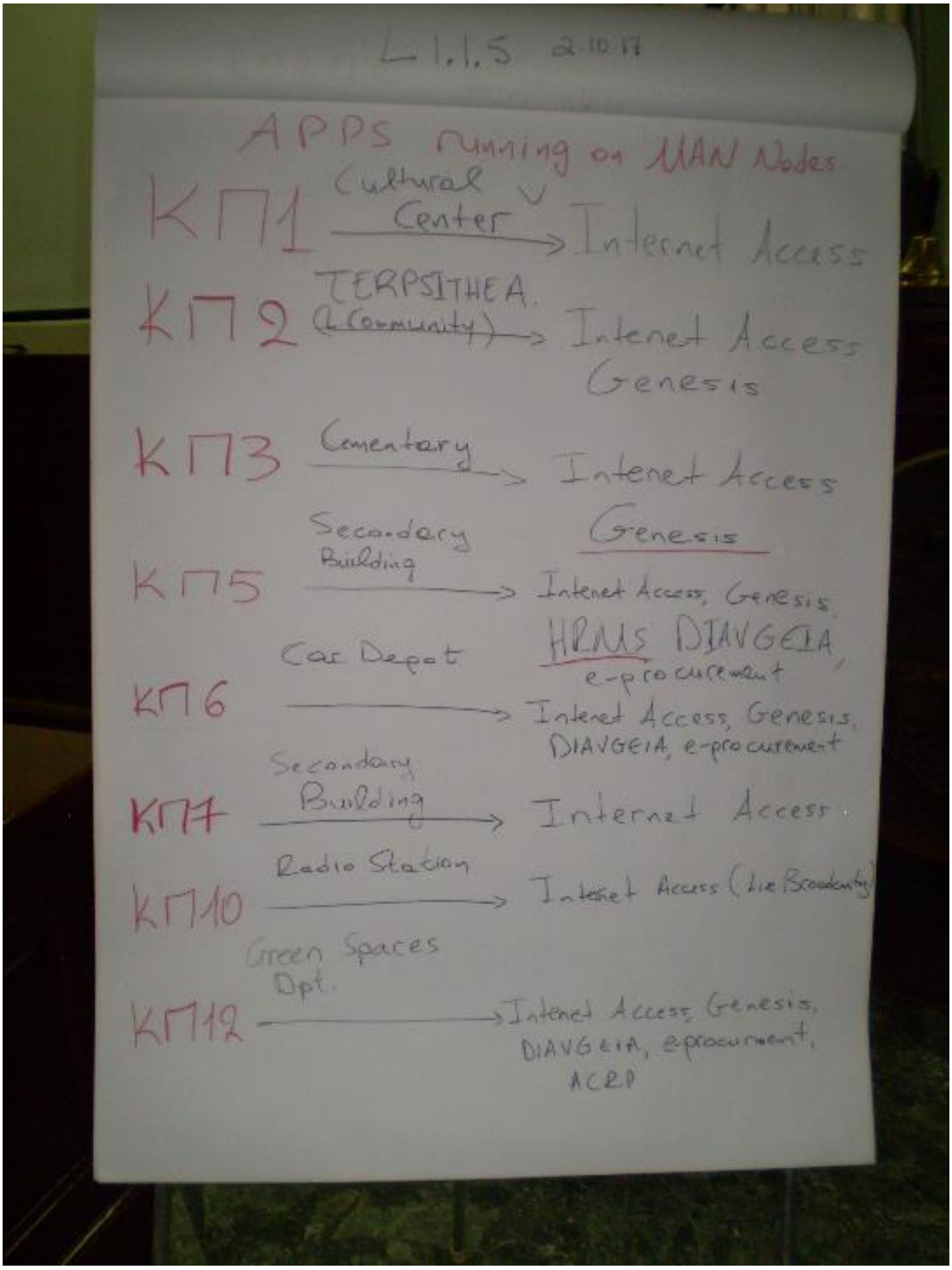
Genesis operates on the Dell Power Edge R710 server (Windows 2008 R2 Enterprise SP1). On the users' PCs the Genesis "client" is installed.
In the municipality's main building, Genesis-users belong to departments (offices) that are placed in different floors of the building. For example, the cash registers, the revenues department and the document-signing department are located at the first floor while the civil registry is found at the ground floor. Each floor's PCs are connected to a switch. All these switches are connected to a switch (Main switch) that is placed at the municipality's computer room.
Larissa's citizens carry out their transactions by coming to the municipality or to all the other spots mentioned above. Payments can also be carried out via web banking. So far, there is no other way citizens can have access to Genesis data (e.g. through municipality's portal or alternative platforms). In case of the system's non-availability, end users are unable to "run" Genesis. This implies that no transactions can be completed and system's recovery must take place promptly.


GENESIS
Lille 2017
Cache
Switch
Secured Signing System
CIVIL REGISTRY
SWITCH
Central Switch
SERVER R710
ORACLE, SYMANTEC
ENDPOINT PROTECTION
WINDOWS2008R2(OS)
Specific Firewall Rules
* The Service is OUT, when the SERVER is Out of Service!

Day 1 RP 5

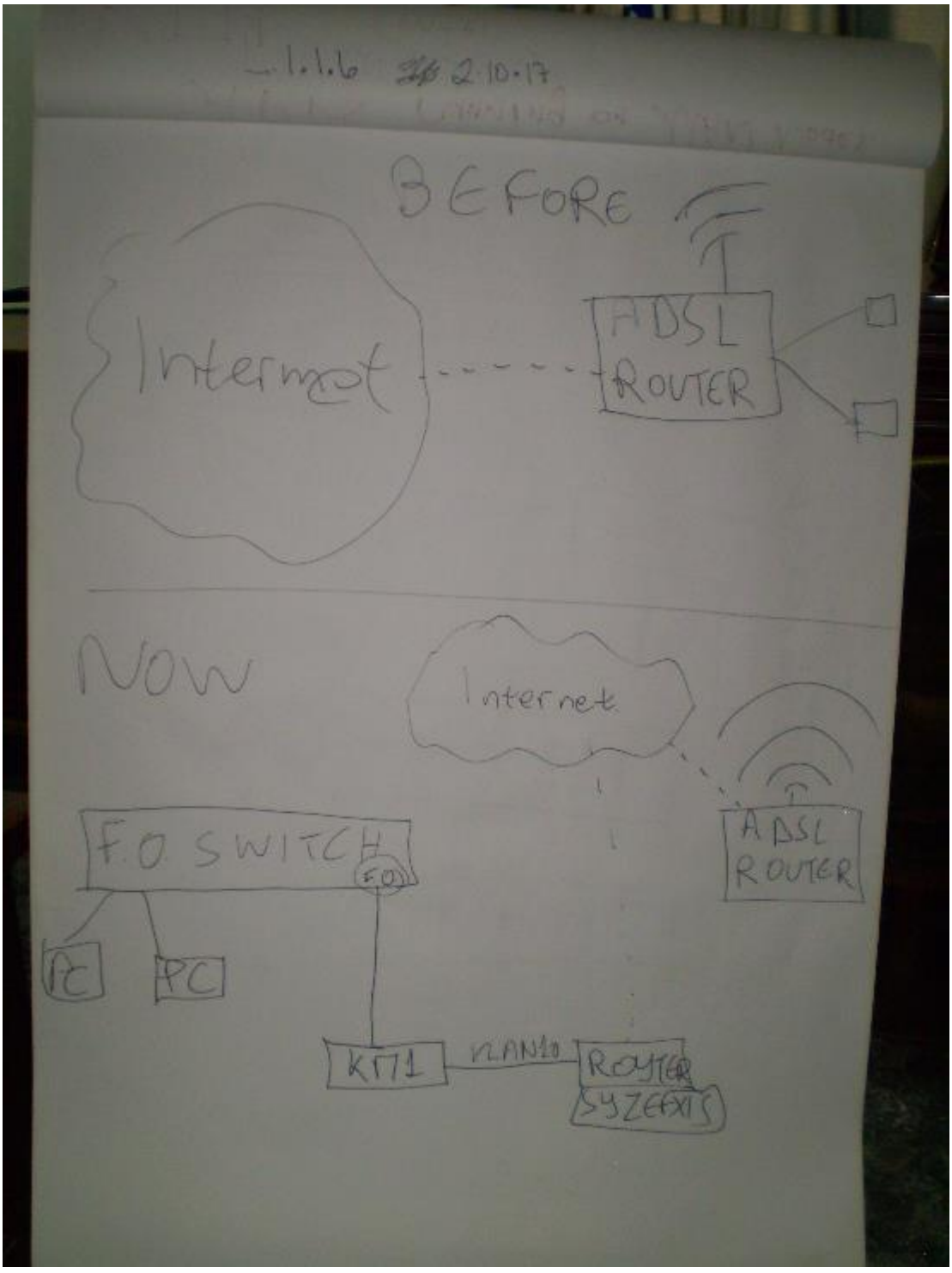
In this picture we can see the nodes of the MAN network where the various departments of Larissa's municipality are providing services, and what services are provided.
In access node 1 (ΚΠ1), a building that hosts a cultural center and provision services is connected in order to have only Internet access (through syzefxis router in the City Hall).

- In access node 2, the local community of Terpsithea is connected, in order to have Internet access and connection to the Genesis r710 server.
- In access node 3, the cemetery is connected, in order to have internet access and connection to the Genesis r710 server.
- In access node 5, a secondary building is connected, in order to have Internet access and connection to the Genesis and HRMS r710 server.
- In access node 6, the car depot is connected, in order to have internet access and connection to the Genesis r710 server.
- In access node 7, a secondary building is connected, in order to have Internet access.
- In access node 10, a building that hosts the municipality's radio station is connected, in order to have Internet access.
- In access node 12, green spaces department is connected, in order to have internet access, connection to the Genesis r710 server and connection to the ACE-ERP r530 server.


L.1.1.5 2.10.17
APPS running on MAN Nodes
ΚΠ1 Cultural Center → Internet Access
ΚΠ2 TERPSITHEA. (Community) → Internet Access Genesis
ΚΠ3 Cementary → Internet Access
Genesis
ΚΠ5 Secondary Building → Internet Access, Genesis,
ΚΠ6 Car Depot → HRMIS DIAVGEIA, e-procurement
Internet Access, Genesis, DIAVGEIA, e-procurement
ΚΠ7 Secondary Building → Internet Access
ΚΠ10 Radio Station → Internet Access (via Broadcast)
ΚΠ12 Green Spaces Dpt. → Internet Access, Genesis, DIAVGEIA, eprocurement, ACRP

Day 1 RP 6

In this picture we can see the situation in a building, that hosts cultural and providence services, before and after the MAN connection. Before we connect this building to our MAN, there was an ADSL line that was connecting two PC's to the Internet and there was an "open" Wi-Fi connection for the visitors. Now that the building is connected to our MAN, we set up a F.O. switch in order to connect these two PC's and the fibre. All the traffic goes through that switch to the distributor and then through the F.O. switch in the City Hall and then via the router Syzefxis to the Internet. The old ADSL line is maintained in order to provide Wi-Fi Internet access to visitors.

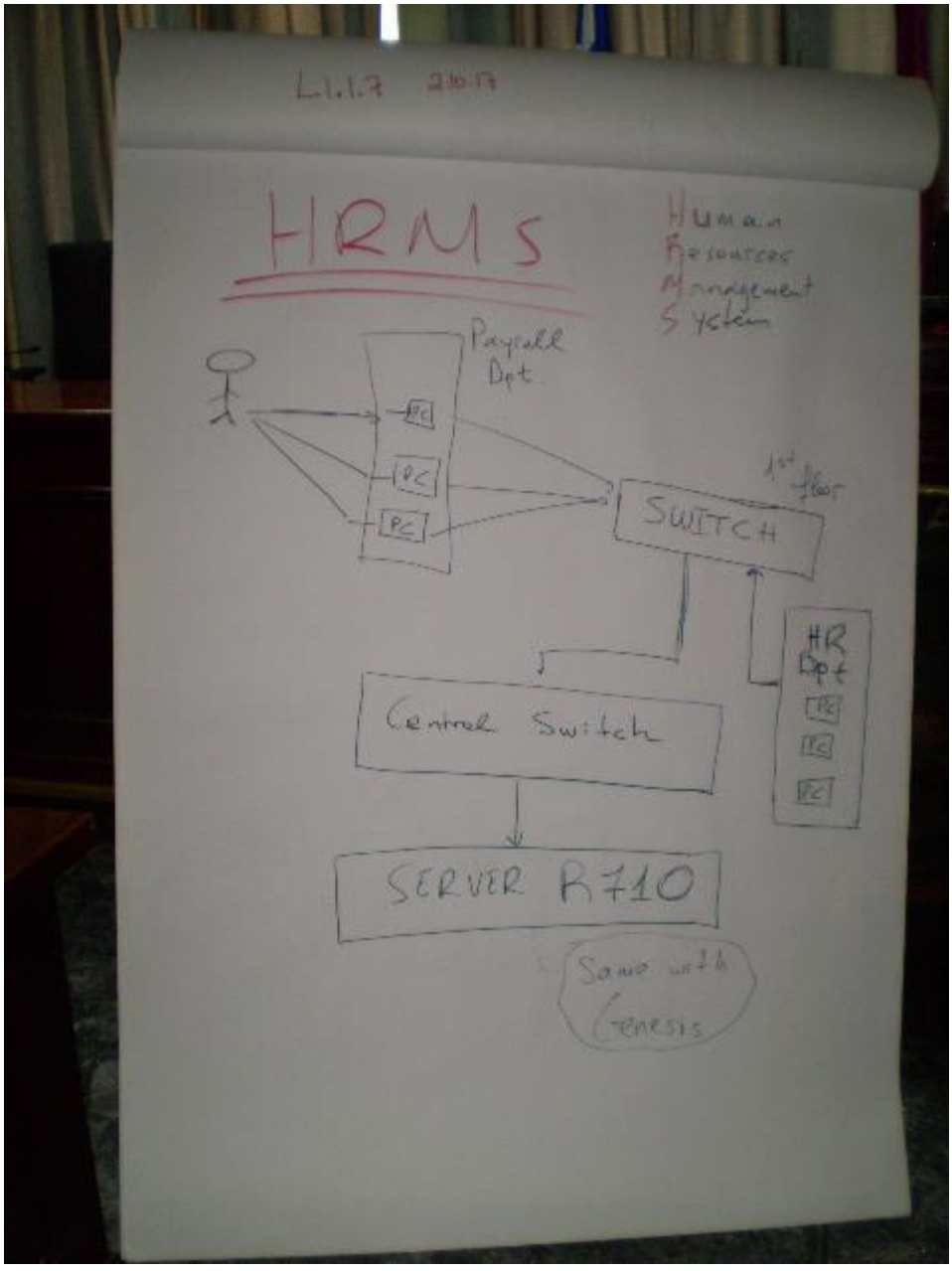


Day 1 RP 7

This is the city's Human Resources Management System. This information system helps the municipality to manage its personnel. It handles employees' personal information such as educational background, job contracts, leaves, salaries along with taxes and deductions. It also produces reports for all management levels as well as official financial statements. HRMS operates on the Dell Power Edge R710 server (Windows 2008 R2 Enterprise SP1). On the users' PCs the HRMS "client" is installed.

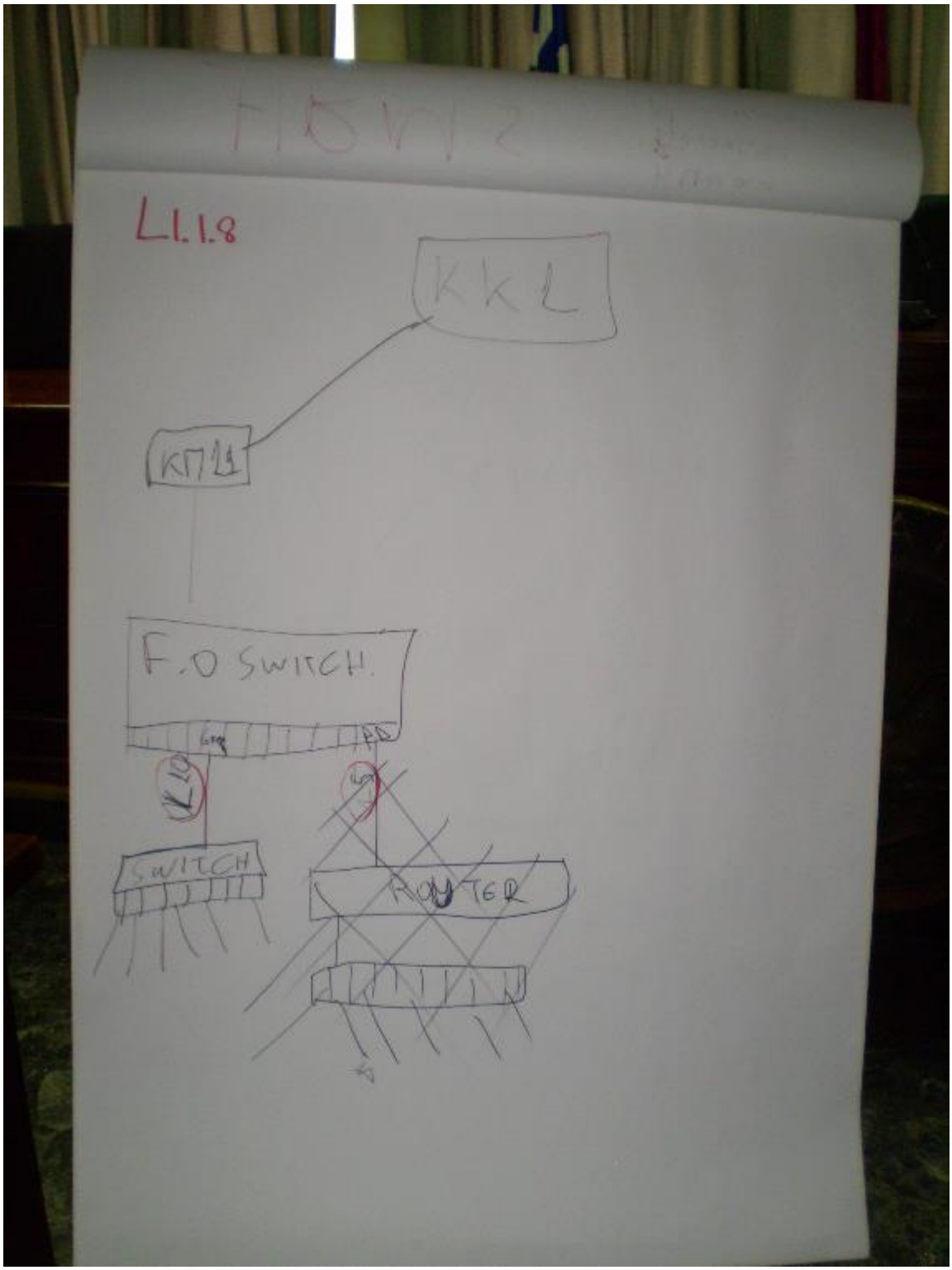
HRMS users are located at the municipality's main building (ACCESS NODE: ΚΠ6). They are employees of the department of payroll and the department of human resources. The network infrastructure is similar to the one mentioned above (Genesis case). Users' PCs are connected to the floor's switch and through the Main switch to the R710 Server. There is no other way employees can have access to HRMS data (e.g. through municipality's portal or alternative platforms).

In case of the system's non-availability, end users are unable to enter any kind of information about their employees and cannot calculate payroll, fees and taxes.



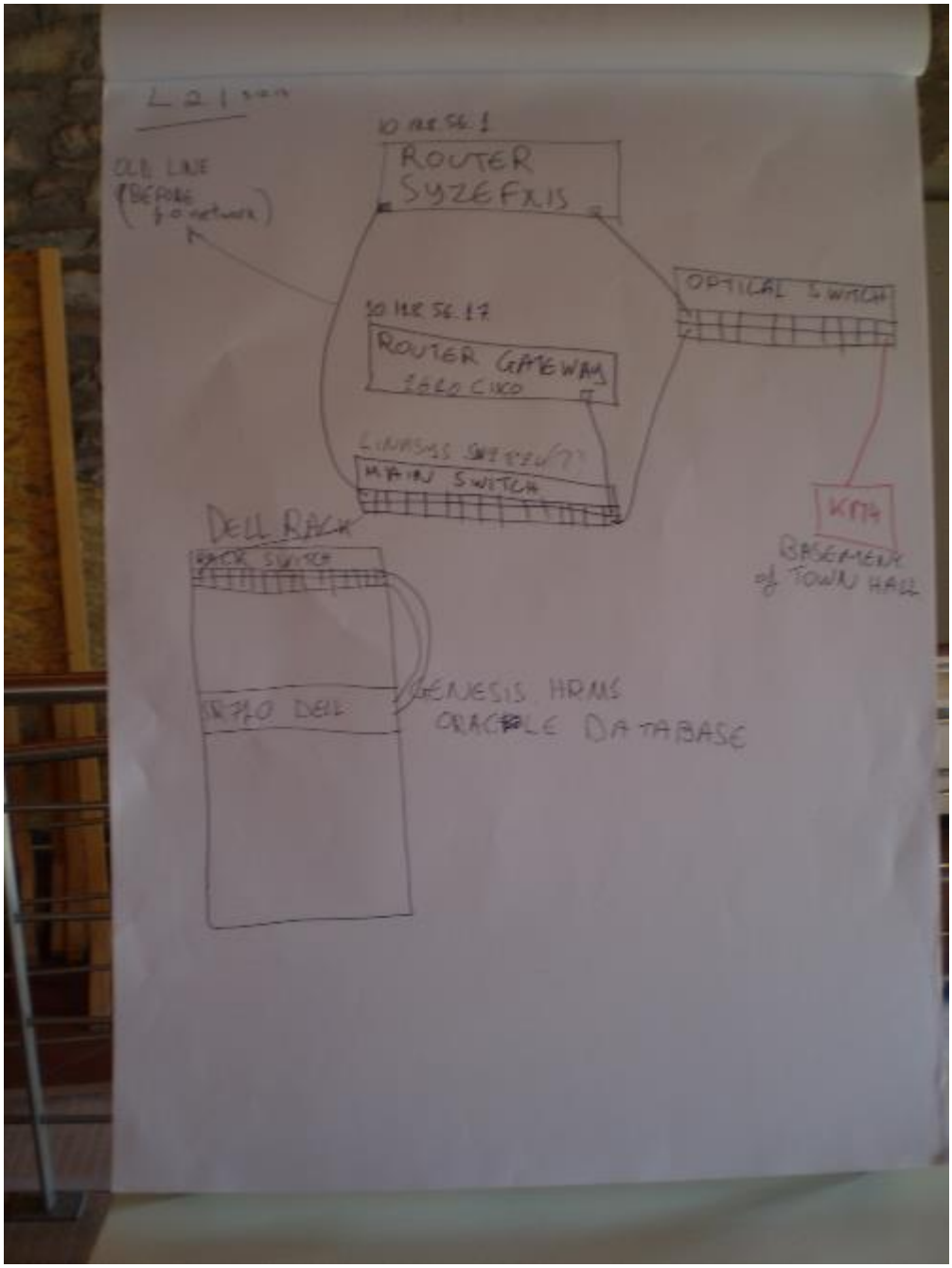
Day 1 RP 8

In this picture we can see an example of the MAN network, from the central node 1 to the end user. So from central node 1 (KK1) a fibre optic cable goes to access node 12. There a fibre optic third layer switch takes over to separate the different users. One for example is the department for green spaces which connects through vlan10 with the city hall. One other user is the police department through a different vlan.



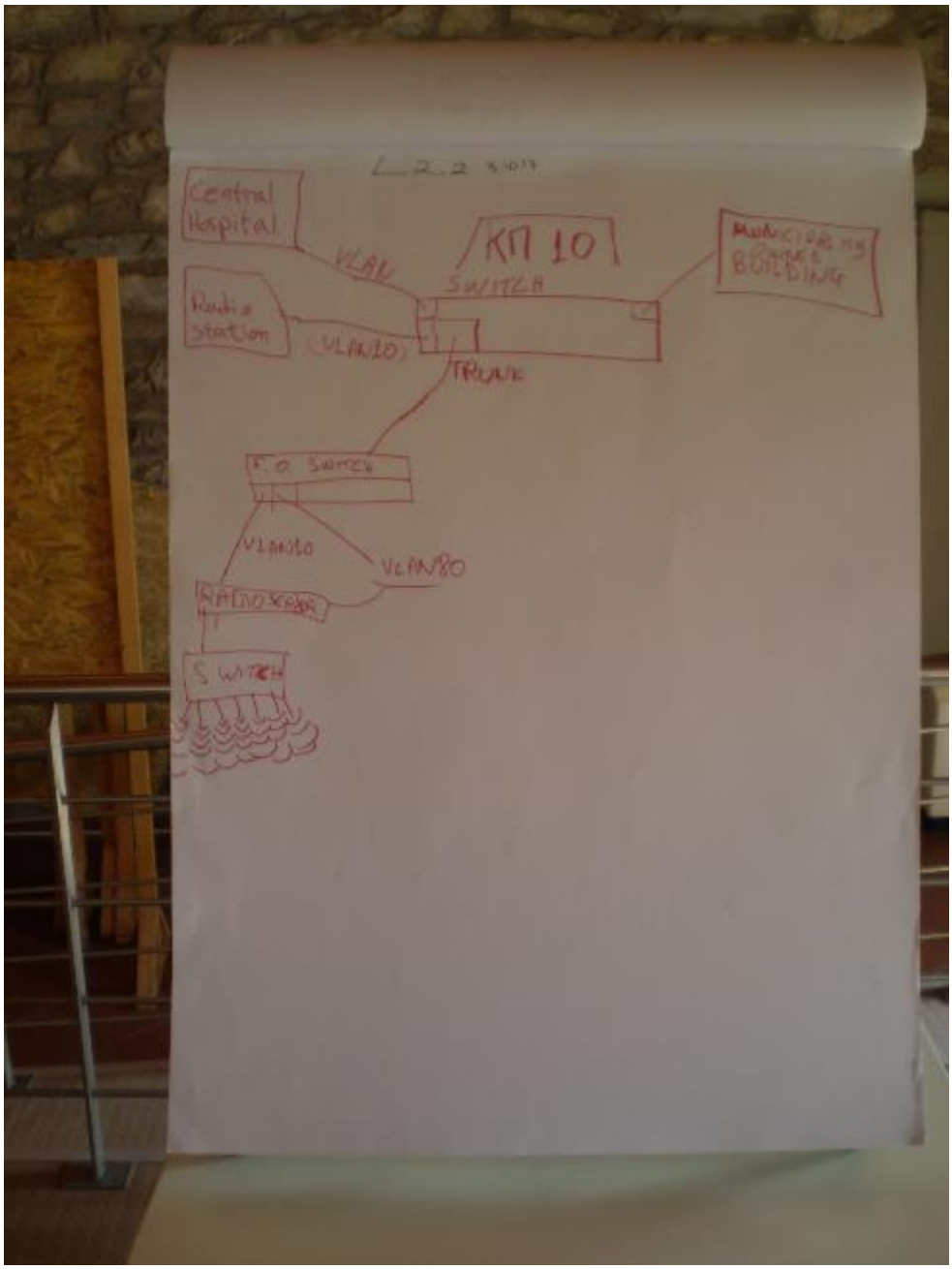
Day 2 RP 1

In this slide we can see how the intranet is connected with the MAN, with the Internet, and goes deep into our servers, which is host into the city hall. A fibre optic switch connects the whole MAN network to the main Syzefxis router, and to our Main switch both. So if a user from outside the city hall (from a different MAN node) wants access to the Internet, then the only way is to reach node 4. The connection then is going through the fibre optic switch to the Main switch and then to the ONLY Gateway router. This Gateway router is the only router that can connect an end user to the SYZEFXIS router, to the Internet. So every end user has to reach the Gateway router in order to access either the Internet or the intranet. This is the gateway we will try to monitor. The Main switch connects all the server racks and the intermediate switch inside the city hall. Before we establish the MAN network, we had not the fibre optic switch. We had a connecting cable from the Main switch directly to the SYZEFXIS router.



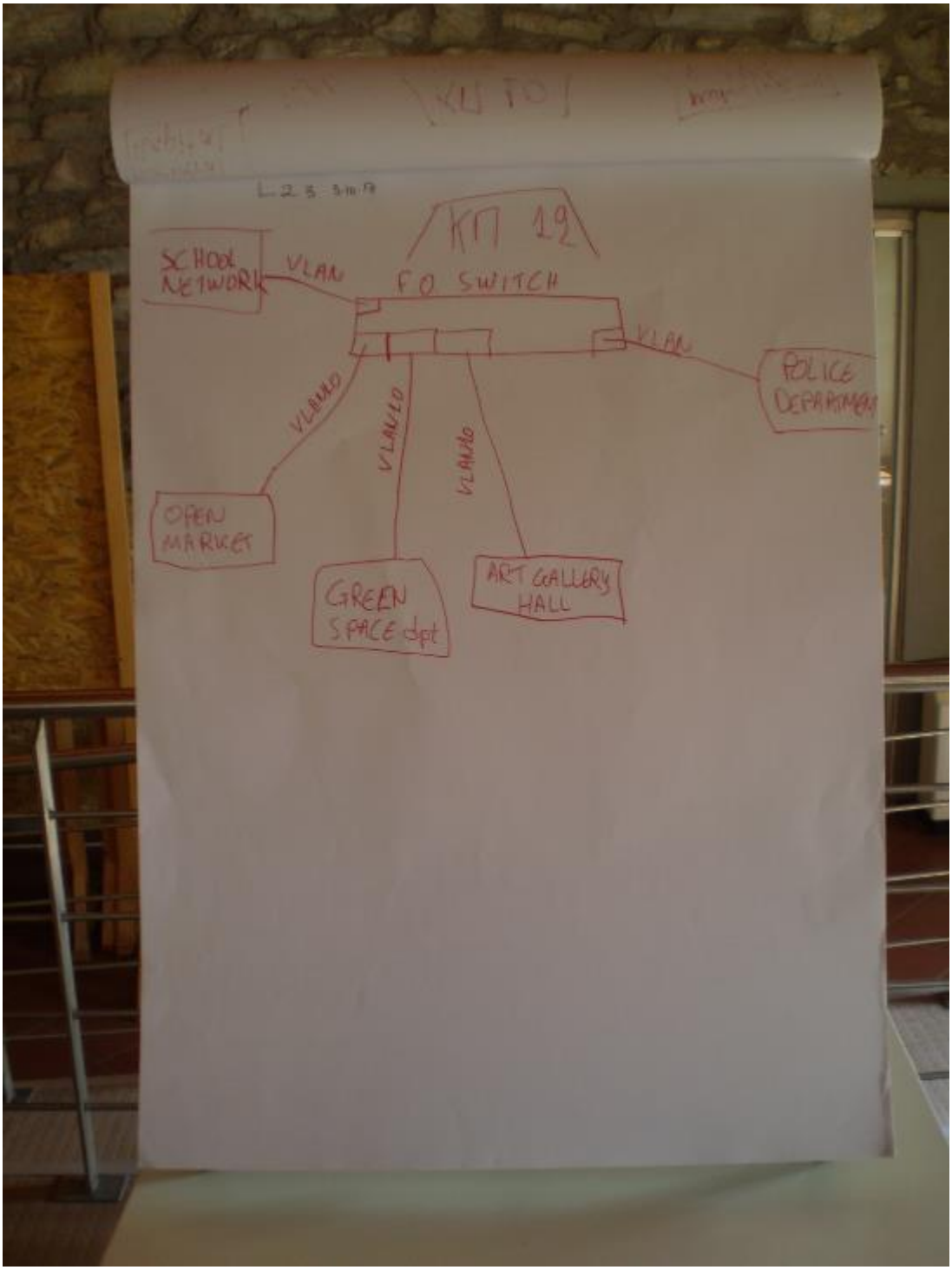
Day 2 RP 2

In this picture we can see the situation in access node 10. There is the fibre optic switch that separates ends users. In this switch is attached the Central Hospital through its own vlan. Another user is the municipality's radio station and connects with vlan 10. There is another building hosting municipality's services that connects through vlan 10 also. As we can see there is a port in the switch that is set up as trunk. This means that allows multiple vlans to pass through. So we have vlan 10 and vlan 80 through this port. This is because, in the building that hosts this end user (Mill of Papas) we want to have both the municipality network (vlan 10) and a free open Wi-Fi network, that is provided through vlan 80 to all MAN in order to possible establish to an end user a free Wi-Fi for visitors. As shown, the whole network in this building is wireless. Access points all over the building are broadcasting both networks. The vlan 10 network requires authentication and uses encryption. The authentication is control through a "radius server", a server set up to control access using user's tables and time restrictions.



Day 2 RP 3

In this picture we can see the situation in access node 12. We want to make clear that in every node we use a fibre optic switch to connect each user to the MAN network. There is a different configuration for each interface that has to do with which vlan can pass through the specific interface. So we have a different vlan for the "school network" (not a municipality service), the "open market" (a municipality service), department for "green spaces" (a municipality service), "art gallery" (a municipality service), the "police department" (not a municipality service). All these users although they are connected to the same physical device, they communicate only with the vlans their interface allows them.



Day 2 RP 4

Our main server is a Dell Power Edge R710 server (IP: 10.128.56.24, computer name SR710), Windows server 2008 R2 Enterprise SP1. It hosts our main database, an Oracle database, version 11g. Oracle client (from version 8i to version 11g) is installed in most client PC's. TCP/IP (Internet Protocol) is used to connect and to communicate with the database (Client and server communication). The default port for this communication is **port 1521**.
The **Listener** is a named process that runs on the Oracle Server, awaiting requests from Clients to connect to the Instance (it "listens" port 1521). All information is kept in **Listener.log** file. (I must apologise for my mistake in slide L2.4, I wrote License.txt instead of Listener.log). In Listener.log each field is delimited by *. This is the format:

(timestamp)*(connect info)*(protocol tcp/ip , host, port)*(SID)*(return value)
1) **(timestamp)** : The date and timestamp of the log entry.
2) **(connect info)** : The connect string used by the client.

SID: The Oracle System IDentifier (in our case OTA).
PROGRAM: The name of the program issued by the client.
HOST: The host name from which it came (in our case Full Computer Name).
USER: The Operating System UserID of the user that issued the command. In other words it is just the Windows login name, so it is not personal data and doesn't need to be anonymised.

3) **(protocol tcp/ip , host, port)** : The protocol related information used by the client

PROTOCOL: The protocol that the client has used to connect (in our case tcp).
HOST: The IP address of the client machine.
PORT: The port number established by the listener. (Note: It's not the port number to which the listener is listening, so this is not especially interesting to us)

4) **SID)**: The Oracle System IDentifier (in our case OTA).
5) **(return value)** : A successful connection returns 0 and a failure connection returns oracle error code.

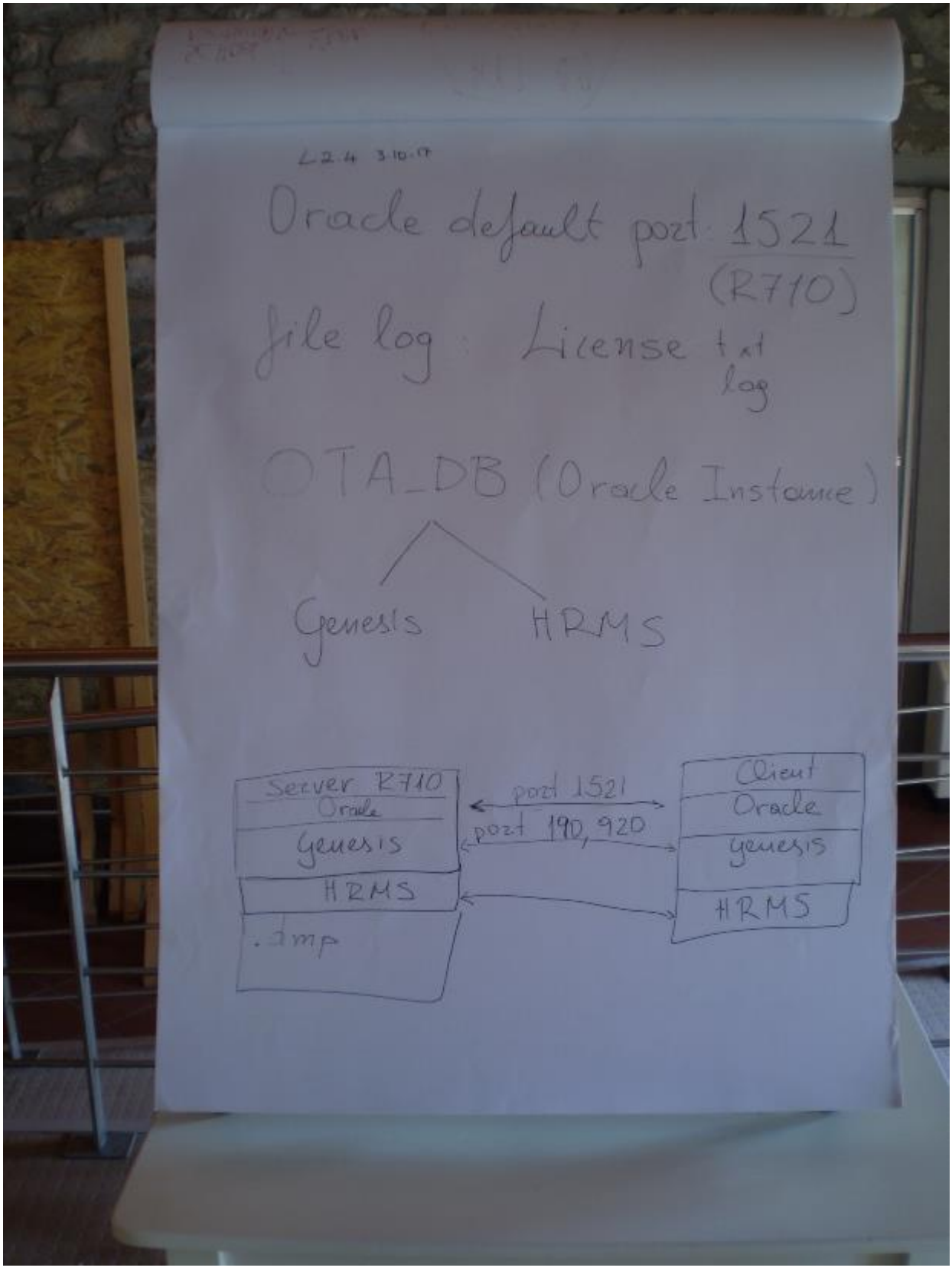
The Oracle database instance name is **OTA_DB** (Oracle System IDentifier, SID=OTA). There are two (2) schemas under OTA_DB:

1) (S92111) that includes the tables, indexes, views etc of our "Integrated System for Local Administrations" named GENESIS. It includes Accounting and Financial Services, Civil Registry etc.

2) (SHR), that includes the tables, indexes, views etc. of our "Human Resources" software named HRMS.

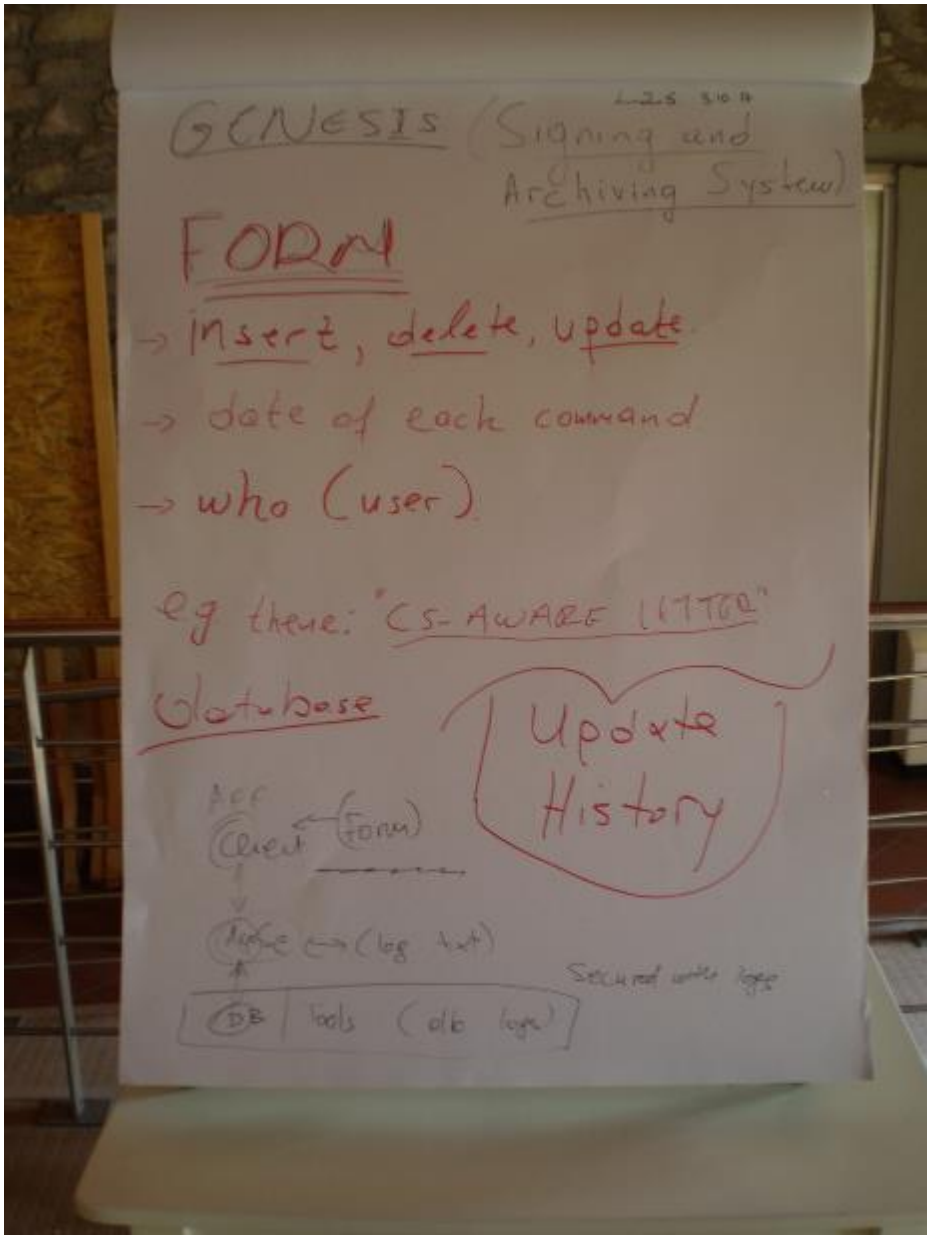
These two software packages (Genesis and HRMS), are developed by SingulaLogic S.A., a Greek software vendor. GENESIS client application connects to **server port 920** (in server SR710) in order to communicate with Genesis' Application Server (SAS server). SAS server can produce a log file with all the sql questions and procedures that SAS server executes after a Genesis client's request. Each question or procedure is related to a Genesis username. The log file gets bigger very quickly, so we keep SAS server logging deactivated. GENESIS client application connects to **server port 190** (in server SR710) in order to communicate with Genesis' Client Object Server. Object server is responsible for Genesis client updates. The physical files of our database are **.dbf** files.

Every day we create **.dmp** files (backup files of our database created with “exp” oracle command). We backup of all those files daily into tapes.



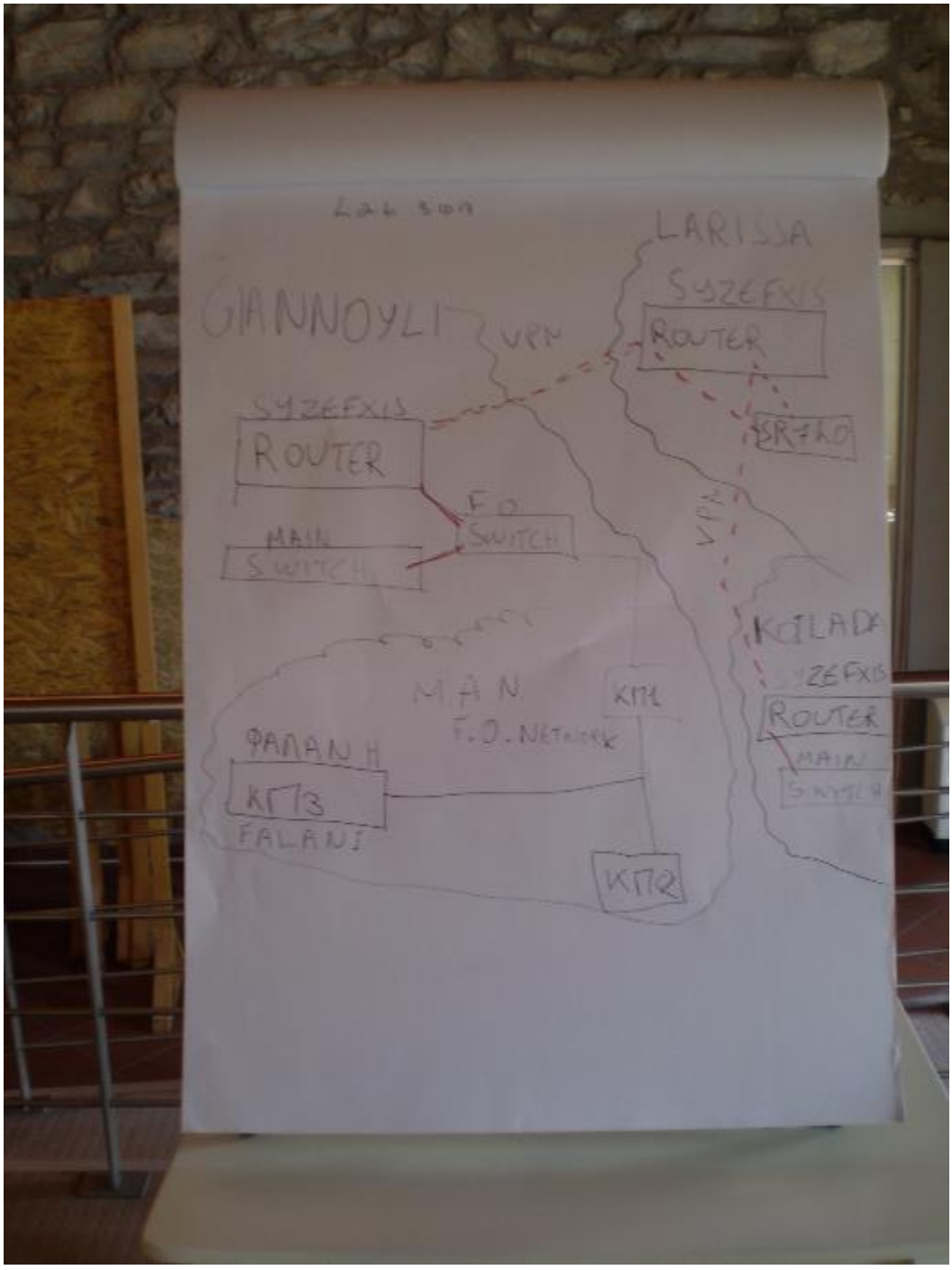
Day 2 RP 5

Genesis contains a group of financial applications that help the municipality manage its' revenues and expenses. These inner apps (modules), are executed by different users, all situated in the spots that are presented in "**DAY1, SLIDE4".** In order to monitor users' activity, an extra module has been developed, called "**Modifications' history".** Each Genesis module has its own "Modifications' history" form. In this form, the user can "ask" the database in order to search the database about 3 types of actions: insert, delete and update. The result is a list of records that shows when (date) the action occurred and who (user) committed it. The user can also set these criteria (date range, user) so as to focus his search. Moreover, in the case of the "update" action, the user can see both the old value and the new value of the field that has been updated. "**Modifications' history"** is a tool that allows simple Genesis users to execute queries and get results in an understandable way. In some Genesis modules, users can export these results as .xls or .csv files. Administrators, on the other hand, have additional access to the Oracle database (instance name: OTA_DB), its tables and views (schema: S92111) and can retrieve information by using tools like SQL Navigator.



Day 2 RP 6

In this picture we can see that except Larissa, both Giannouli and Koilada have their own SYZEFXIS routers in order to go out to the internet. Before 2011 Giannouli and Koilada were different municipalities, and had their own infrastructure Giannouli even has its own fibre optic MAN. After 2011, Kallikratis plan was applied, and Larissa consumed these smaller municipalities. Now, if a user from Giannouli wants internet access, then he is directed to Giannulli's SYZEFXIS router; but if he wants to communicate with our server in Larissa's city hall then he is directed through his SYZEFXIS router to Larissa's SYZEFXIS router via a VPN network that is established between Larissa, Giannouli and Koilada in order to have this interconnection.

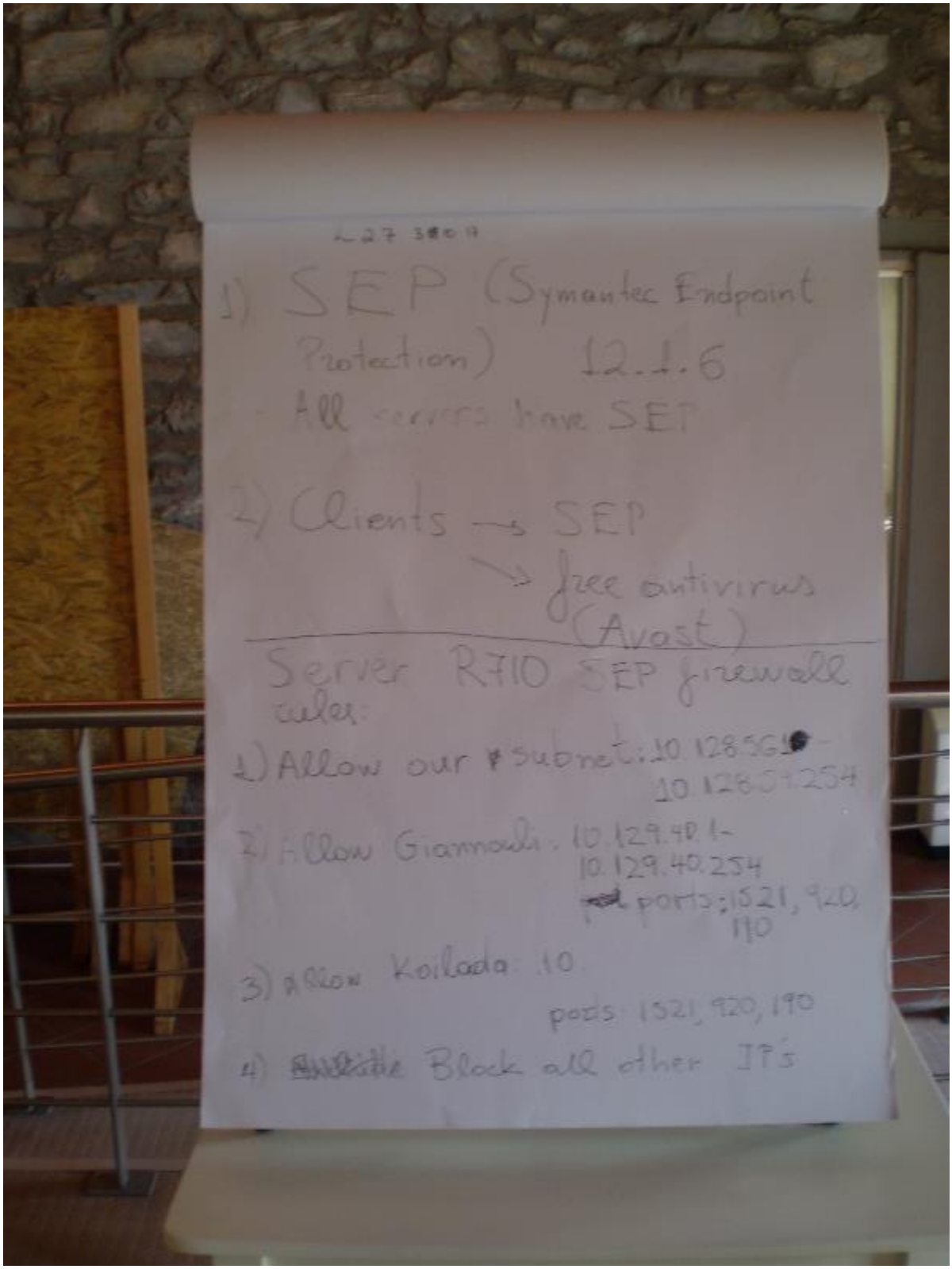


Day 2 RP 7

All PC's and servers have up to date antivirus protection programs, purchased or free. Every year we pay for the renewal of the maintenance of the purchased antivirus software. All servers have **S**ymantec **E**ndpoint **P**rotection (SEP) version 12.1.6 installed, including our main server SR710. PC‘s have either **S**ymantec **E**ndpoint **P**rotection (SEP) version 12.1.6 or free antivirus software (mostly Avast) installed.

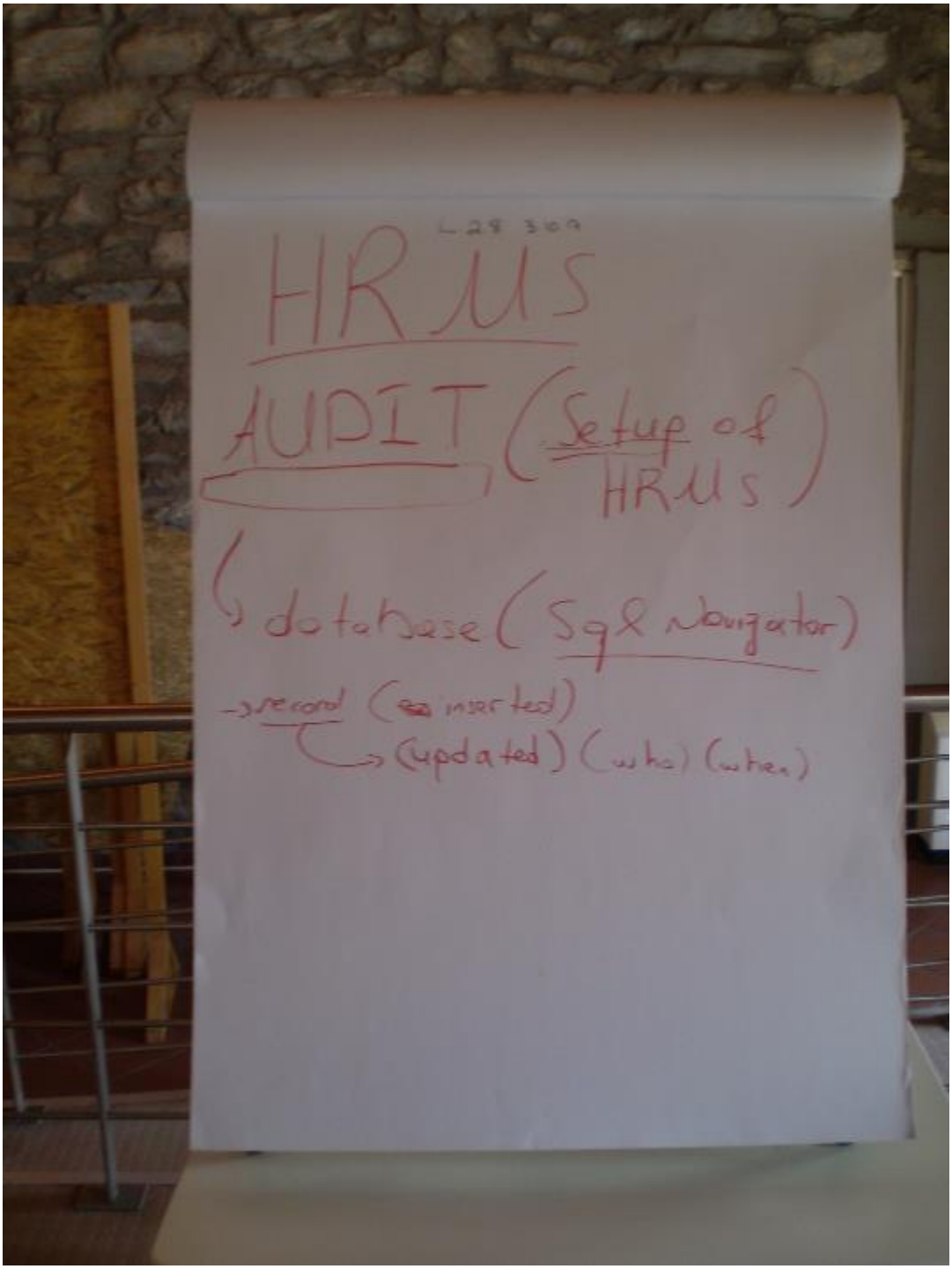
Specific firewall rules have been configured in SR710 server’s SEP :

1) Allow all traffic from Larissa‘s Syzefxis VPN. This includes only the city of Larissa and allows traffic from IP’s [IP1] to [IP2], All Protocols.
2) Allow traffic from Giannouli’s Syzefxis VPN, only for protocol TCP and for specific server ports 1521, 920 and 190 (as explained in “L day 2 slide4”). This includes only the community of Giannouli and allows traffic from IP’s [IP1] to [IP2] only for the connections with Oracle database and Genesis software.
3) Allow traffic from Koilada’s Syzefxis VPN, only for protocol TCP and for specific server ports 1521, 920 and 190 (as explained in “L day 2 slide4”). This includes only the community of Koilada and allows traffic from IP’s [IP1] to [IP2] only for the connections with Oracle database and Genesis software.
4) Block traffic from all other IP’s, besides the aforementioned IP’s, in subnets [SUBNET1] and [SUBNET2].


1) SEP (Symantec Endpoint Protection) 12.1.6
All servers have SEP
2) Clients → SEP
→ free antivirus (Avast)
Server R710 SEP firewall rules:
1) Allow our subnet: 10.128.5[illegible] - 10.128.1.254
2) Allow Giannadi: 10.129.40.1 - 10.129.40.254 ports: 1521, 920, 110
3) Allow Koilada: 10 ports: 1521, 920, 190
4) Block all other IPs

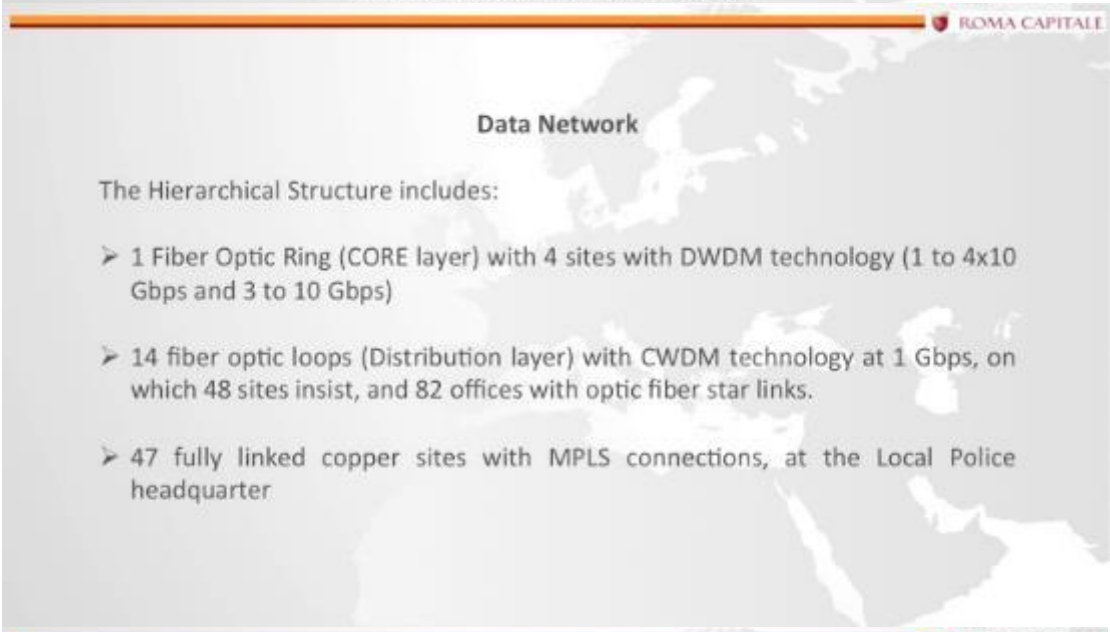
Day 2 RP 8

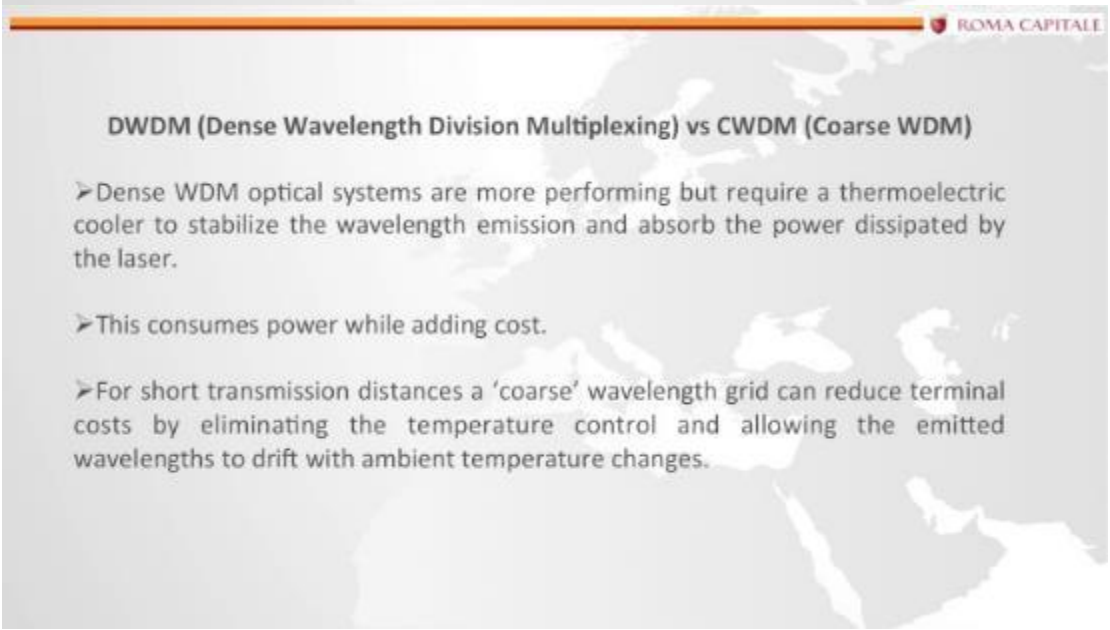
HRMS SETUP (Human Resources Management System Setup) offers an additional tool, named "Audit" with the intention of keeping track of the changes that are made by the users. Users must apply criteria such as who (user) updated, what (table-record) and when (date range). In the result screen the user can see the updated records and the old and new values of the fields, and doesn't have the ability to export the results. Administrators have additional access to the Oracle database (instance name: OTA_DB), its tables and views (schema: SHR) and can retrieve information by using tools like SQL Navigator.

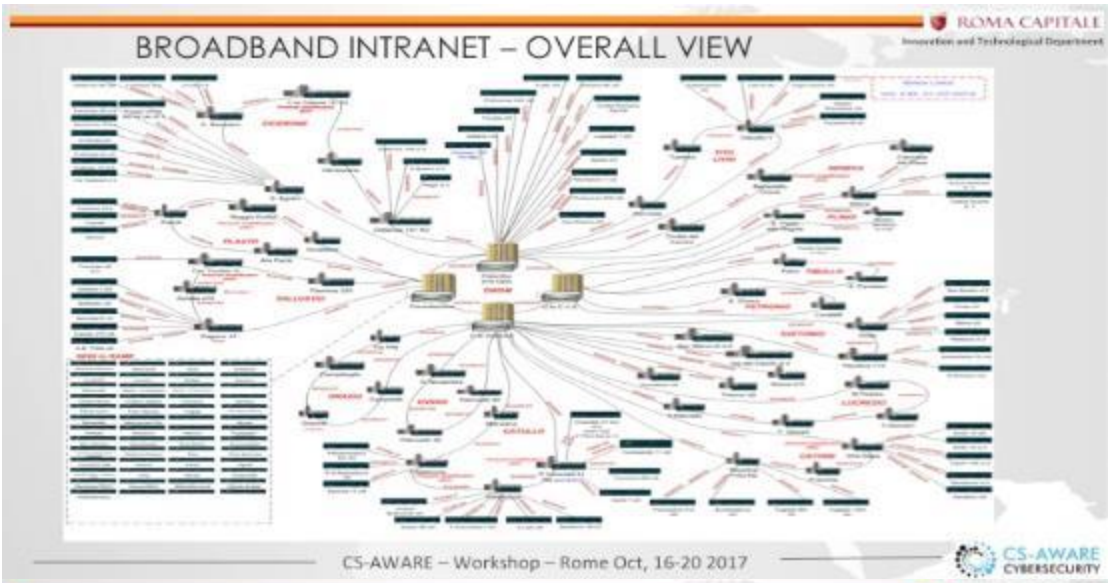


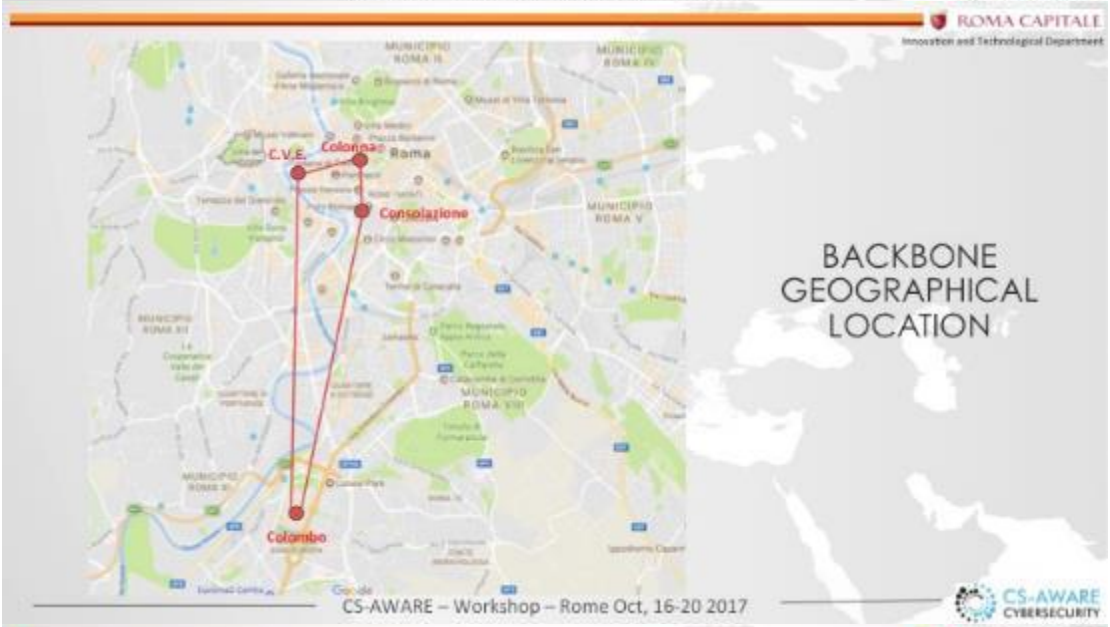
Annex 3

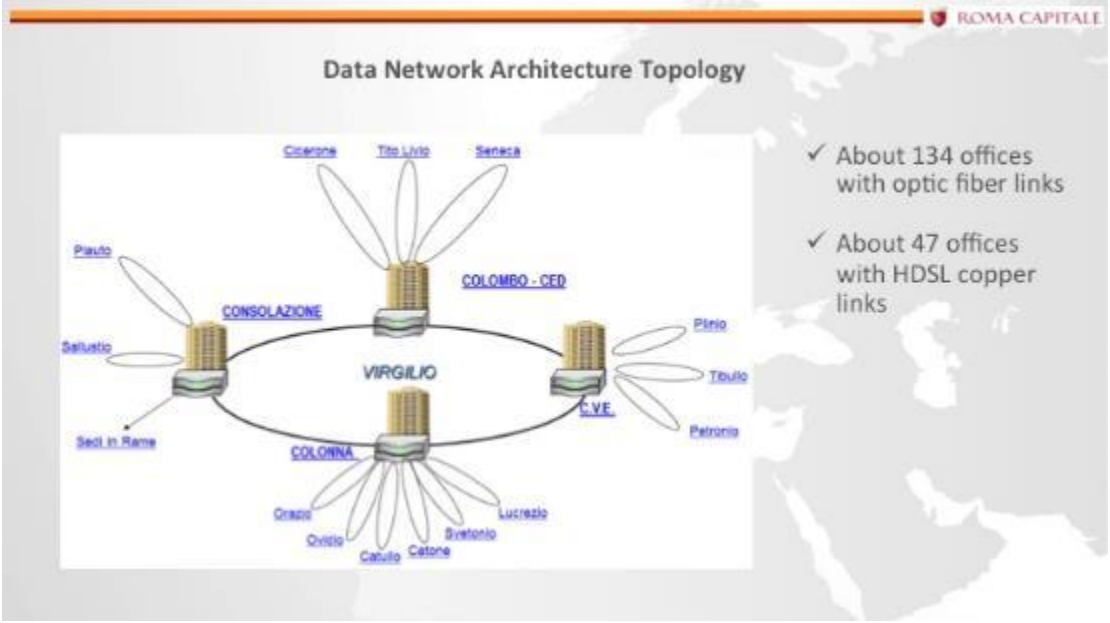
Presentations slides describing various aspects of Roma Capitale's systems






ROMA CAPITALE
BROADBAND INTRANET – OVERALL VIEW
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
C.V.E.
Colonna
Roma
Consolazione
Colombo
BACKBONE GEOGRAPHICAL LOCATION
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
Data Network Architecture Topology
Cicerone
Tito Livio
Seneca
Plauto
COLOMBO - CED
CONSOLAZIONE
Sallustio
VIRGILIO
Plinio
Tibullo
C.V.E.
Petronio
Sedi in Rame
COLONNA
Orazio
Ovidio
Catullo
Catone
Svetonio
Lucrezio
✓ About 134 offices with optic fiber links
✓ About 47 offices with HDSL copper links

ROMA CAPITALE

Roma Capitale public hot spots distribution in the territory

Offices of Roma Capitale

Digit Roma

ROMA CAPITALE

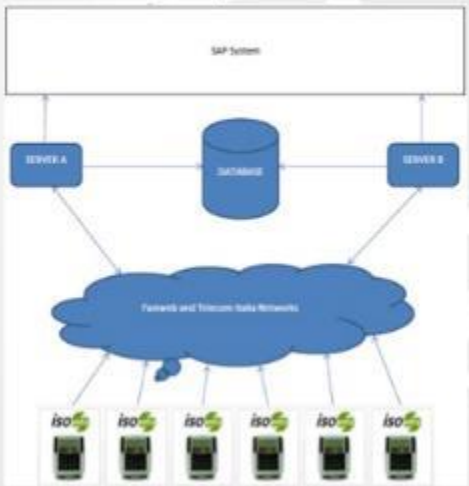
Attendance detection system

- About 1000 readers installed in the offices and in the schools (nursery schools)

Monitoring tool of badge readers

ROMA CAPITALE

Attendance detection system network architecture



ROMA CAPITALE

Voice Network

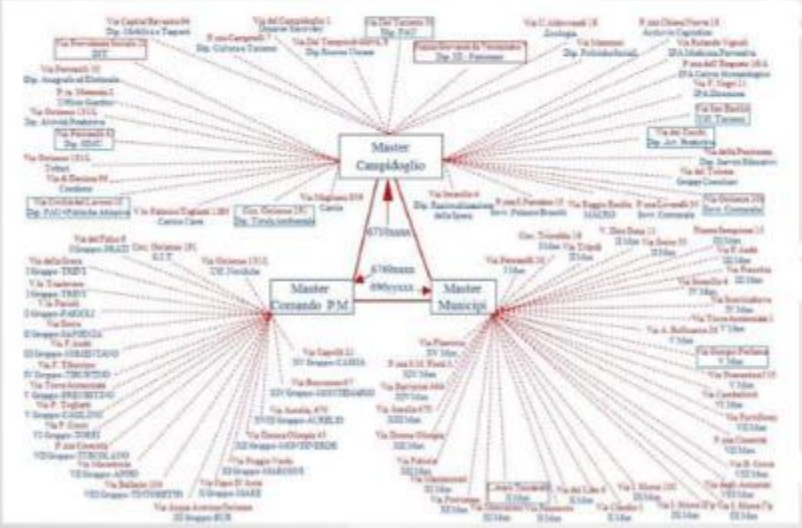
The Voice Network of Rome Capital is structured in three main Poles for a total of 14,500 users.

The three Poles are :

- **Polo Campidoglio**, numbered 066710xxxx, to which all Central Rome Departments and Headquarters are connected;
- **Local Police Pole**, numbered 066769xxxx, to which the Local Police Command and Municipal Groups are connected;
- **Municipal Town Halls**, numbered 06696 (01/20) xxx, to which all municipalities are connected (numbering 01/20 identifies the town halls according to the territorial division prior to the merger process implemented in 2013).

=

ROMA CAPITALE



VOICE NETWORK ARCHITECTURE

Total 90 interconnected nodes

SPC: THE ITALIAN CONTEXT

The Public Connectivity System, also known as the System of Public Connectivity (**SPC**) is a network that connects Italy's government agencies, allowing them to share and exchange data and information resources.

SPC is defined as "the set of Infrastructure Technology rules and techniques for developing, sharing, integration and dissemination of information assets and government data, necessary to ensure basic interoperability and application cooperation and evolved computer systems and information flows, **ensuring security, confidentiality and preservation of information assets and the autonomy of each government**"-

The system was established by the Legislative Decree of February 28, **2005**, no. 42.

Old SPC lasted from 2006 to 2017.

New SPC was born in 2017 and is provided by 3 Qualified Internet Service Provider (QISP):
-Fastweb
-British Telecom
-Vodafone

Fastweb is SPC provider for Roma Capitale.

SPC: BASIC PRINCIPLES AND OBJECTIVES

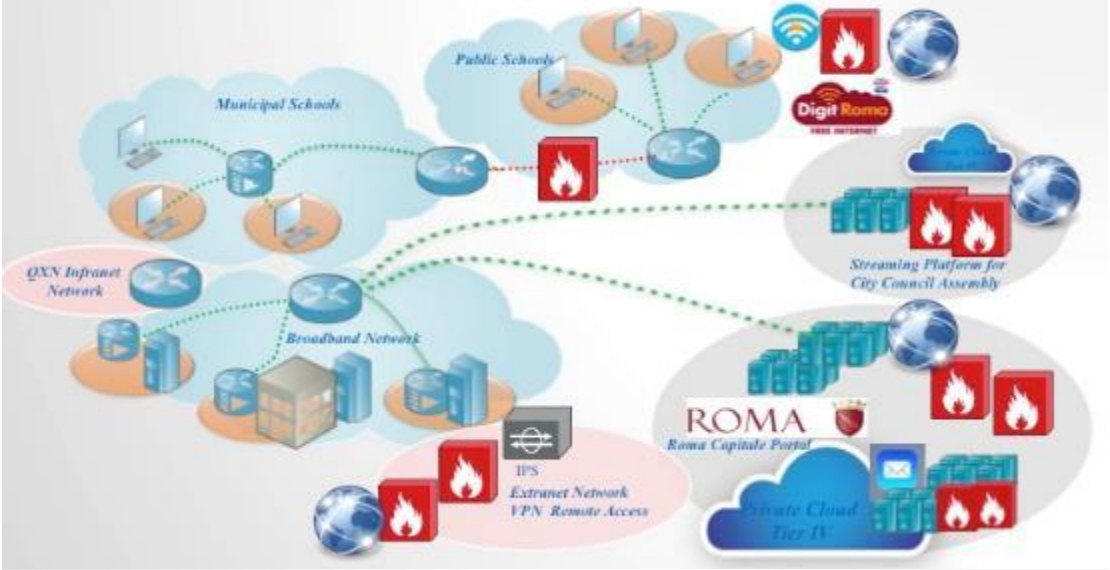
- Develop architecture and organization to ensure a federated, polycentric and non-hierarchical system.
- Economize use of network services, maintaining interoperability and support for application cooperation.
- Develop markets and competition in information and communication technology.
- Provide connectivity services shared by Public Administrations (PA) that are connected and scalable.
- Ensure the interaction of central and local PA on all Internet-related subjects and other bodies, promoting the delivery of quality services.
- Provide a shared interchange that allows interoperability among existing Pa networks.
- Provide service connectivity and co-PA to agencies that so request to allow the interconnection of their seats and enable for internal communication.
- Make a multi-vendor service delivery model consistent with the current market and the size of the project.
- Ensure the development of computer systems under the SPC safeguarding data security, confidentiality and the autonomy of the information assets of the Administration.

Source:
https://en.wikipedia.org/wiki/Public_Connectivity_System_(SPC)

QXN: QUALIFIED EXCHANGE NETWORK

- SPC Q-ISPs may implement their backbones by using different technologies, with different services and SLAs and according to different evolution paths.
- QXN "smooths" all these differences, by binding all Q-ISPs to comply with specific technical requirements and rules set by QXN Technical Committe.
- This results in creating a single SPC "virtual" network (integrating QXN and QISP's backbones) that provides all SPC customers (the PAs) with services with high and homogeneous levels of quality, no matter what Q-ISP is.
- QXN is a **consortium** that provides SPC Q-ISPs with access to QXN services (such as housing, access ports, guaranteed bandwith, centralized DNS, NTP server)
- QXN guarantees equal access conditions to QXN infrastructure and services both to Members of Consortium and to other Q-ISPs.

OVERVIEW OF IT INFRASTRUCTURE, TLC, PORTAL AND E-MAIIL SERVICES



MUNICIPAL SCHOOL NETWORK

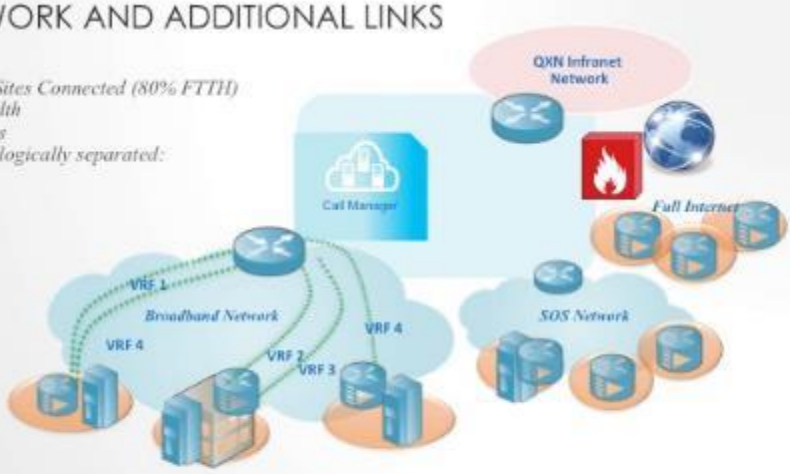
- *# 520 Municipal Schools Connected*
- *2,5 Gbps Aggregated Bandwidth*
- *# 1600 Managed IP Phones*
- *# 520 Managed Local Area Network Switches*

PUBLIC SCHOOL NETWORK

- # 247 Public Schools Connected
- 2 Gbps Aggregated Bandwidth
- # 750 Managed IP Phones
- WI-FI Services (# 750 Access Point)
- Coverage of Musei Capitolini with 50 AP
- Authentication via Captive Portal

BROADBAND NETWORK AND ADDITIONAL LINKS

- Broadband Network - # 176 Sites Connected (80% FTTH)
- 52 Gbps Aggregated Bandwidth
- # 30.000 Managed Extensions
- Multi-VRF Network (5 VRF) logically separated:
  - RomaCapitale_VDS
  - RomaCapitale_WIFI
  - RomaCapitale_FONIA
  - RomaCapitale_DATI
  - RomaCapitale_IMPIANTI

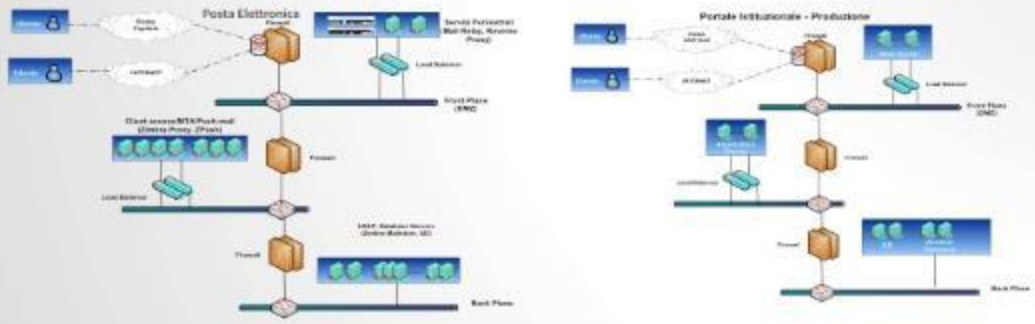


- Additional Links:
  - # 50 SOS Links 300 Mbps Aggregated Bandwidth
  - # 11 Full Internet and WIFI sites (160 Mbps Aggregated Bandwith) + Firewalling Protection

EXTRANET NETWORK VPN REMOTE ACCESS

- 503 VPNs
- 51 DMZs
- 7 Inter domain Networks
  - 5 external,
  - 1 internal,
  - 1 private.

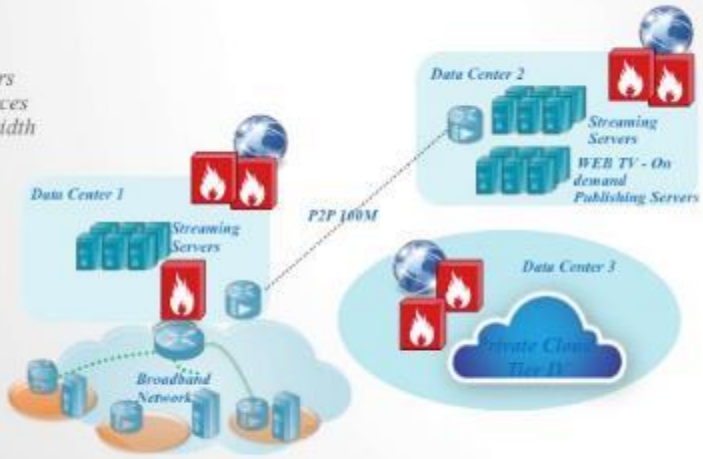
ROMA CAPITALE PORTAL AND E-MAIL SERVICES



- *More than 5 millions email messages monthly managed;*
- *More than 1.5 millions email messages monthly blocked;*
- *More of 28 Millions of Web Attacks monthly blocked*
- *# 15.500 protected endpoints;*

STREAMING PLATFORM

- *# 8.000 concurrent users*
- *# 20 simultaneous sources*
- *1 Gbps Internet Bandwidth*



CYBERSECURITY DATA SOURCES

Security capability	*Data Source*
Next Generation Firewall	Next Generation Firewall Log
Intrusion Prevention System	*IPS Log*
Web Application Firewall	*Web Application Firewall Log*
Mail Protection	*Secure E-Mail Gateway Log*
DDoS Protection	*DDoS Mitigation Platform Log*
EndPoint Protection	*Console Logs*
Security Operations Center (SOC)	*Incident Report*
Sandboxing	*Advanced Threat Protection Log*

ROMA

CS-AWARE

Topic DS-02-2016:
Cyber Security for SMEs, local public administration and individuals

TETRA PROJECT FOR A DIGITAL MULTI-ACCESS RADIO SECURE NETWORK

CS-AWARE – Workshop – Rome Oct, 16-20 2017

ROMA CAPITALE

NETWORK HIGHLIGHTS

- TErrestrial Trunked RAdio (TETRA) standard
- Native Full-IP network ➡ each component has its own private IP address
- 43 Base Stations (Nodes)
  - 19 " Air " Sites
  - 2 " Gallery " Sites ➡ leaky feeder for indoor coverage

  1 Base Station ➡ 7 traffic channels
  Total = 280 avalaible channels
- 14 carrier frequencies (f_c) couples in the 450 ÷ 470 MHz band
  - Each (f_c) has 25 KHz bandwith and carries 4 channels
- IP fiber optic backhauling network provided by TIM connects :
  - 9 Workstations in Local Police HQ
  - 2 Workstations in Backup Site
  - 25 Workstations in Remote Local Police Offices
  - BS Sites
- Disaster Recovery features ➡ full redundancy of all networks elements and servers

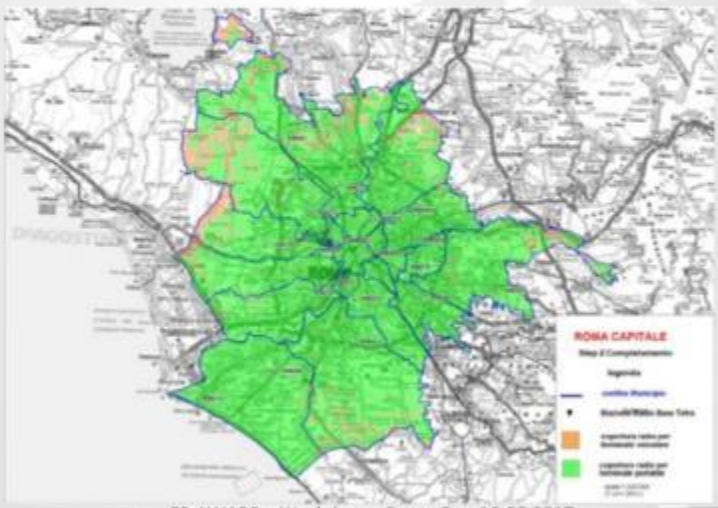
	9+2
	25
	43
	6.000
	600

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE

NETWORK COVERAGE



CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

NETWORK LOGICAL ARCHITECTURE

ROMA CAPITALE

TIN (Tetra IP Node)→ Main control platform

SMN(Subscriver Mgmt Node) → stores all info about users and groups

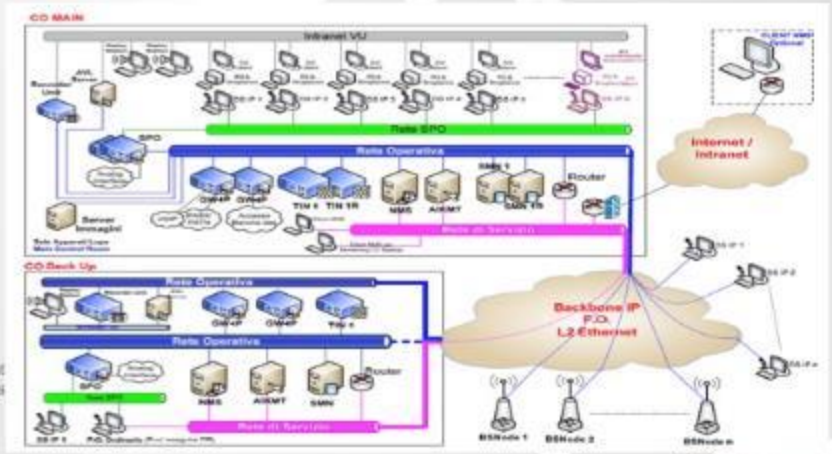
NMS(Network Mmgt System)

AVL → radio localization

Recorder Unit → all on-net data and voice traffic

GW-IP → interface to PABX/ PSTN and external DB access

AIKMT(Air Interface Key Mgmt System) → creates, transmits and stores safely keys



CS-AWARE – Workshop – Rome Oct, 16-20 2017

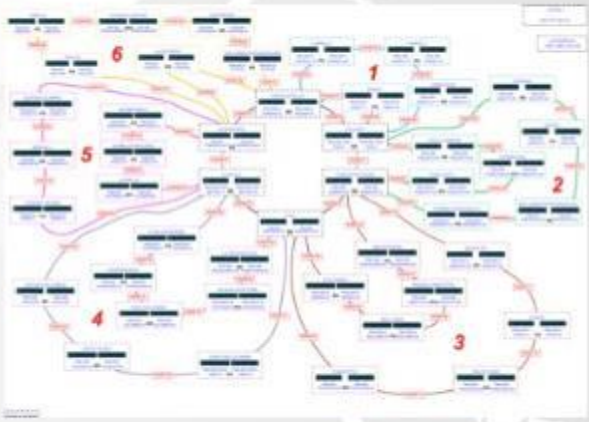
CS-AWARE CYBERSECURITY

TRASNPORT NETWORK

ROMA CAPITALE

GIGABIT ETHERNET FIBER RINGS LAYOUT

- Primary ring connecting 6 TIM Exchange Sites
- 6 Access rings collecting data from all Base Stations, TIM Exchange Sites and Remote Workstations



CS-AWARE – Workshop – Rome Oct, 16-20 2017

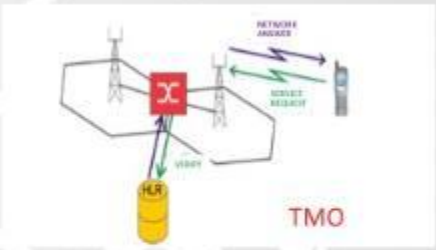
CS-AWARE CYBERSECURITY

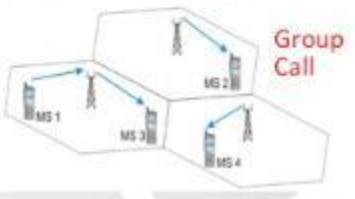
NETWORK FEATURES 1/2

ROMA CAPITALE

The network allows the following operations :

- **TMO** → in normal conditions all user requests are admitted according to their profiles , stored on the Home Location Register DB
- **Group Call** → only members (can be both mobile users or WS) belonging to the same group receive the call, the network allocates for each involved cell a dedicated channel (Half-Duplex manner)
- **Individual Call** → exclusive call between 2 members





CS-AWARE – Workshop – Rome Oct, 16-20 2017

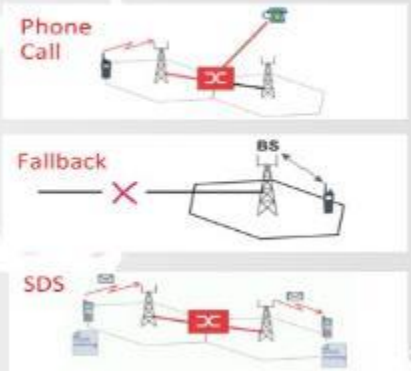
CS-AWARE CYBERSECURITY

NETWORK FEATURES 2/2

ROMA CAPITALE

The network allows the following operations :

- **Phone call** → between a TETRA user authorized on HLR and a PSTN number, through a Gateway
- **Fallback**→ in the unlike case of a fiber link disruption the BS is still able to guarantee a partial service in its coverage area
- **Emergency Call** → highest priority level, the network can shut down ongoing calls to release communication channels and force user to accept it
- **SDS** → to exchange text messages among single users or group members
- **DMO** → direct communication (walkie-talkie) between users out of coverage areas



CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

NETWORK SECURITY

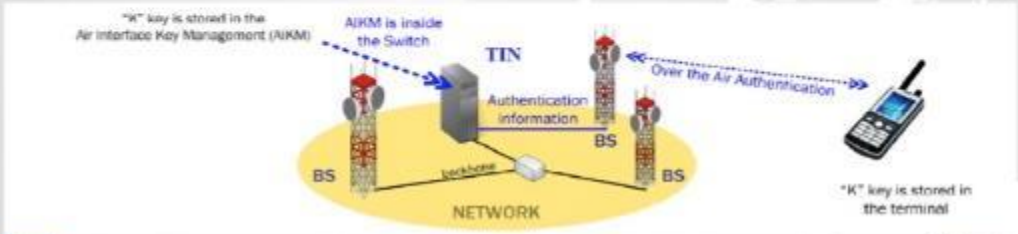
ROMA CAPITALE

AUTHENTICATION

- At setup the network asks the mobile handset to validate its identity before logging
- Based on a 128bit secret key unique for each terminal

AIR ENCRYPTION

- Protects the link between mobile device and BS
- Also signalling info (i.e. GPS coordinates) are encrypted
- Based on TEA2 standard , dedicated to European Police Corps
- Relies on dynamic keys



CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

GEOGRAPHIC LOCALIZATION

ROMA CAPITALE

- The Cartographic Server allows to display on a map the exact location of each terminal
- Each terminal is programmed to send a periodic SDS containing its GPS coordinates
- Each Workstation can track the related user path and speed in the last 24 hours

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE
Innovation and Technology Department

TETRA ADDRESSING FEATURES

Each user or group has a unique address on the TETRA network composed by:
- Country prefix (222 for Italy)
- Network code (24 for Roma Capitale)
- 7 digit Short Subscriver Identity

Due to HLR partitoning system, it is feasible to allow other Organizations to share the TETRA network, creating several VPNs with dedicated address spaces
- Today the range 1.000.000 ÷ 1.999.999 is assigned to Roma Capitale Local Police

SSI structure
X Y Z A B B B

FIELD	VALUE	MEANING
X	1	VPN code
YZ	00	HQ Work Station user
YZ	01÷24	Membership to Local or Special Group
A	01÷07	User class : WS, mobile terminal, static group etc
BBB	000 – 999	Reserved to Network Administrators

CS-AWARE – Workshop – Rome Oct, 16-20 2017

ROMA CAPITALE
Innovation and Technology Department

Security is necessary to ensure the availability, integrity and confidentiality of the information provided by the Public Administration Information System. It is also directly related to the privacy principles provided by the EU.

Interconnected field

CS-AWARE – Workshop – Rome Oct, 16-20 2017

ROMA CAPITALE
Innovation and Technology Department

Regulatory background in Italy 1/2

The publication in Official Gazette (General Series No. 103 of 5-5-2017) of Circular **18th of April 2017**, no. 2/2017 on "**Minimum ICT Security Measures for Public Administrations**". Those measures have now become mandatory for all Administrations. Deadline 31/12/2017

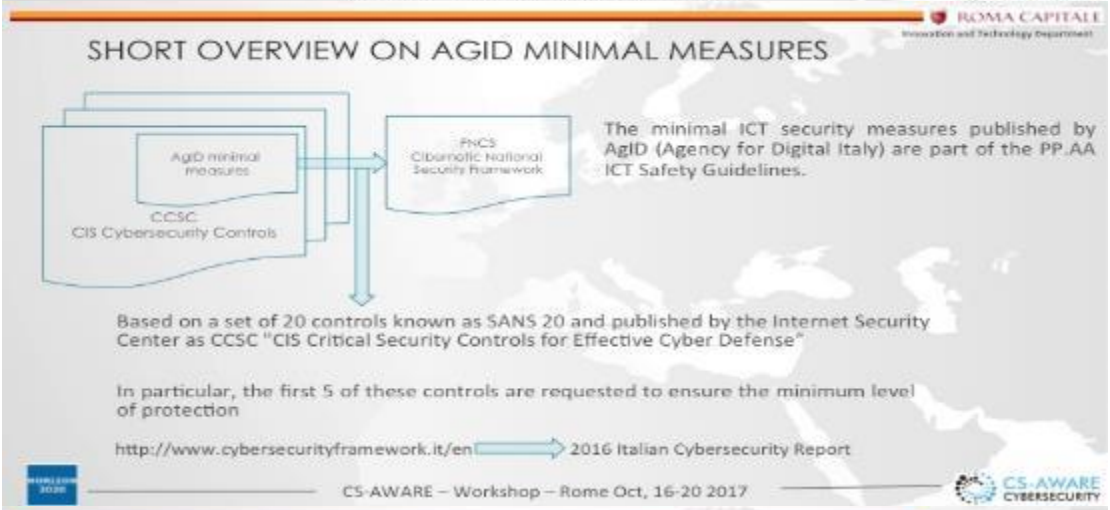
AGID

The General Data Protection Regulation (**EUR 2016/679**) is a Regulation whereby the European Commission aims unify the protection of personal data within the European Union. **Deadline 24/05/2018**

GDPR

CS-AWARE – Workshop – Rome Oct, 16-20 2017


ROMA CAPITALE
Regulatory background in Italy 2/2
The new CAD. The publication in the Official Gazette no. 214 of 13th of September 2016, take into account the Security Issues
Digital Administration Code
Decree of the President of the Council of Ministers 17th of February, Guideline on cyber protection and national computer security (published on 13/4/2017)
CyberSecurity National Strategy
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
SHORT OVERVIEW ON AGID MINIMAL MEASURES
AgID minimal measures
CCSC
CIS Cybersecurity Controls
FNCS
Cibernetic National Security Framework
The minimal ICT security measures published by AgID (Agency for Digital Italy) are part of the PP.AA ICT Safety Guidelines.
Based on a set of 20 controls known as SANS 20 and published by the Internet Security Center as CCSC "CIS Critical Security Controls for Effective Cyber Defense"
In particular, the first 5 of these controls are requested to ensure the minimum level of protection
http://www.cybersecurityframework.it/en
2016 Italian Cybersecurity Report
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

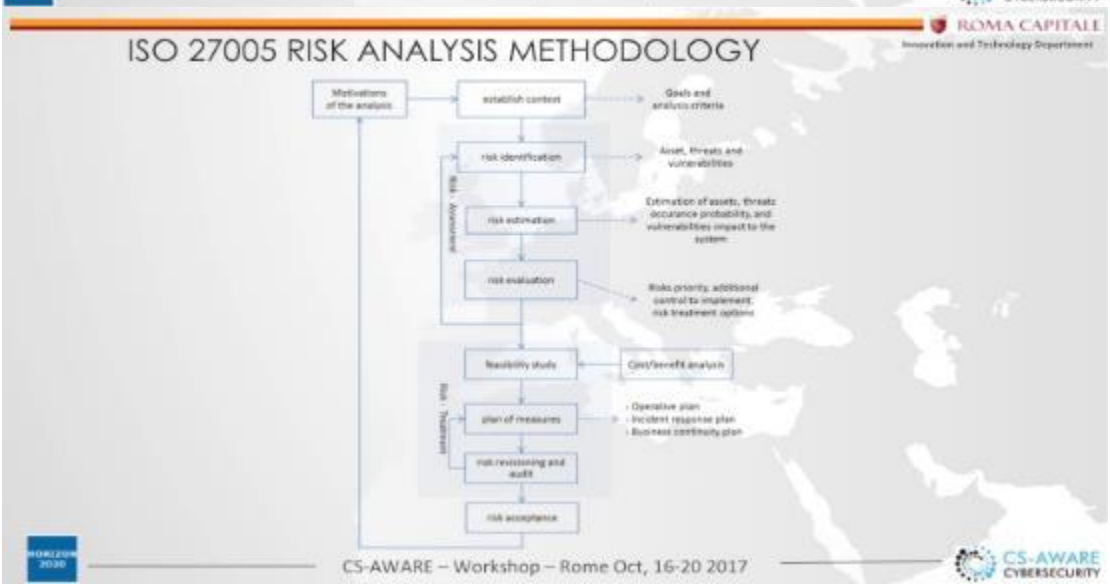

D.I.T. RISK ASSESSMENT ACTORS
Roma Capitale – Innovations Technology Department
One of the target Roma Capitale Digital Agenda
AgID minimal measures
The purpose of this document is to indicate to public administrations the minimum ICT security measures that must be taken to counter the common and most common threats to which their information systems are subject.
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

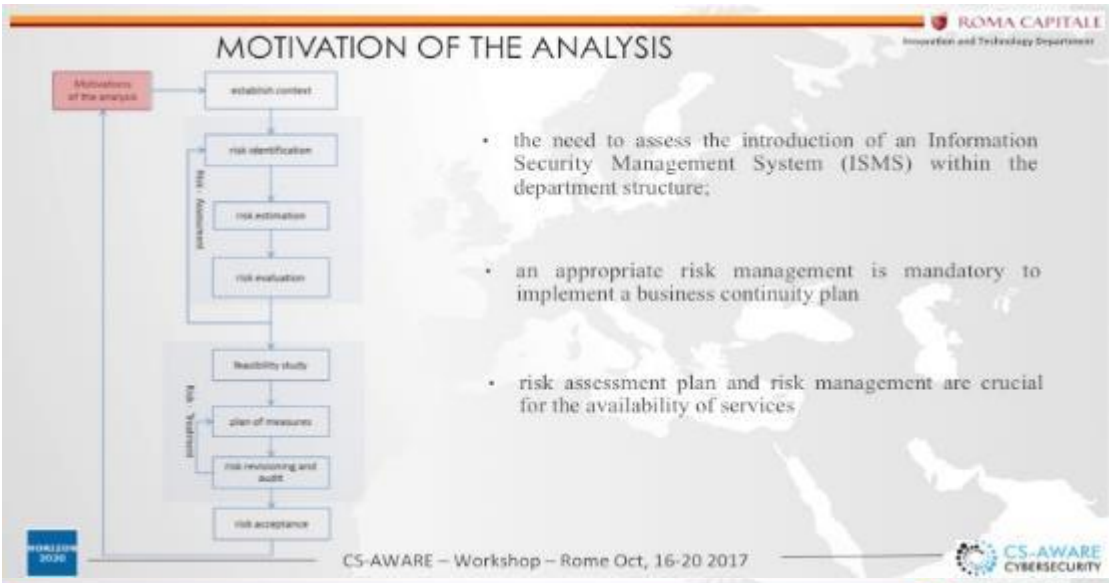

The role of the Minimum Security Measures in DIT risk Assessment
Innovation and Technology Department
Detalied and simple check list
This measures support the pubblic administrations to contrast the common threat
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

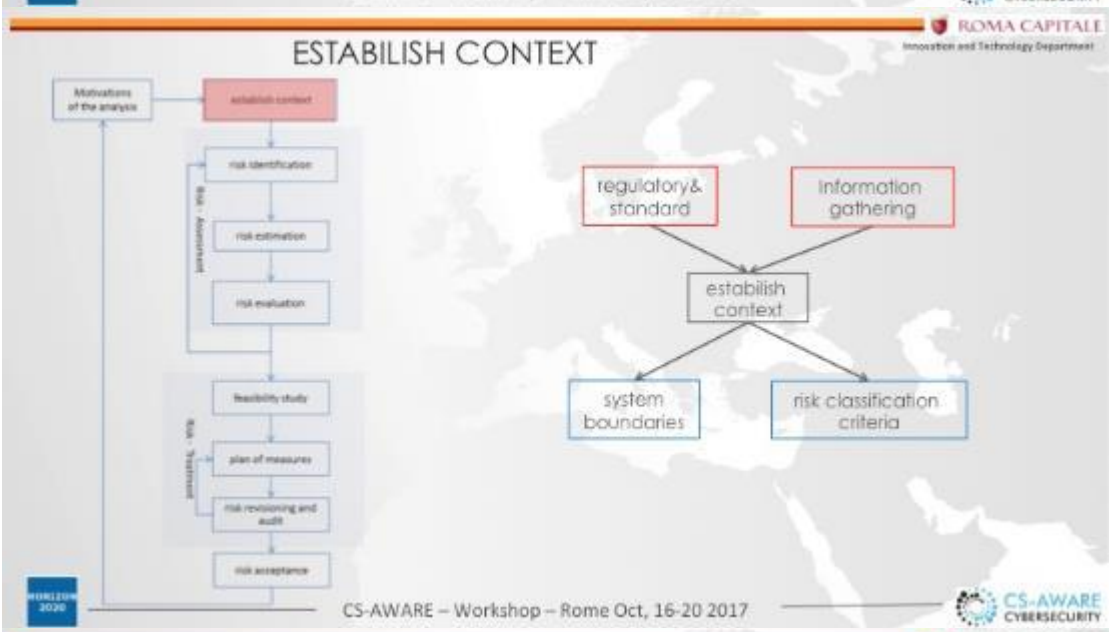

Innovation and Technological Department
Many Thanks !!!
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

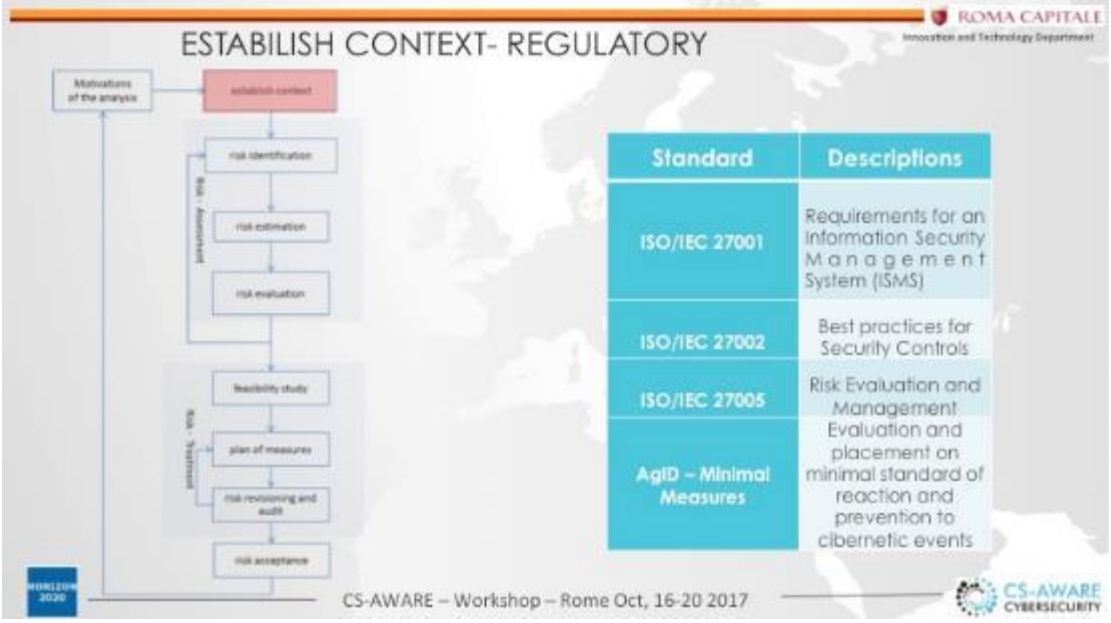

ROMA
CS-AWARE
CS-AWARE CYBERSECURITY
Topic DS-02-2016:
Cyber Security for SMEs, local public administration and Individuals
Roma Capitale – Risk Assessment
CS-AWARE – Workshop – Rome Oct, 16-20 2017

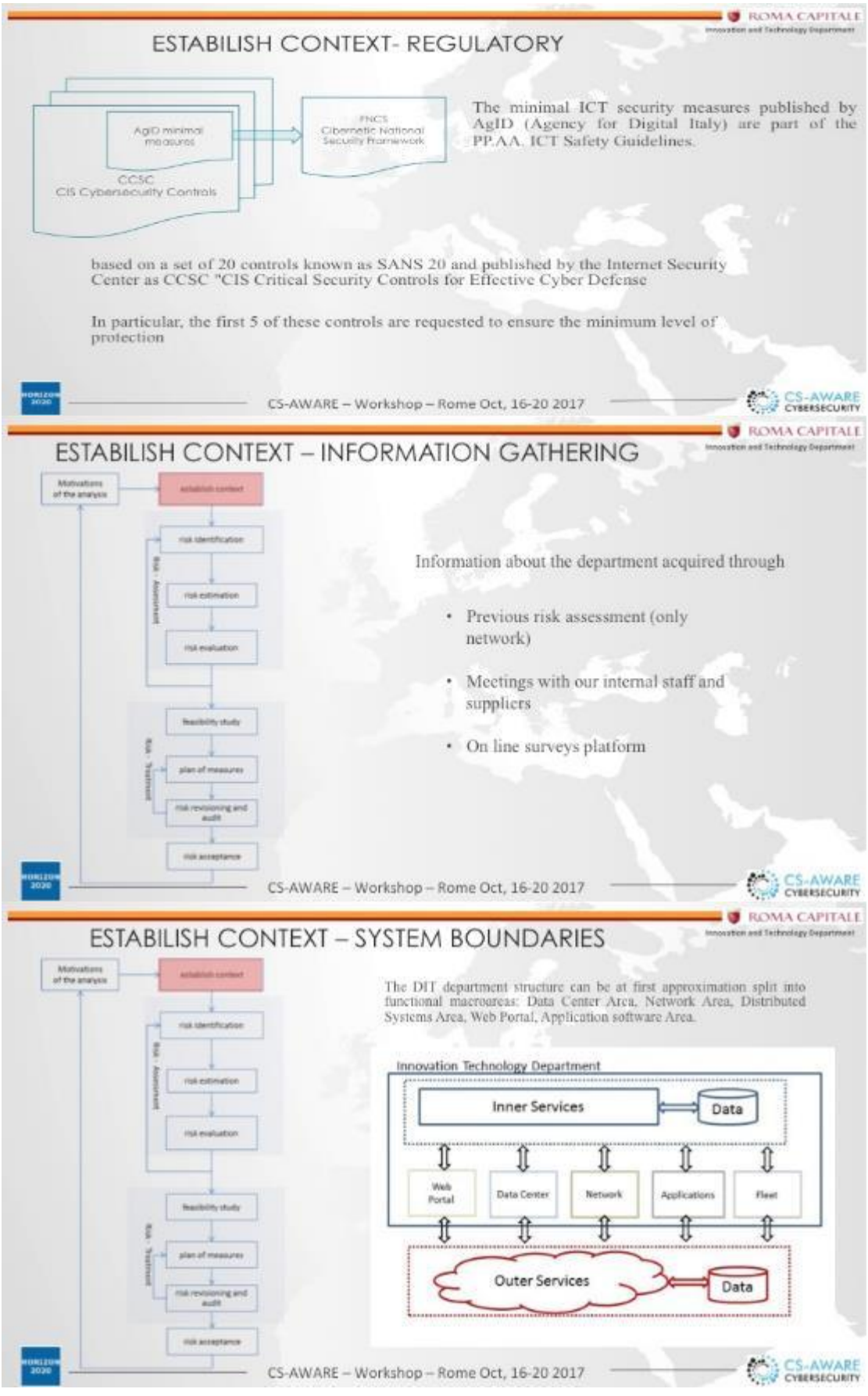

ROMA CAPITALE
DIT APPROACH TO SECURITY
PLAN
Risk assessment
Task completed
DO
Implement a risk treatment plan on Information Security according to current regulations
Definition of an ISMS
CHECK
Internal audit
ACT
Corrective measures & Preventive action
work in progress
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

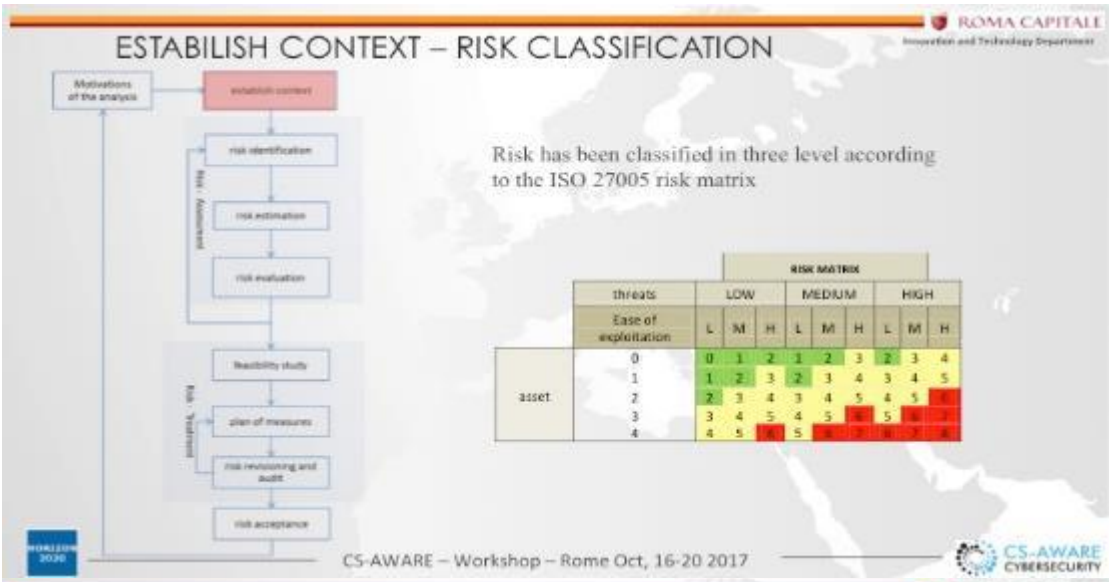

ROMA CAPITALE
ISO 27005 RISK ANALYSIS METHODOLOGY
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

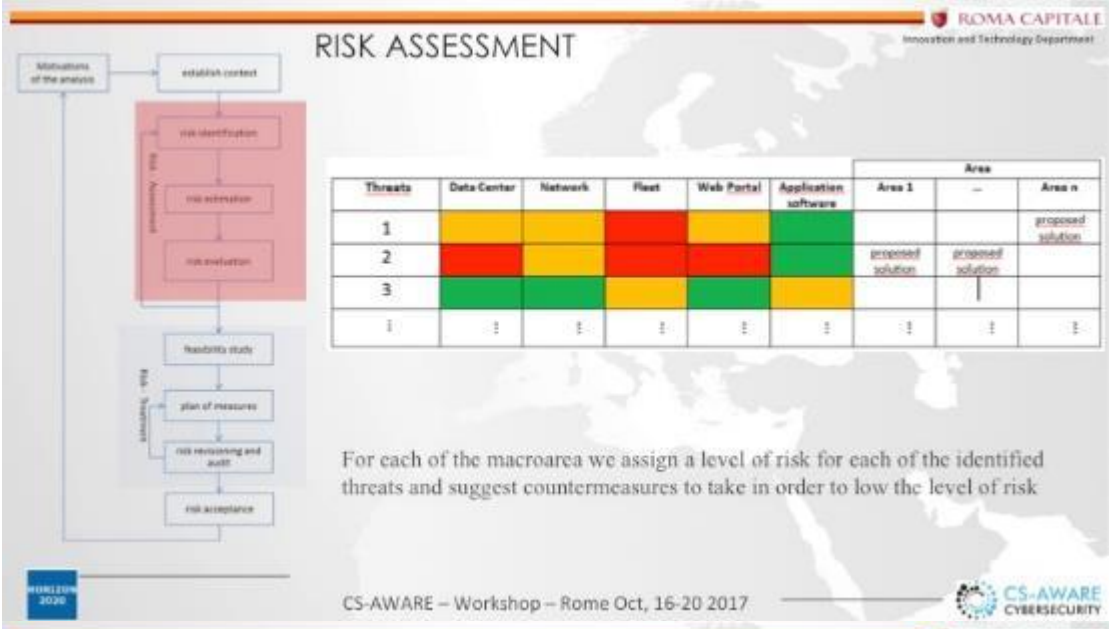

ROMA CAPITALE
MOTIVATION OF THE ANALYSIS
• the need to assess the introduction of an Information Security Management System (ISMS) within the department structure;
• an appropriate risk management is mandatory to implement a business continuity plan
• risk assessment plan and risk management are crucial for the availability of services
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

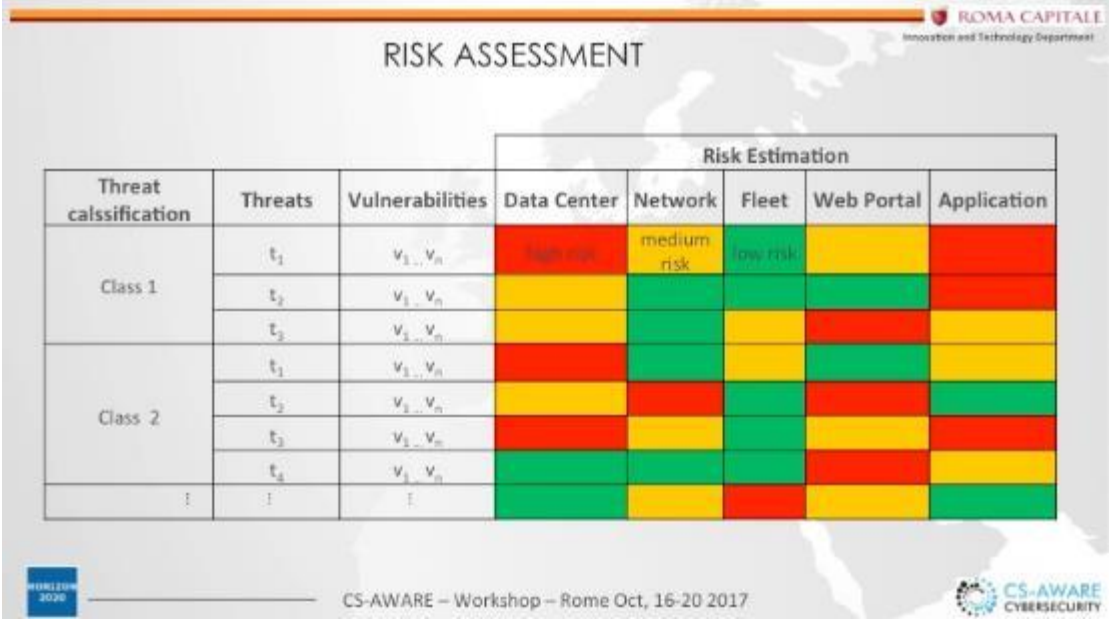

ROMA CAPITALE
ESTABILISH CONTEXT
regulatory& standard
information gathering
estabilish context
system boundaries
risk classification criteria
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

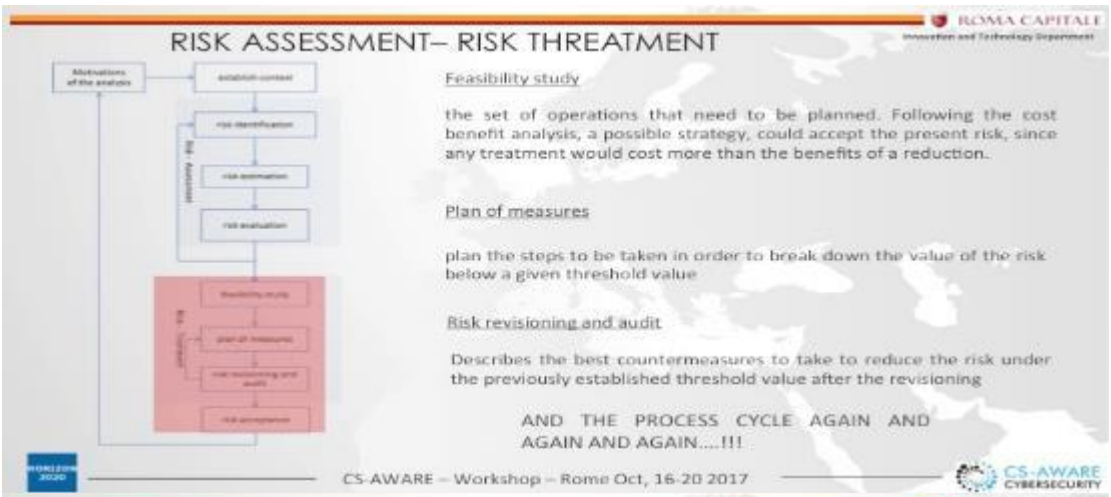

ROMA CAPITALE
ESTABILISH CONTEXT- REGULATORY
Standard
Descriptions
ISO/IEC 27001
Requirements for an Information Security Management System (ISMS)
ISO/IEC 27002
Best practices for Security Controls
ISO/IEC 27005
Risk Evaluation and Management
AgID – Minimal Measures
Evaluation and placement on minimal standard of reaction and prevention to cibernetic events
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

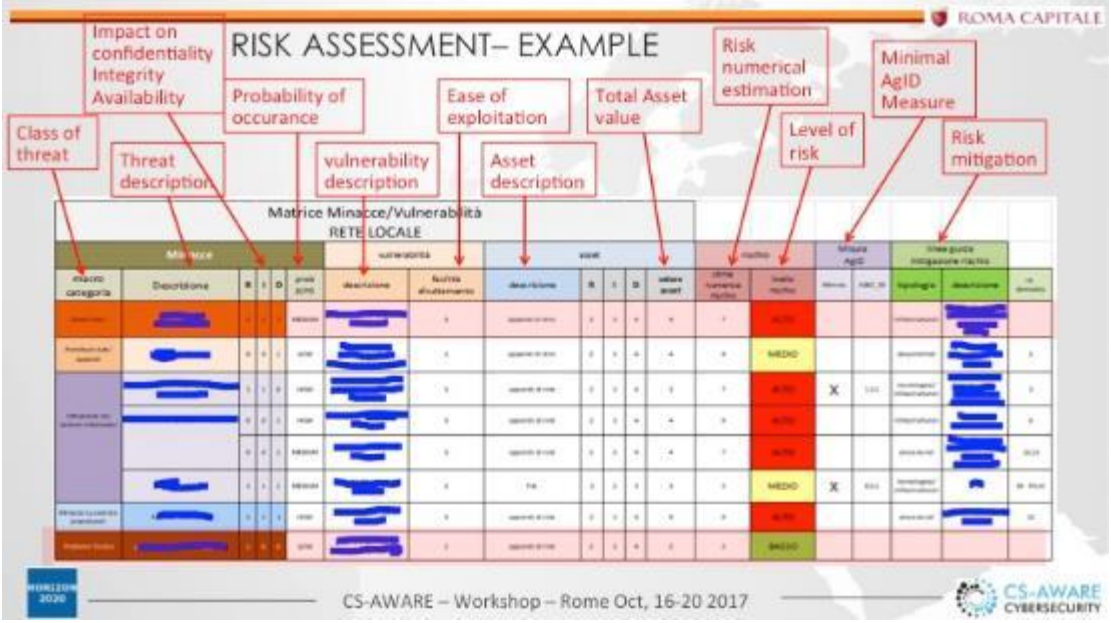

ROMA CAPITALE
ESTABLISH CONTEXT- REGULATORY
AgID minimal measures
CCSC
CIS Cybersecurity Controls
FNCS
Cibernetic National Security Framework
The minimal ICT security measures published by AgID (Agency for Digital Italy) are part of the PP.AA. ICT Safety Guidelines.
based on a set of 20 controls known as SANS 20 and published by the Internet Security Center as CCSC "CIS Critical Security Controls for Effective Cyber Defense
In particular, the first 5 of these controls are requested to ensure the minimum level of protection
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY
ROMA CAPITALE
ESTABLISH CONTEXT – INFORMATION GATHERING
Information about the department acquired through
Previous risk assessment (only network)
Meetings with our internal staff and suppliers
On line surveys platform
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY
ROMA CAPITALE
ESTABLISH CONTEXT – SYSTEM BOUNDARIES
The DIT department structure can be at first approximation split into functional macroareas: Data Center Area, Network Area, Distributed Systems Area, Web Portal, Application software Area.
Innovation Technology Department
Inner Services
Data
Web Portal
Data Center
Network
Applications
Fleet
Outer Services
Data
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
ESTABLISH CONTEXT – RISK CLASSIFICATION
Risk has been classified in three level according to the ISO 27005 risk matrix
RISK MATRIX
threats
LOW
MEDIUM
HIGH
Ease of exploitation
L M H L M H L M H
asset
0 1 2 1 2 3 2 3 4
1 1 2 3 2 3 4 3 4 5
2 2 3 4 3 4 5 4 5
3 3 4 5 4 5
4 4 5
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
RISK ASSESSMENT
Area
Threats
Data Center
Network
Fleet
Web Portal
Application software
Area 1
Area n
1
2
3
proposed solution
For each of the macroarea we assign a level of risk for each of the identified threats and suggest countermeasures to take in order to low the level of risk
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
RISK ASSESSMENT
Risk Estimation
Threat calssification
Threats
Vulnerabilities
Data Center
Network
Fleet
Web Portal
Application
Class 1
Class 2
medium risk
low risk
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
RISK ASSESSMENT– RISK THREATMENT
Feasibility study
the set of operations that need to be planned. Following the cost benefit analysis, a possible strategy, could accept the present risk, since any treatment would cost more than the benefits of a reduction.
Plan of measures
plan the steps to be taken in order to break down the value of the risk below a given threshold value
Risk revisioning and audit
Describes the best countermeasures to take to reduce the risk under the previously established threshold value after the revisioning
AND THE PROCESS CYCLE AGAIN AND AGAIN AND AGAIN....!!!
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
RISK ASSESSMENT– EXAMPLE
Impact on confidentiality Integrity Availability
Class of threat
Threat description
Probability of occurance
vulnerability description
Ease of exploitation
Asset description
Total Asset value
Risk numerical estimation
Level of risk
Minimal AgID Measure
Risk mitigation
Matrice Minacce/Vulnerabilità
RETE LOCALE
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

ROMA
Innovation and Technological Department

CS-AWARE

Topic DS-02-2016:
Cyber Security for SMEs, local public administration and individuals

Disaster Recovery

ROMA CAPITALE
Innovation and Technological Department

DISASTER RECOVERY

- Data Center of Roma Capitale produces IT services more than 15000 Internal users, local companies and citizens
- Data Center (DC) is connected to about 200 local headquarters and pubblic administration networks
- Datacenter hold about 100 *racks*

ROMA CAPITALE
Innovation and Technological Department

DISASTER RECOVERY

- Data Center of Roma Capitale produces IT services more than 15000 Internal users, local companies and citizens
- Data Center (DC) is connected to about 200 local headquarters and pubblic administration networks
- Datacenter hold about 100 *racks*

CS-AWARE – Workshop – Rome Oct, 16-20 2017

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

Main application fields of DC:

A) Data Processing → *environment IBM-AIX*, *environment* Intel x86, *environment* Unisys

B) Data Storage → EMC Symmetrix VMAX 10K, EMC VNX5300

C) Backup Infrastructure → EMC Data Domain DD6300, Oracle SL500, Oracle SL48, EMC Data Domain DD630, EMC Data Store Avamar

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

Dc of Roma Capitale is equipped with a set of physical and logical safegards.

- Air conditioning is used to control the temperature and humidity in the data center
- Uninterruptible power supplies (UPS) and a diesel generator.
- Fire protection systems
- Physical Security: Physical access to the site is usually restricted to selected personnel
- Video surveillance system and permanent security guards are always present in the data center

...But despite this...DC could crash, for example for natural events as floods, or earthquakes and so on, or man-made disaster as tampering of data, bioterrorism, virus, warm etc.

so we have been equipped of a Disaster Recovery Site

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

.....*but what's happen if DC crashes?*

The services are ensured by a Disaster Recovery Plan

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

- Recovery point objective (RPO) and recovery time objective (RTO) are two important measurements in disaster recovery and downtime.
- RPO is the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster
- RTO is the maximum amount of time, following a disaster, for an organization to recover files from backup storage and resume normal operations. In other words, the recovery time objective is the maximum amount of downtime an organization can handle.

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

DR Site in Perugia:

- The surface is 1400 square meters
- The main room of Data Center is 200 square meters, and there are 38 racks
- Inside the building, we can find private offices, workshop, open space, conference hall

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

Reserved space to Roma Capitale

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

The DR Site uses 3 different technologies related to different level of service to ensure.

The applications are split up in 3 classes

- Class 1: app with RPO=5 minutes and RTO=8 hours for Unisys
- Class 2: app with RPO=5 minutes and RTO=8 hours for IBM-AIX/Intel x86
- Class 3: app with RPO=24 hours e RTO=48 hours for IBM-AIX/Intel x86

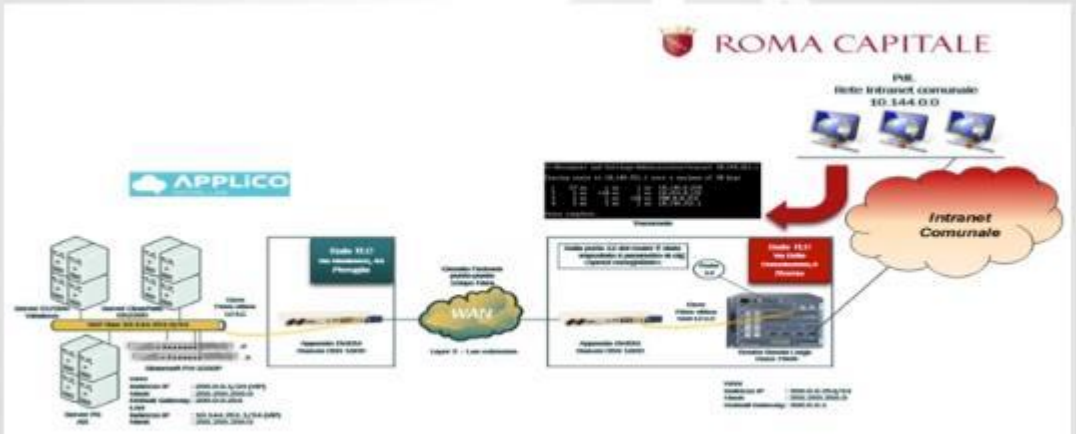
Class of service	RTO	RPO	Technology used
1	8 hours	5 minute	Asynchronous Data Replication disk to disk with EMC SRDF/A
2	8 hours	5 minute	Asynchronous Data Replication , disk to disk , with EMC RecoverPoint
3	48 hours	20 hours	

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department



Access to recovery services in Perugia's site (DR Site) by Roma Capitale (Main Site)

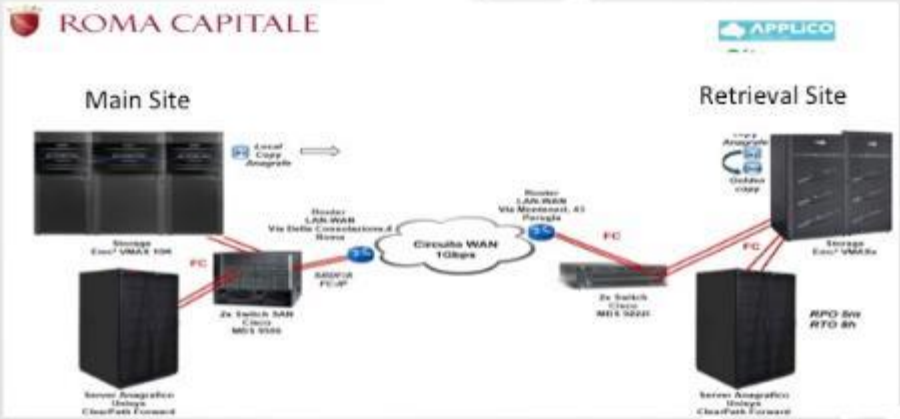
CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DISASTER RECOVERY

ROMA CAPITALE
Innovation and Technological Department

Class 1: Replace date EMC SRDF (Symmetrix Remote Data Facility/Asynchronous)



Anagrafic system replaced based on Symmetrix Remote Data Facility/Asynchronous: Allows replace on theoretically infinity distance

CS-AWARE – Workshop – Rome Oct, 16-20 2017

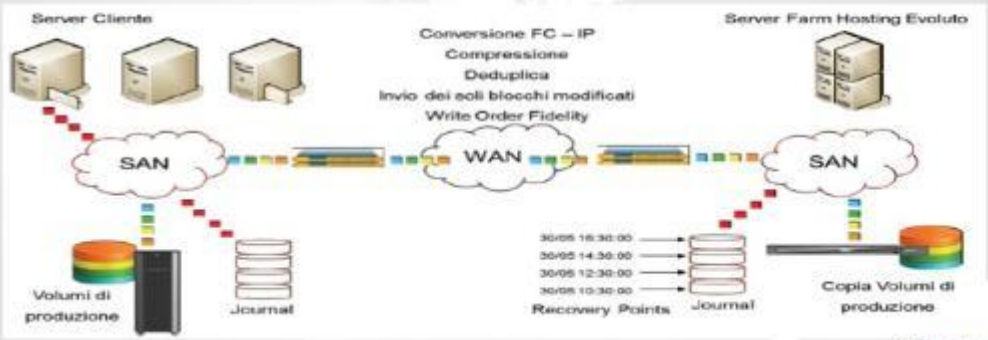
CS-AWARE CYBERSECURITY

ROMA CAPITALE
Innovation and Technological Department

DISASTER RECOVERY

Class 2, 3: Replace date EMC (RecoverPoint)

- It's based on hardware appliance that support many data stored on server or heterogenius storage.



ROMA CAPITALE
Innovation and Technological Department

DISASTER RECOVERY

Main features of EMC RecoverPoint are:

- Far distance replace: bandwidth management, TCP optimization
- Fast Recovery: recovery in any point in time without data loss
- Instant access to safe data: RecoverPoint can be used for backup, testing, recovery on-demand

Safety of Data

ROMA CAPITALE
Innovation and Technological Department

DISASTER RECOVERY

Operative Steps of DR Procedure:

Step	Person in charge	Activity
1	Referent Roma Capitale	Starts the procedure of DR
2	Action Center	Contacts the team leader
3	Team leader	Endorse the replace on DR site
4	System engineer	Starts replace EMC SRDF to DMX4 and recovery point to VMAX
5	System engineer	Coordinate the operation staff
6	Team leader	Inform the referent Roma Capitale that the services are started on DR Site


ROMA CAPITALE
Innovation and Technological Department
DISASTER RECOVERY
Last test was performed in may 2017
We simulated a crash of main site in Rome
We have involved two work groups, the first one in Rome and the second one in Perugia
Application tested:
SAP HR
SIPO
SIC
GED
SIAG and SIZA
It was stopped a normal operation on main site, we started the retrieval operation on Perugia site in accord to DR plain.
The test was succesfull!
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY
ROMA CAPITALE
Innovation and Technological Department
DISASTER RECOVERY
Thanks!
References:
Luca Iezzi
Roma Capitale
luca.iezzi@comune.roma.it
06671074059
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY

ROMA

CS-AWARE

CS-AWARE CYBERSECURITY

Topic DS-02-2016:
Cyber Security for SMEs, local public administration and individuals

Roma Capitale Data Center

CS-AWARE – Workshop – Rome Oct, 16-20 2017

ROMA CAPITALE

DATA MANAGED

- Personal - Demographic - Census
- Urban Development - Map Databases
- Election - Polling - Projection
- Companies - Production Activities
- Local Police Authority
- Financial - Payments - Billing
- Accounting - Human Resources
- Open Data

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE

SERVICES & APPLICATIONS

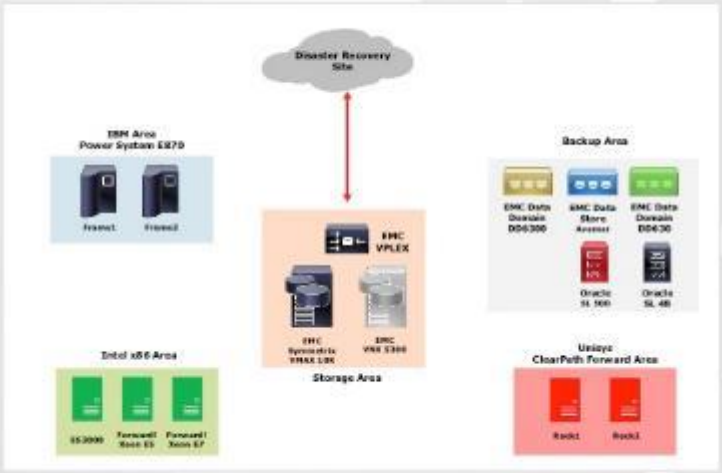
- On-Line Services (Citizen, Companies, Internal Employee)
  - ✓ Civil Registry
  - ✓ Certificates
  - ✓ Tax-Related
  - ✓ Payment
- Internal Applications
  - ✓ Accounting - Finacial
  - ✓ Human Resources
  - ✓ Infrastructure
  - ✓ Payment

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE

MAIN AREAS



ROMA CAPITALE

INTEL X86 AREA

- Microsoft Hyper-V Infrastructure
- Over 60 Applications
- DMZ Network

	ES3000	Forward! Xeon E5	Forward! Xeon E7	Total
CPU Type	Intel E7-4650	Intel E5-2667 v2	Intel E7-4890 v2	
Core	256	128	360	744
RAM (Gb)	1024	1024	3072	5120
Virtual Machines	75	146	105	326

ROMA CAPITALE

IBM AREA

- Internal Network
- Back-End Systems
- Over 50 Applications

	IBM E870 Frame 1	IBM E870 Frame 2	Total
CPU Type	Power 8@4.19Ghz	Power 8@4.19Ghz	
Core	36	36	72
RAM (Gb)	1280	1280	2560
Logical Partition (Lpar)	88	89	177

ROMA CAPITALE

UNISYS CLEARPATH FORWARD AREA

- Internal Network
- Demographic – Census – Election Process Applications
- Mainframe OS2200 Operating System

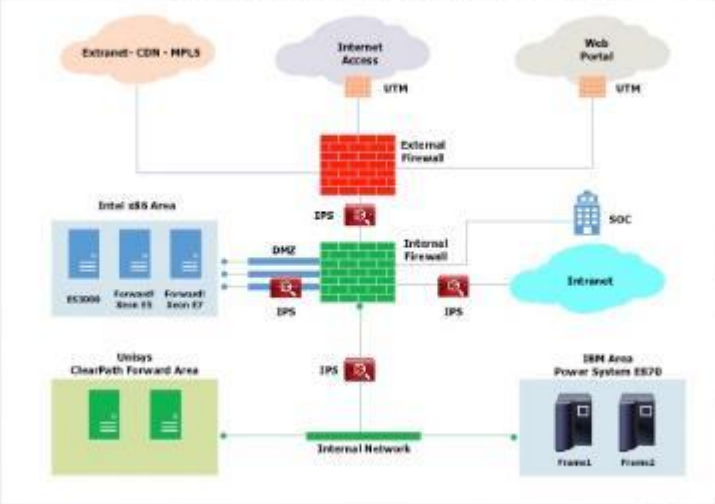
	Production System	Development System	Total
CPU Type	Intel E5-2600 v2	Intel E5-2600 v2	
CPU	11	8	19
RAM (Gb)	256	256	512
MIPS	4200	200	4400

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE

IT SECURITY INFRASTRUCTURE



CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE

IT SECURITY INFRASTRUCTURE COMPONENTS

- Firewall - Intrusion Protection/Detection Systems (over 1 Million IPS alarms per month)
- Central Log Collector - SIEM
- Monthly Vulnerability/Security Incidents Reports
- Central Management (SOC)
- Physical Security Assessment
- Security Policies Authorization/Validation Process

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY


ROMA CAPITALE
DATA CENTER EVOLUTION
New Networking Infrastructure Design (Spine-Leaf)
Security Infrastructure Development
Improve Web Application Security (WAF)
Protection of servers at the hypervisor level.
Protection of individual server instances.
Sandboxing/Advanced Malware Protection
Data Center Centralized Management (Orchestrator Tools)
Technology Lock-In Mitigation
Open Source Oriented Applications
Application Containers Evaluation
Private Cloud for Disaster Recovery and Backup
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY
ROMA CAPITALE
Thank you
Roberto Massimiliani
Roma Capitale
roberto.massimiliani@comune.roma.it
0667103943
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY


ROMA CAPITALE
AGENDA
Department of Technological Innovation (DIT) overview
"On going" Main Projects
Innovation Cross Projects
Focus: New Portal
Procurement procedures and contracts
E-procurement for Public Administrations
Agenda
1.
2.
3.
CS-AWARE – Workshop – Rome Oct, 16-20 2017
CS-AWARE CYBERSECURITY
ROMA
CS-AWARE
CS-AWARE CYBERSECURITY
Topic DS-02-2016:
Cyber Security for SMEs: local public administration and individuals
Main Projects, Services and Contracts
CS-AWARE – Workshop – Rome Oct, 16-20 2017

DEPARTMENT OF TECHNOLOGICAL INNOVATION

ROMA CAPITALE

- The Department of Technological Innovation (DIT) is a staff structure of Roma Capitale.
- Its aims are:
  - as procurement station, to launch public tenders relating to contracts for ITC services and supplies
  - management of the technological environment
  - monitoring of the ICT contracts
  - innovative development of the information systems
  - maintenance of the online services provided by the city portal
  - to carry out the principles and guidelines of the Digital Agenda
  - to support the day-to-day work of the «administrative machine» (Smart Governance)
  - to support the erogation of efficient services toward citizens and companies (Smart City), in order to ensure a continous improvement of the relationship between citizenship and PA

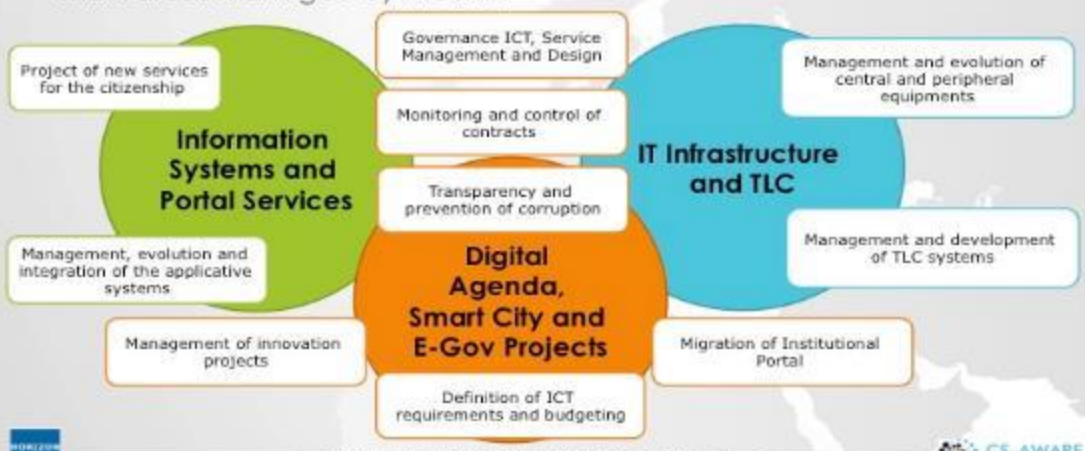
CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

DEPARTMENT OF TECHNOLOGICAL INNOVATION

ROMA CAPITALE

- Main areas managed by the DIT :

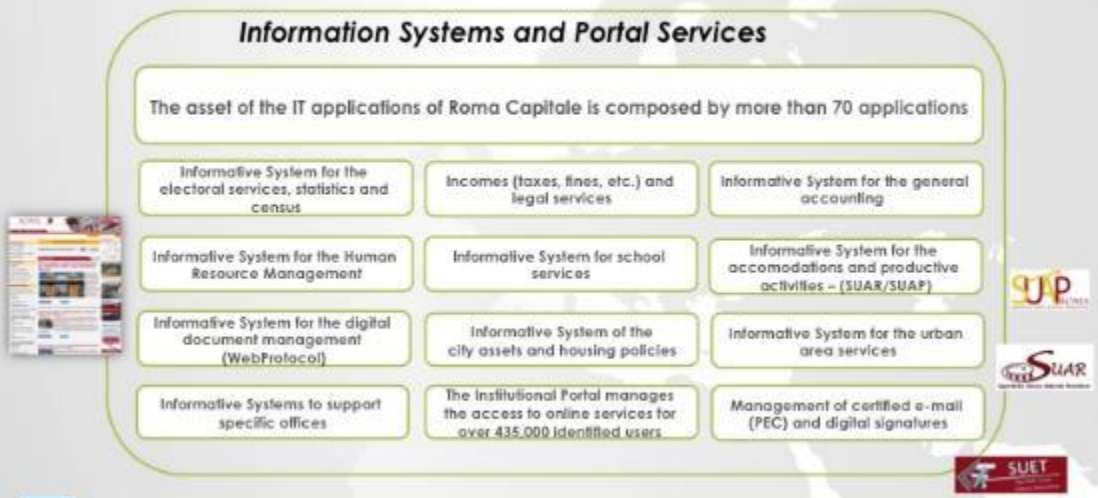


CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

INFORMATION SYSTEMS AND PORTAL SERVICES OVERVIEW

ROMA CAPITALE



CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE
Department of Technological Innovation

IT INFRASTRUCTURE AND TLC OVERVIEW

IT Infrastructure and TLC

The ICT infrastructure supports approximately 200 municipal offices, of which 150 are served by the broadband fiber network and approximately 1000 schools connected to the data network and land lines

Assisting services for around 14,000 workstation (office desks) and over 70 peripherals servers (Fleet Management)

Management of the offices equipped with over 15,000 land lines and about 1,100 mobile phones

Content Filtering and Computer Security

Management of 12 repeaters in the territory serving 3500 terminals of the TETRA mobile radio network for the Local Police

Data Center and Disaster Recovery

Management of peripheral equipment and SW licenses

Handling of 1200 Wifi access points (DigitRoma) that guarantee free internet connection for the citizenship

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE
Department of Technological Innovation

"ON GOING" MAIN PROJECTS

- Multi-year public tenders for purchasing assistance and maintenance services on information systems and infrastructures:
  - Population Information System (SIPO)
  - Digital Document Management (Protocollo Web - GED)
  - Educational Information System (MESIS)
  - Urban Area Information System (SIT-I)
  - Information System for Accomodation and Productive Activities (SUAR/SUAP)
  - Information System for Incomes
  - Information System for Human Resource and Accounting Areas (SAP)
  - Information System for Contracts Management
  - Web Portal for Digital Home of the Citizen
  - ...
- System Assistance Services and Management of Data Center Hardware and Software
- New Framework Agreements on the Public Electronic Market Platform for the TLC Services (telephony, network, broadband connection....)

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE
Department of Technological Innovation

INNOVATION CROSS PROJECTS

- The Innovation Cross Projects (ICP) involve many structures of Roma Capitale.
- In the following the list of the main «on going» cross projects:
- **New Portal:** to implement the new Rome Capital web portal and to ensure its design in a "citizen-centric" way
- **Open Data:** to implement the new Open Data web portal and to ensure its design in a "citizen-centric" way
- **New Geographic Information System (NIC):** to implement the NIC as the unique geographic information system of Rome Capitale
- **Unique access for citizen (a direct line to report issues):** to implement a unique web responsive platform able to handle reports and messages sent by citizens to Roma Capitale

CS-AWARE – Workshop – Rome Oct, 16-20 2017

CS-AWARE CYBERSECURITY

ROMA CAPITALE
Department of Technological Innovation

FOCUS: NEW PORTAL

- The new Rome Capital portal is a highly complex project that involves not only the Department of Technological Innovation (DIT), but all the structures responsible for providing information and/or online services to the citizenship

Actual Web Portal

- 12 years old
- 350 / 500 daily published news
- 249 active editors
- 312.000 external registered users
- 60.000 / 85.000 daily visitors
- Digital ecosystem consisting of more than 200 sites
- More than 70 online services

WWW.COMUNE.ROMA.IT

ROMA CAPITALE
Department of Technological Innovation

FOCUS: NEW PORTAL

- Actual Web Portal weak points:
  - Contents tailored to the administrative structures of Roma Capitale and not to the citizen needs
  - Contents not updated
  - Difficulty in retrieving information
- Aim: switching from the «silos-based» model to a shared model where the services and information are organized in a more «citizen driven» approach, thus improving the easiness and the efficiency of use

- SERVICES
- NEWS
- PARTICIPATE
- CONTACTS
- ...

ROMA CAPITALE
Department of Technological Innovation

FOCUS: NEW PORTAL

- The main objective is to provide a unique tool, easy-to-use, focused on citizen's needs and based on thematic areas, that allows to find and to use services and information

FOCUS: NEW PORTAL

ROMA CAPITALE
Department of Technological Innovation

- The new version will be available with online services compliant with the following requirements:
  - Responsiveness
  - Usability
  - Accessibility
  - Brand identity
  - Transparency

- In order to achieve the project objectives, a cross engagement of the stakeholders has been needed with the coordination/governance of the Department (Assessorato) "Roma Semplice" based on a change management strategy

PROCUREMENT PROCEDURES AND CONTRACTS

ROMA CAPITALE
Department of Technological Innovation

- All services and applications are provided through contracts signed with economic operators (firms)
- Both the previous Code for Public Contracts (Legislative Decree 163/2006) and the current Code of Public Procurement and Concession contracts (Legislative Decree 50/2016) discipline procurement procedures (public tender) and the subsequent contracts
- According to the Public Contract Codes, Public Administrations are required to use the IT public platforms in order to purchase goods and services
- The Italian Public Administration e-Marketplace (MePA) is a procurement platform managed by Consip, a public stock company entirely owned by Italian Ministry of Economy and Finance (MEF)
- Consip is committed to elaborate and implement framework agreements (conventions) with goods and services suppliers in order to reduce public procurement costs thanks to economy scale and process rationalization

E-PROCUREMENT FOR PUBLIC ADMINISTRATIONS

ROMA CAPITALE
Department of Technological Innovation

- The MePA is a virtual market in which any PA can buy goods and services offered by several suppliers
- The entire process is digital, using a digital signature in order to ensure legal compliancy and overall transparency of the process. It works just like a real market, as the same products can be found and are sold by several suppliers at different prices, terms and conditions

WWW.ACQUISTINRETEPA.IT

- The main advantages of the Electronic Market for Public Authorities are:
  - Time savings
  - Transparency and monitoring of the entire purchasing process
  - Wider possibility to choice among various offers
  - Meeting specific requirements through a wide and varied offer of available products and the possibility to request offers

ROMA CAPITALE
Department of Technological Innovation

E-PROCUREMENT FOR PUBLIC ADMINISTRATIONS

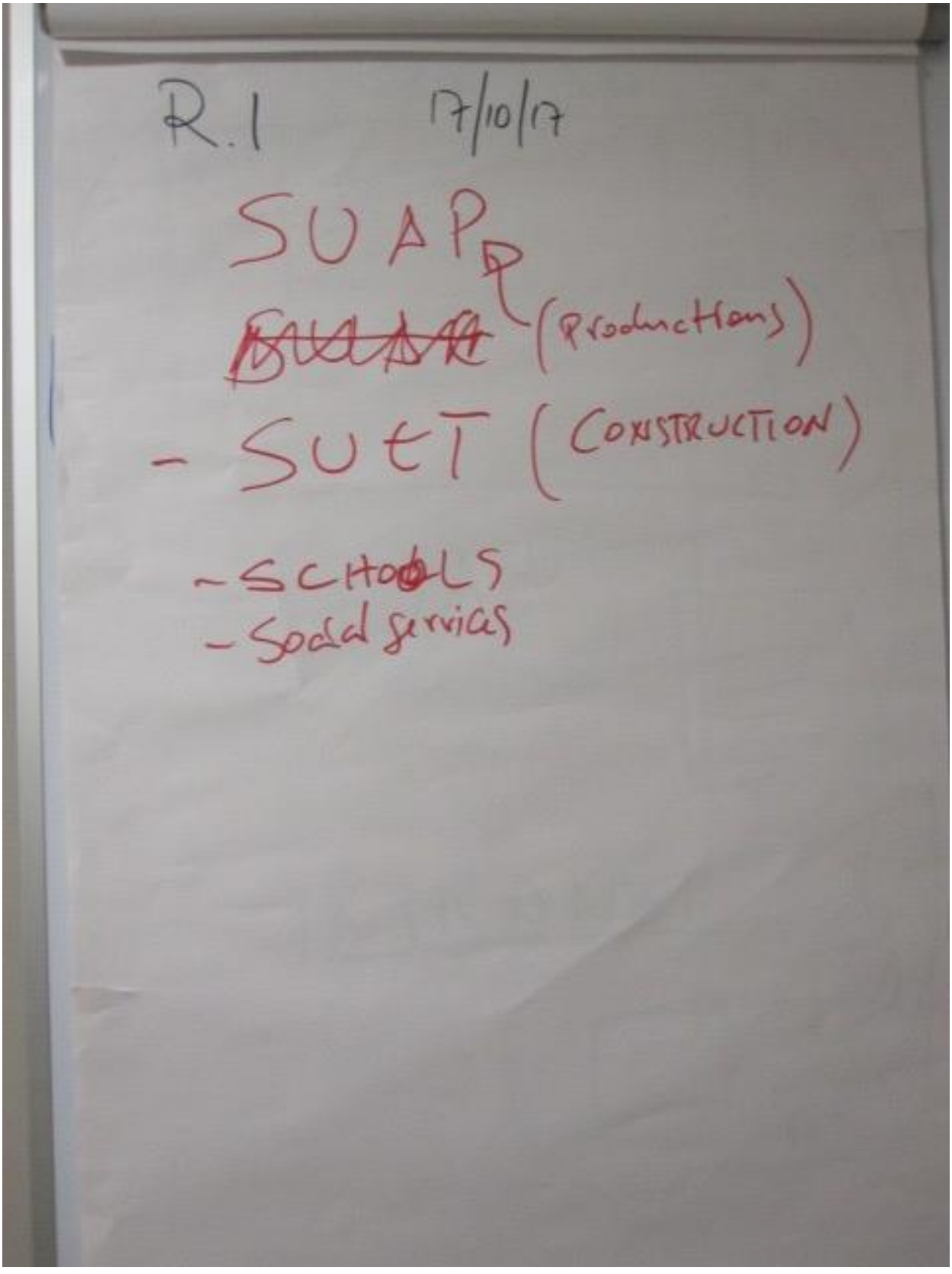
- Public Administrations can purchase goods and services on the e-Procurement platform by means of two alternative buying options:
  - Direct Order (ODA): making a direct purchase selecting goods and services from the eCatalogue
  - Request for Quotation (RDO): negotiating the product quality and service levels with qualified firms (handling on-line the entire purchasing process)

ROMA CAPITALE
Department of Technological Innovation

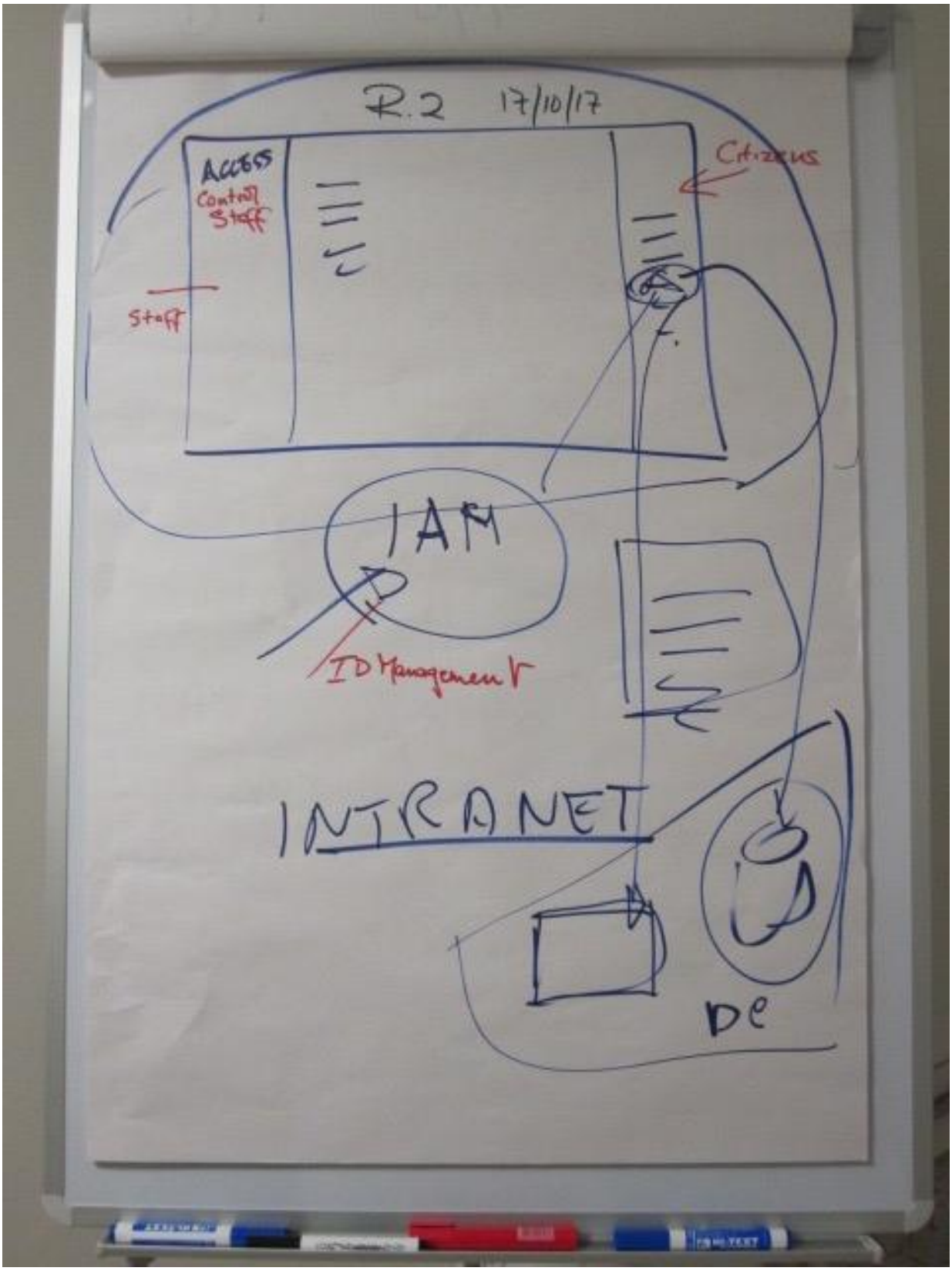
Giuseppe Bartoli
Silvia Guglielmucci
Department of Technological Innovation – Roma Capitale
giuseppe.bartoli@comune.roma.it
silvia.guglielmucci@comune.roma.it

Rich Pictures

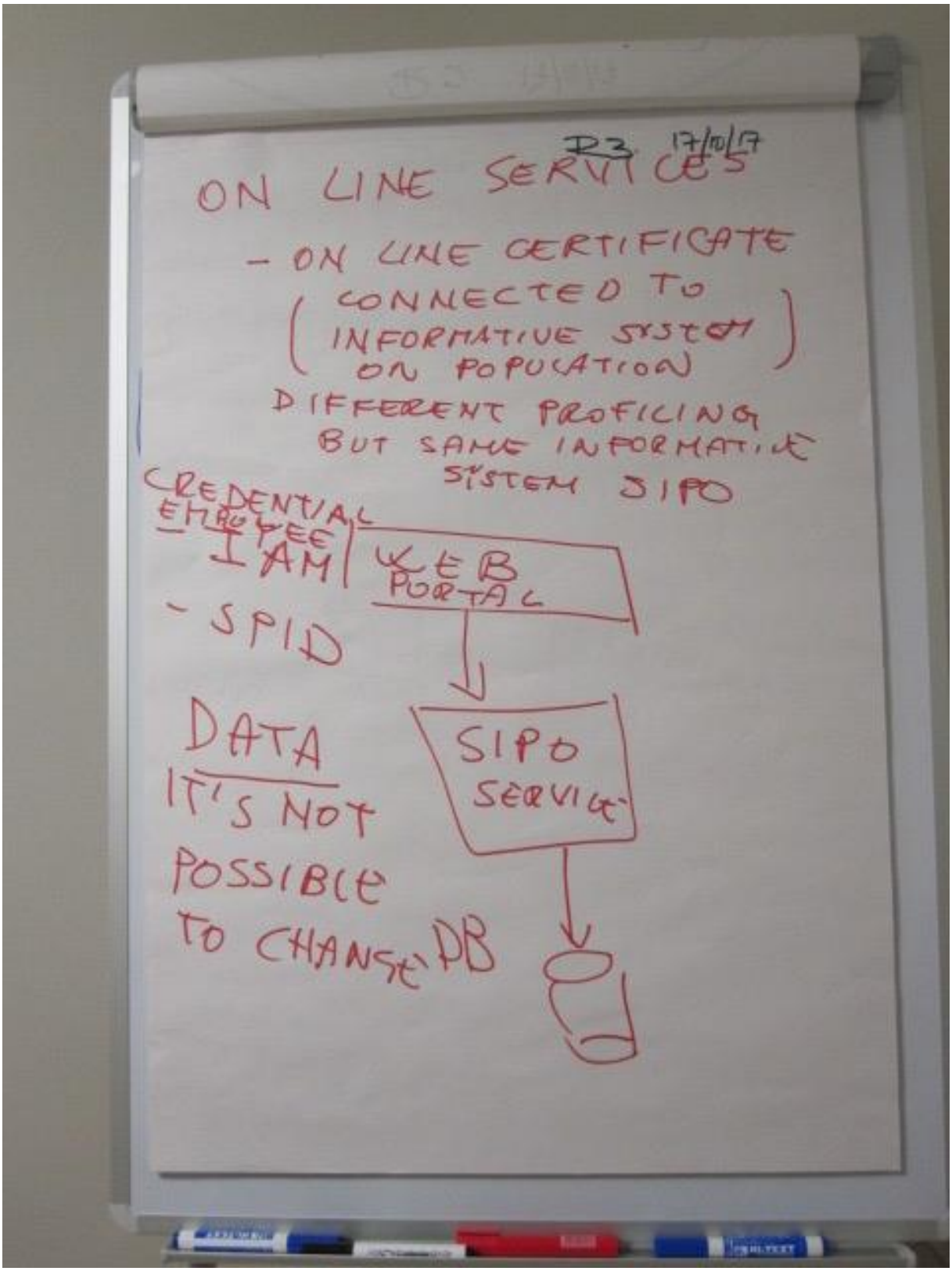
RP 1



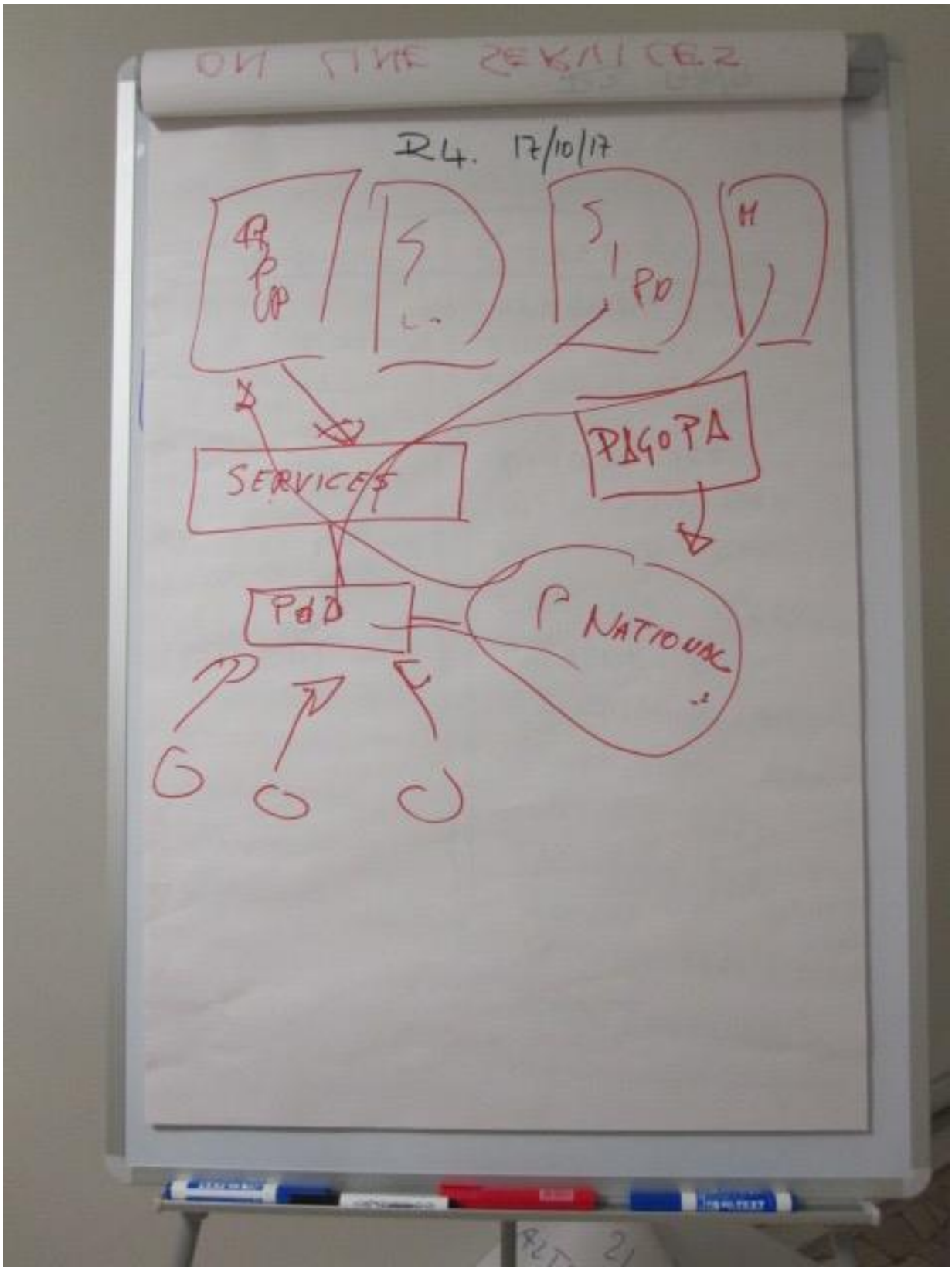
RP 2


R.2 17/10/17
ACCESS
Control
Staff
Staff
Citizens
IAM
ID Management
INTRANET
DC

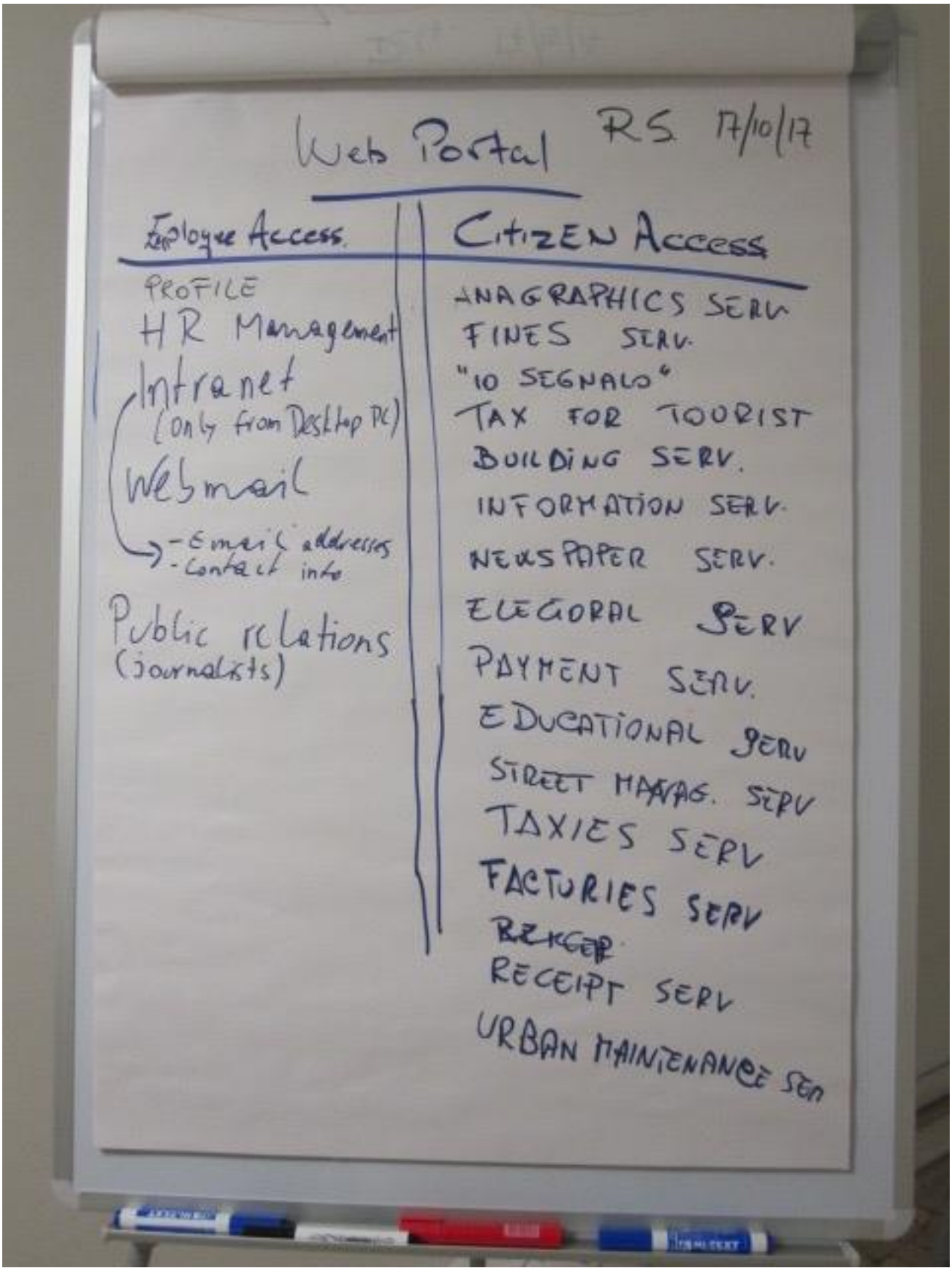
RP 3


R3 17/10/17
ON LINE SERVICES
- ON LINE CERTIFICATE
(CONNECTED TO INFORMATIVE SYSTEM ON POPULATION)
DIFFERENT PROFICING BUT SAME INFORMATIVE SYSTEM SIPO
CREDENTIAL
EMPLOYEE
I AM
- SPID
WEB PORTAL
SIPO SERVICE
DATA
IT'S NOT POSSIBLE TO CHANGE DB

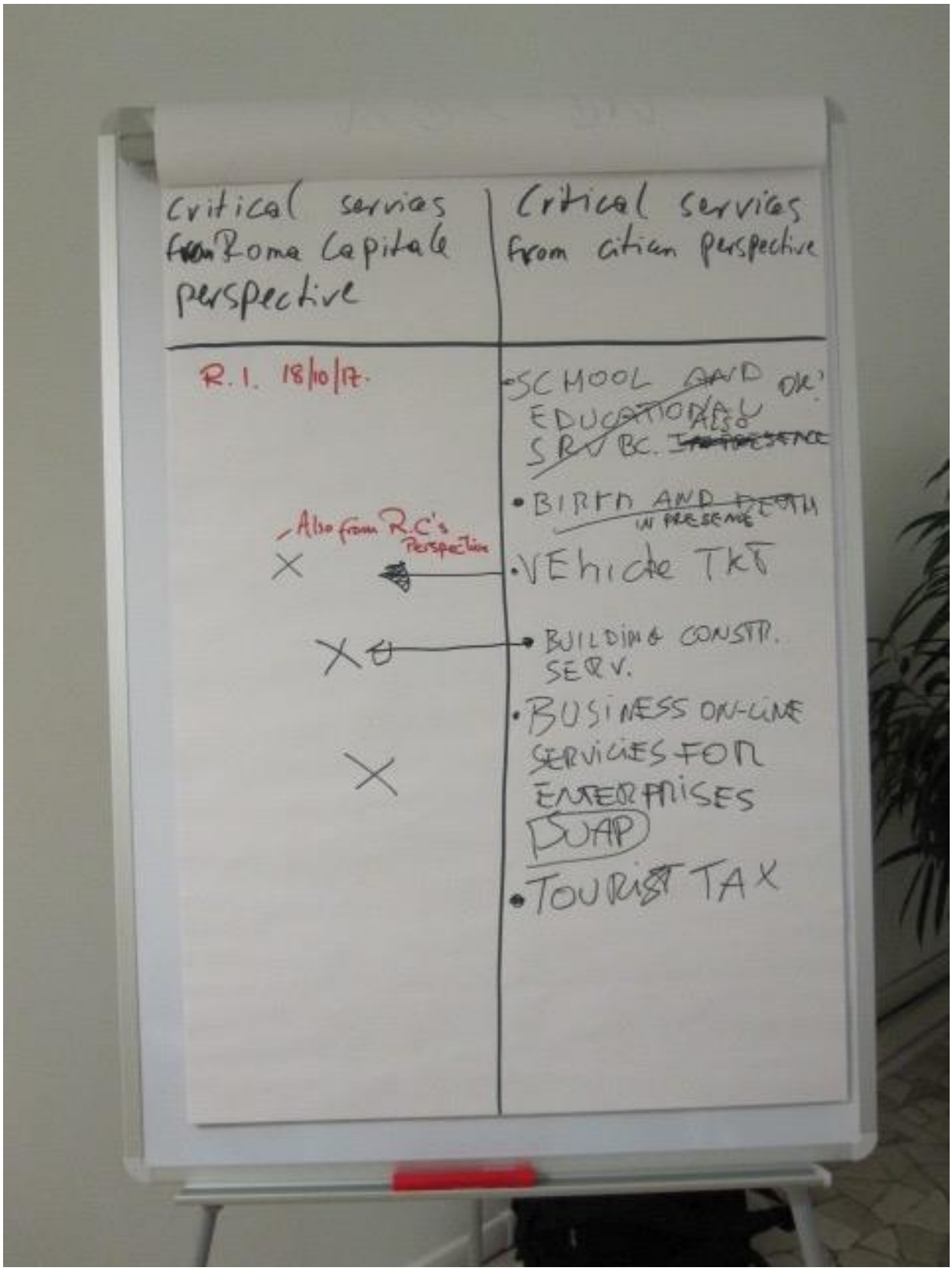
RP 4



RP 5


Web Portal
RS 17/10/17
Employee Access
PROFILE
HR Management
Intranet
(only from Desktop PC)
Webmail
- Email addresses
- Contact info
Public relations
(Journalists)
Citizen Access
ANAGRAPHICS SERV
FINES SERV.
"10 SEGNALO"
TAX FOR TOURIST
BUILDING SERV.
INFORMATION SERV.
NEWSPAPER SERV.
ELECTORAL SERV
PAYMENT SERV.
EDUCATIONAL SERV
STREET MANAG. SERV
TAXIES SERV
FACTORIES SERV
RECEIPT SERV
URBAN MAINTENANCE SER

RP 6

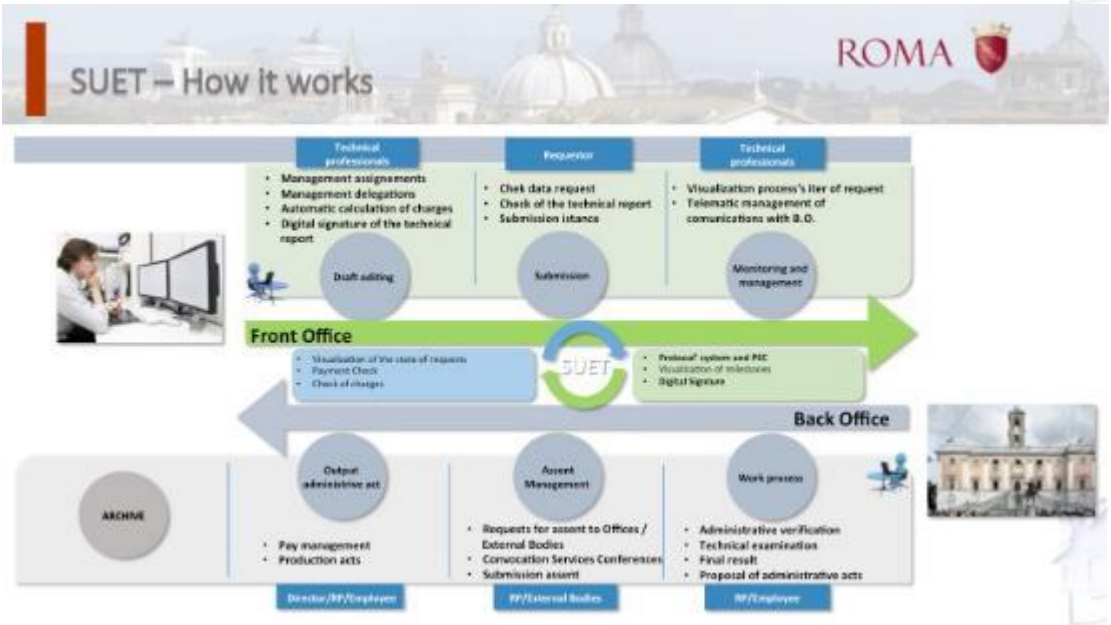

Critical servies from Roma Capitale perspective
Critical servies from citizen perspective
R.1. 18/10/17.
SCHOOL AND EDUCATIONAL SERV. ALSO BC.
BIRTH AND DEATH IN PRESENCE
Also from R.C's Perspective
VEHICLE TKT
BUILDING CONSTR. SERV.
BUSINESS ON-LINE SERVICES FOR ENTERPRISES
SUAP
TOURIST TAX

Annex 4

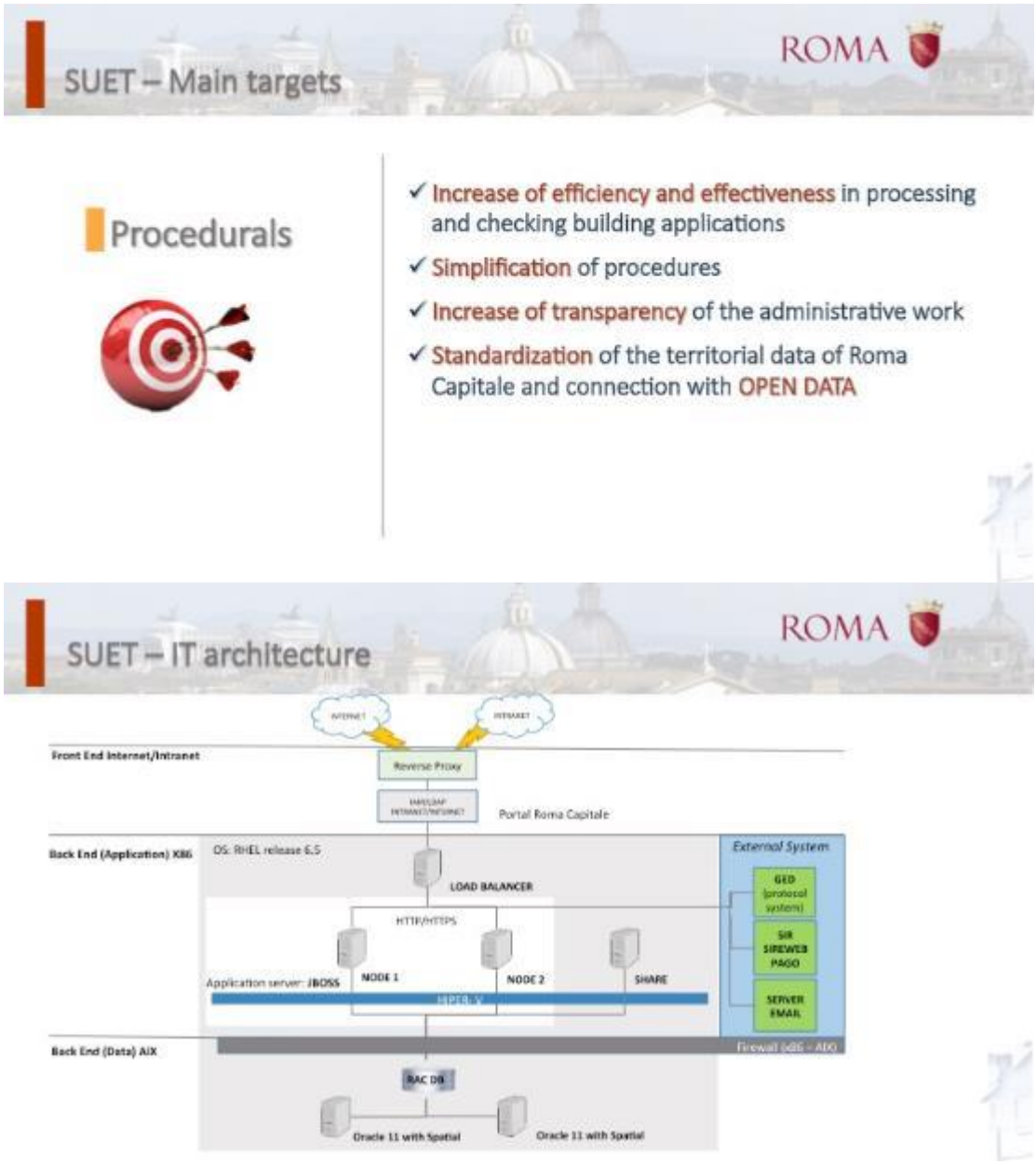
Presentations slides describing a high level overview of the SUET service

SUET - Sportello Unico per l'Edilizia Telematico


SUET - Actors
ROMA
Front Office
Back Office
SUET
• Citizens – Requestors
• Professionists – Technical professionals registered on SUET and delegated by the requestors
• Director of Office
• Responsible of Work process (RP)
• Techincal Employee


SUET – How it works
ROMA
Technical professionals
Requestor
Technical professionals
• Management assignements
• Management delegations
• Automatic calculation of charges
• Digital signature of the technical report
• Chek data request
• Check of the technical report
• Submission istance
• Visualization process's iter of request
• Telematic management of comunications with B.O.
Draft editing
Submission
Monitoring and management
Front Office
SUET
Back Office
ARCHIVE
Output administrative act
Assent Management
Work process
• Pay management
• Production acts
• Requests for assent to Offices / External Bodies
• Convocation Services Conferences
• Submission assent
• Administrative verification
• Technical examination
• Final result
• Proposal of administrative acts


SUET – What is it?
ROMA
End to end management of processes for the editing, submission and processing of building requests (permits, sanctions and so on)
Creation and submission of requests for building permissions and building sanctions
Back Office due diligence
Administrative verification
Technical examination
Pay management
Final result
Output act (Creation of building permissions/sanctions)
Requests for assent to Offices / External Bodies / Conferences
Telematic sending of communications by protocol's system and PEC
Access to GIS services and Web Portal
SUET


SUET – Main targets
ROMA
Procedurals
✓ Increase of efficiency and effectiveness in processing and checking building applications
✓ Simplification of procedures
✓ Increase of transparency of the administrative work
✓ Standardization of the territorial data of Roma Capitale and connection with OPEN DATA
SUET – IT architecture
ROMA
Front End Internet/Intranet
Reverse Proxy
Portal Roma Capitale
Back End (Application) X86
OS: RHEL release 6.5
LOAD BALANCER
External System
HTTP/HTTPS
Application server: JBOSS
NODE 1
NODE 2
SHARE
SERVER EMAIL
Back End (Data) AIX
RAC DB
Oracle 11 with Spatial
Oracle 11 with Spatial

Rich Pictures and Commentary

Team 1 RP 1

There are two sites one in Milan and one in Rome. In Milan there are 2 data centers in two different locations in the city of Milan, working as an active-active cluster according to a Business Continuity architecture. The data centers in Milan are owned by Fastweb (a supplier), that also provides RC with Internet and network perimeter security services. Fastweb has its own Disaster Recovery site in Rome to ensure compliance with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) needed by RC. RC's main data center is located in Rome and it is duplicated in Perugia, for disaster recovery purposes. The site of Rome is connected with the site of Milan with two dedicated MPLS VPN links (1 Gbps each link). This network connection is geographically differentiated (each link has its own bidirectional path from Rome to Milan) to enhance reliability, service availability and network resilience. The RC portal (www.comune.roma.it) is on a server located in Milan, while the services (including SUET service) are located in Rome.
There is a front end user access for citizens to the Milan site, while employees can directly gain access to the Rome infrastructure. The mail server and related protection services are located in Milan. Security is enforced and monitored by following elements:

- DDoS mitigation services to protect the RC portal and e-mail services.
- Web Application Firewall to protect Roma Capital portal.
- Security Information and Event Monitoring capability to correlate events and alert for potential security issues.
- A Network Load balancer
- A Next Generation Firewall, both in Milan to protect the RC portal and e-mail services (network perimeter security) and another in Rome to protect each and every Web Service published by the RC portal home page (Data Center security). There are many firewall layers in this arrangement.
- IPS, both in Milan and Rome, deployed following the Next Generation Firewall architecture described above.

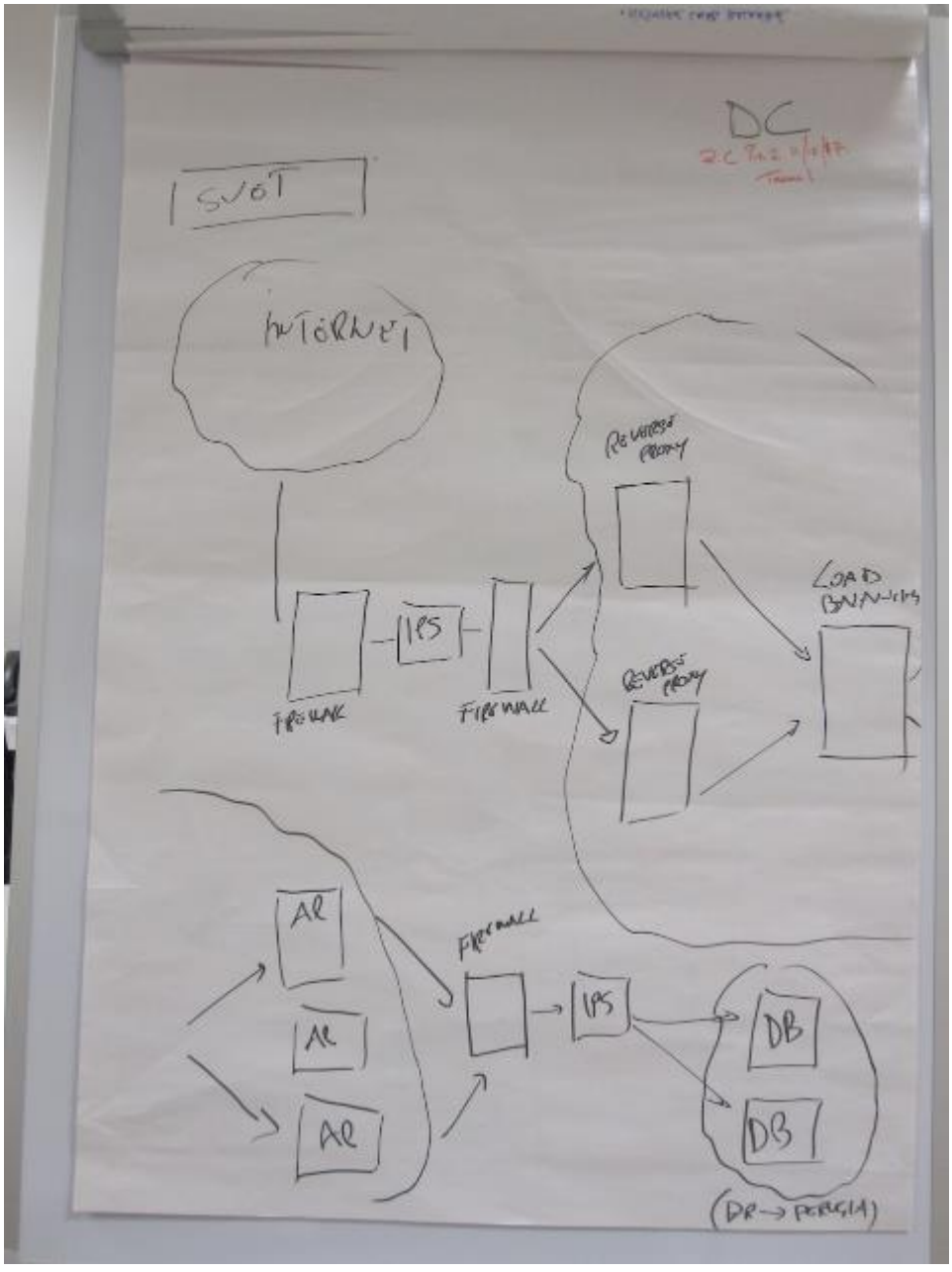

MILAN (FASTWEB PREMISES)
DATA CENTER 1
DATA CENTER 2
BUSINESS CONTINUITY
FRONT-END LAYER
SERVICE 1
SERVICE 2
SERVICE n....
SUET SERVICE
THE WEB PORTAL PUBLISHES MANY SERVICES
THOSE SERVICES LIVE IN ROME MAIN DATA CENTER INFRASTRUCTURE
MPLS VPN DEDICATED LINK PRIMARY LINK
MPLS VPN DEDICATED LINK SECONDARY LINK
DUAL INTERNET LINK 1 GBPS
INTERNET
CITIZEN
DUAL INTERNET LINK
ROME
MAIN DATA CENTER
PERUGIA
DISASTER RECOVERY SITE
BACK END LAYER

Team 1 RP 2

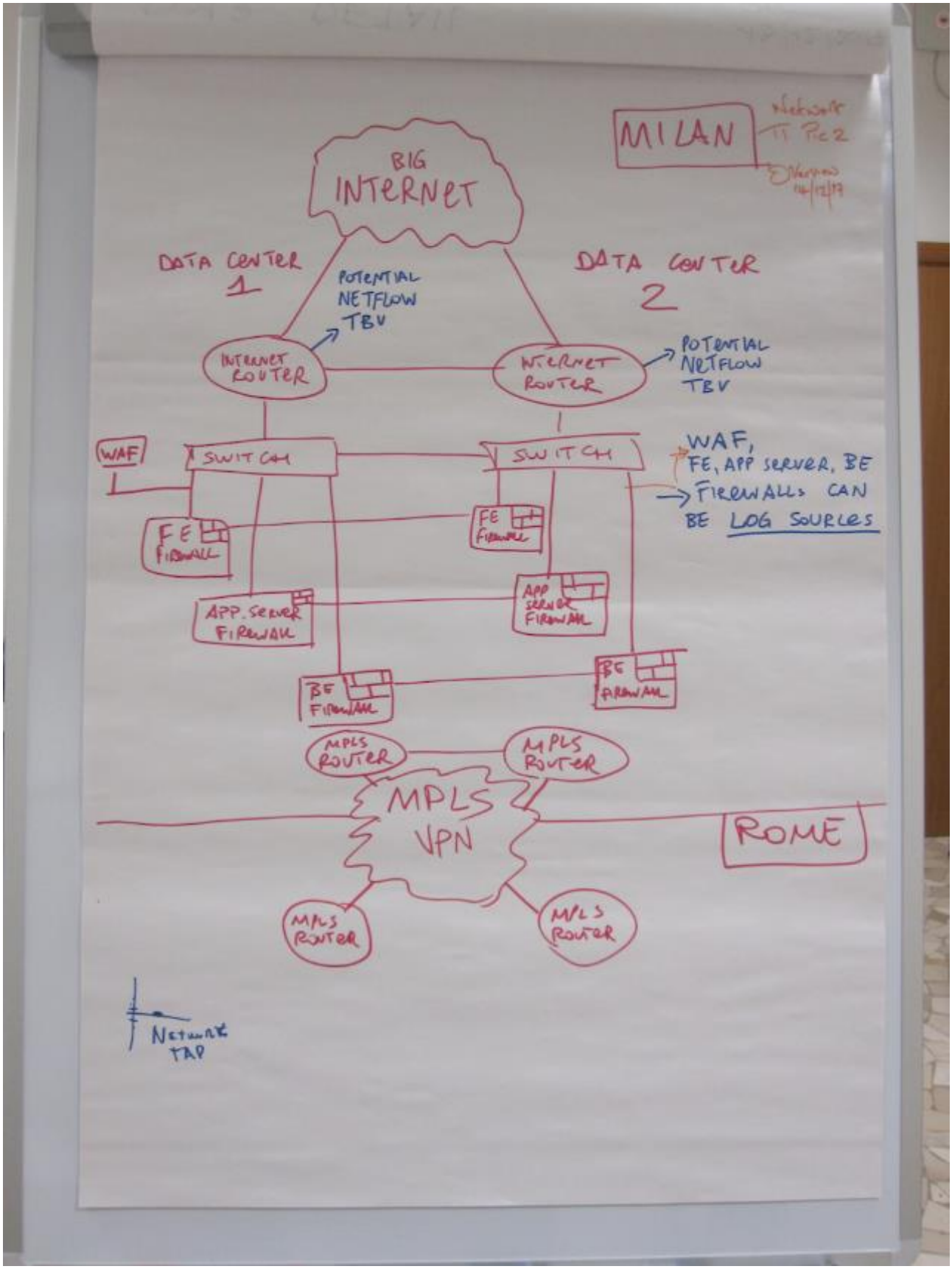
RP2 of team 1 is displayed in three different iterative versions (Team 1 RP2, Team 1 RP 2A and Team 1 RP 2A-V2). They depict the Internet Routers that are hosted on Fastweb premises in Milan, according to the previously described architecture of Team 1 RP 1. Possible monitoring points for CS-AWARE are pictured in Team 1RP 2A-V2. Potentially, Internet Routers can be configured collect IP Network traffic through, in example, the NetFlow feature. Network perimeter security devices hosted on Fastweb premises can potentially be log sources:

- Front End Firewall Cluster
- Application Server Firewall Cluster
- Back End Firewall Cluster
- Web Application Firewall

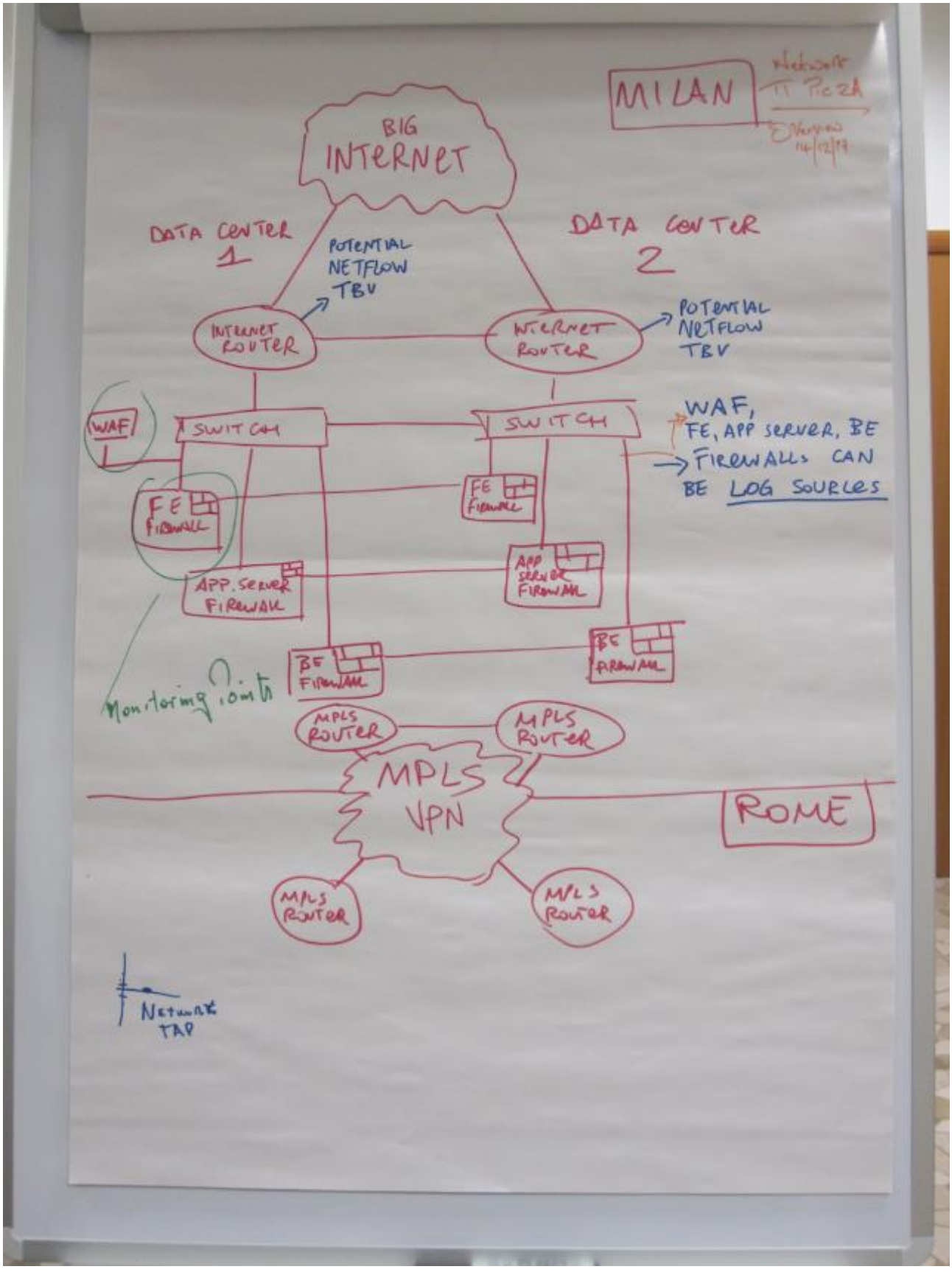
Version Team 1 RP 2



Version Team 1 RP 2A



Version Team 1 RP 2A-V2



Team 2 RP 1

This picture exhibits the authentication process to the RC's web portal and SUET service. This picture shows how both citizens and employees gain access to RC's web portal and to the SUET online service, along with the user authentication process. The process can split to the process into two phases:

- Authentication to RC's web portal
- Authentication to SUET system

In the first phase there are two kinds of users: Citizens and Employees.

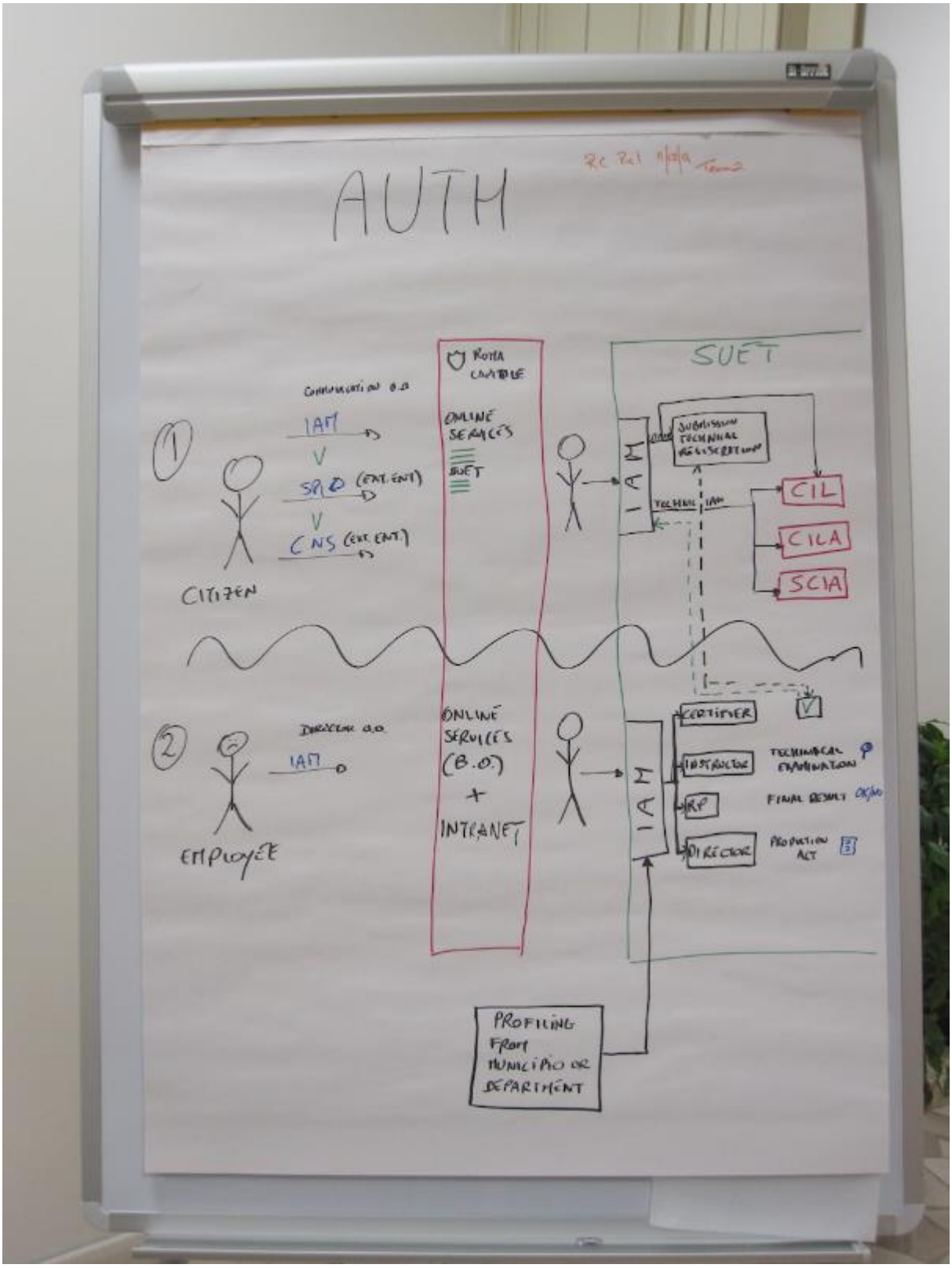
Citizens: For citizens there are three ways to access the web portal:

- Direct access via IAM (Identify and Access Management)
- Public system of digital identity (SPID) (external service)
- National services card (external service)

Through the RC web portal, the citizen can access online services and can interact with them. The SUET is the online service allows the users to submit planning and construction documentation.

Employees: For employees connect to the portal via the IAM service which allows access to the back end portal services and the intranet infrastructure. In the second phase users can connect to the SUET platform. If the user is a citizen s/he can have two different roles:

- S/he can submit the requests of building dossiers (CIL) as a citizen
- S/he can request to be identified as an SUET technician (engineer, quantity surveyor, architect, etc.).
- A SUET technician must be certified by the urbanistic department by a verification process.
- A citizen can manage only the CIL by himself, while to manage these CILA and the SCIA is requested the technician support.
- If a user is an employee, s/he can have different back office operator roles granted by the municipality structure or Urbanistic department -
- Certifier: verifiers a technician's identity and, if necessary, contacts the professional orders.
- Instructor: takes care of examining documents from a technical point of view
- Process manager: determines the financial outcome of the document or dossier (if OK or KO)
- Director: provides for the external rejection of applications, documents or dossiers.


AUTH
SUET
ONLINE SERVICES
SUET
CITIZEN
EMPLOYÉE
ONLINE SERVICES (B.O.)
+
INTRANET
IAM
CIL
CILA
SCIA
CERTIFIER
INSTRUCTOR
RP
DIRECTOR
PROFILING
FROM
MUNICIPIO OR
DEPARTMENT

RP IAM

As can be seen in the IAM RP (a substantiation of Team 2 RP 2), There are two different actors in the system:

1. Users
2. City Hall Operators

The user, as a citizen or as an employee:

- Can access the USER ON-LINE REGISTRATION if is not yet register in the system;
- Can modify some user account fields through ON-LINE SELF-SERVICE MANAGEMENT FUNCTIONS, if he is already registered;

The city hall operator can retrieve information about citizens using a specific application. The two kinds of requests that can come from users and the one kind of request that can come from the municipal operator, are processed by the Identity Manager (IDM). The IDM components are:

- Oracle Http Server (OHS),
- Oracle Identity Manager (OIM),
- Oracle Unified Directory (OUD),
- Web Logic (WL), Oracle DB (ODB).

The IDM creates a Virtual Identity of the new requesting user. The IDM service is accessed via the IDM console by the operator, in order to collect and the process requests. The operator is responsible for the assessment of the identity of the requesting user. The IDM and the IDM console are located in the Data Elaboration Office (Centro Elaborazione Dati – CED- of RC). The IDM is connected to different nodes:

- The ACCESS MANAGER (AM)
- The PROXY SERVER (PS)
- The MAIL SERVICE (MS)
- The REVENUE OFFICE (RO)

The IDM interacts with the AM, the PS, the MS; the RO acts only as a receiver of virtual identity information. The AM registers the new user and grants the access for his/her future access requests. The AM components are:

- Oracle Http Server (OHS),
- Oracle Access Manager (OAM),
- Oracle Unified Directory (OUD),
- Web Logic (WL), Oracle Database (ODB).

The AM is interrogated whenever a user logs into the web-portal or tries to access online services; it is also accessed by (internal) medical doctors via a health surveillance system. The PS, together with the Active Directory, registers the new employee-type user and allows these users to access Internet from within RC Offices. The MS registers the new employee-type user mail account and allows these users to use the mail service of RC.

Citizen Registration: The citizen registration can be achieved using basically three different systems:

1. The RC Website online direct service: In the first phase the citizen is expected to insert the basic information over an online form and to verify the correctness of his/her own email. In

the following step the requested documentation necessary for the legal identification of the user is sent by the same user to the RC back-office trough his/her email. The back office is responsible for controlling and approving the received documentation. If the documentation is correct, the citizen will be uniquely identified and will receive, through his/her email, the credentials for logging in the RC website.

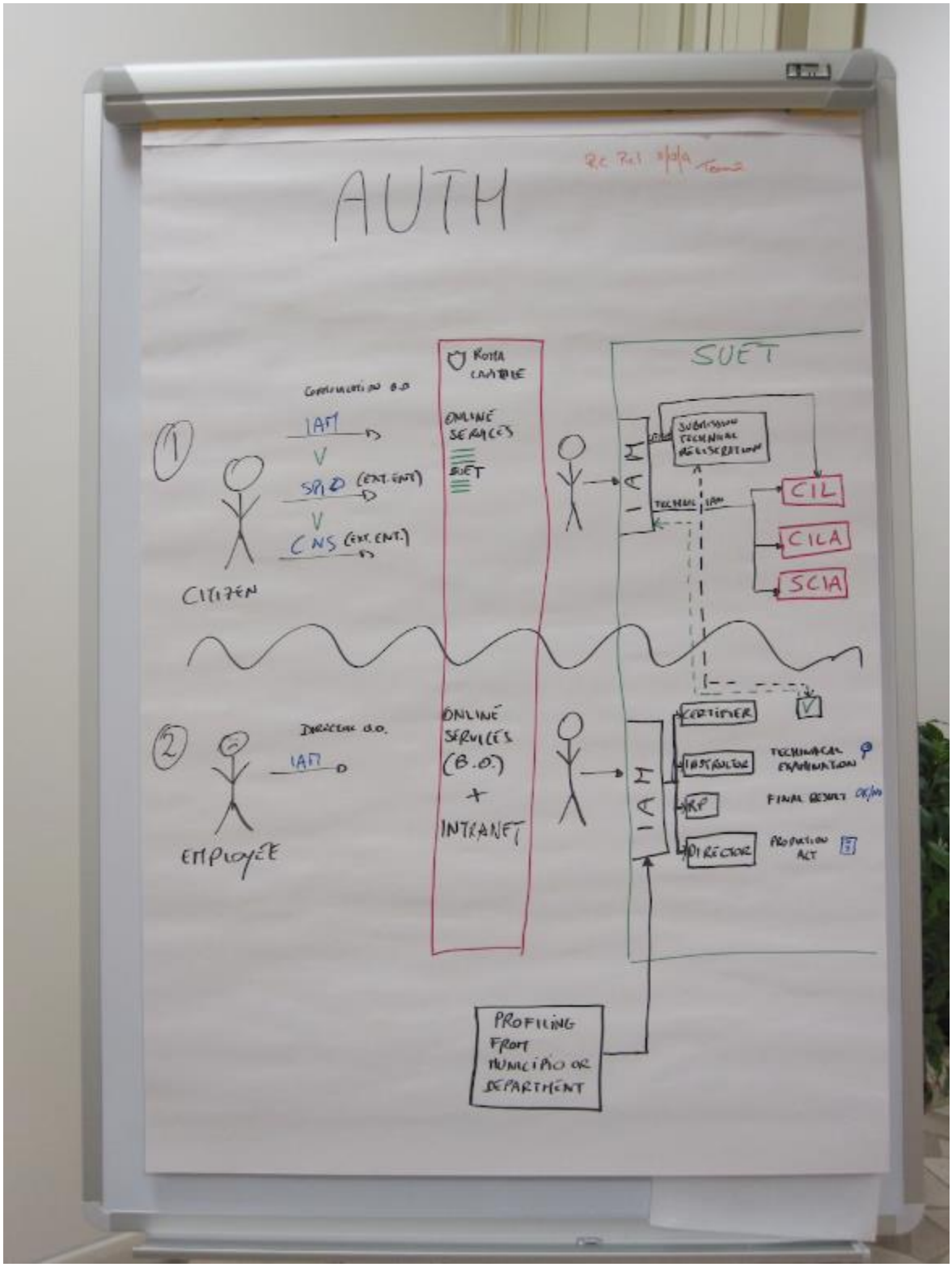
2. The RC SPID online service: In this case, the citizen has been previously identified by a certified Identity Provider by the SUET (the national agency for the digital transformation of the Public Administration that sets out "Minimum ICT Security Measures of Public Administrations"). The first time that the citizen logs into the RC website, using the previously received SPID credentials, s/he will be asked to fill a subscription form in order to gain access to the RC online services.
3. The City Hall desk: The citizen presents him/herself to the/his/her own city hall office where the operator carries out a face-to-face recognition. The operator inserts the citizen data using a specific form, located in the intranet. There is no need of a further elaboration by back-office operators. From this point on the citizen will be able to log in the RC website.

Employee Registration: The employee fills a "protected" form providing the requested information. S/he receives the contract in return. The contract must be signed both from him/her and from his/her director. The contract is sent to the back-office that verifies and approves the registration. Once this phase is completed, the employee is able to log in the RC website as an employee-type user. S/he can access the online services for the employees, the RC email system and can access the Internet through the RC proxy.

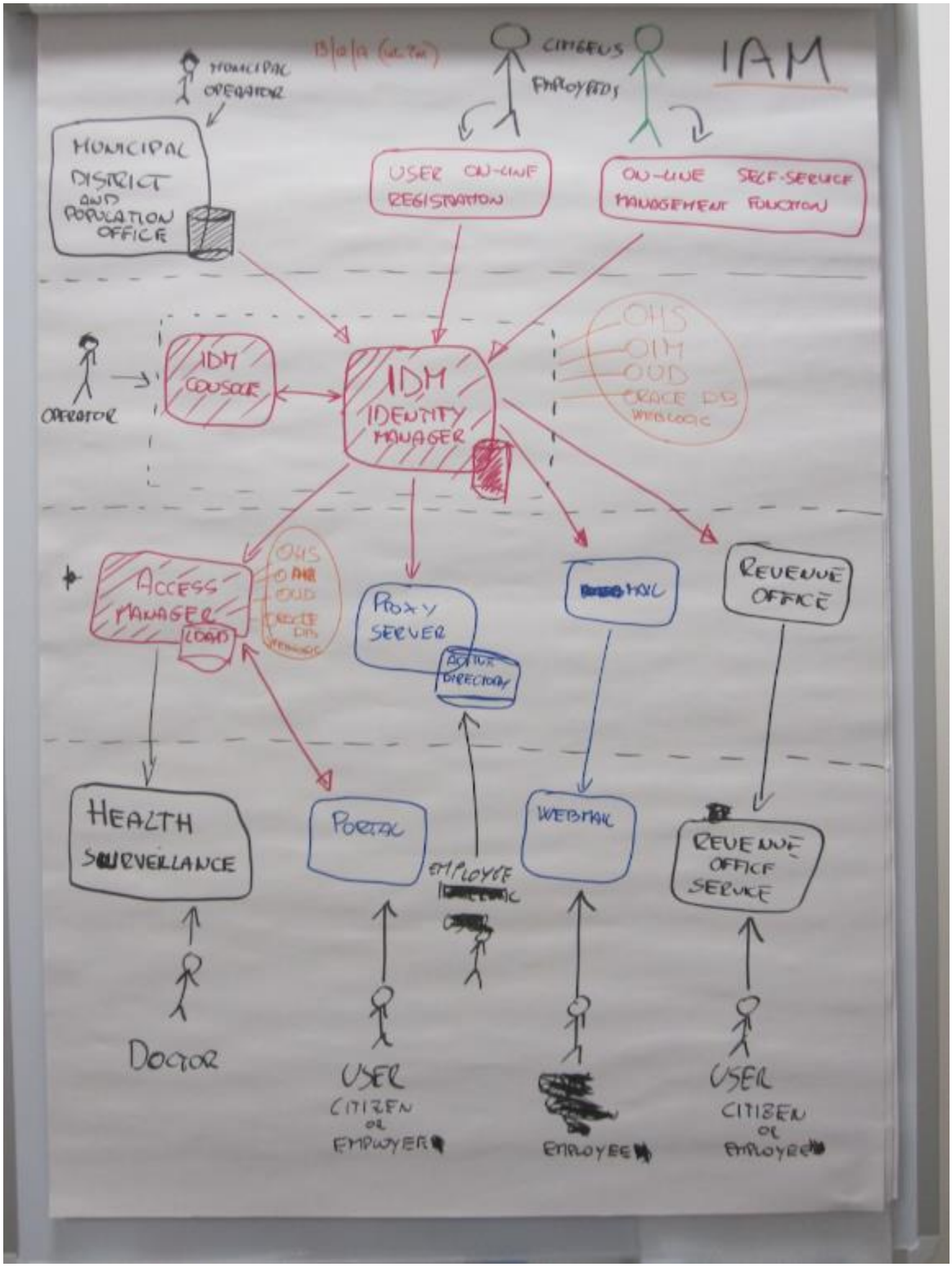
- Online self-service management function
- The citizen and the employee can change the password, can reset the password and can modify the registered data.
- ProxyServer / Active Directory

The IDM system manages the employee's identity inside the Active Directory System through the following actions: insert, modify, enable, profile and erase. The Proxy Server uses the employee credentials, defined and registered inside the Active Directory System, to authorize and profile the Internet browsing.
Mail: The IDM system manages the email box through the following actions: insert, modify, enable, profile and erase.
Access Manager: The IDM system manages the access to the online services handled by the Access Management. The Access Management system is "responsible" for the authentication phase (SPID, CNS, Username and Password) and for the authorization of the service access.
Revenue Office: The IDM system sends to Roma Tributi Service the data necessary for the tax payment. (The IDM system has no knowledge of any data related to the payments)
Health Surveillance: It is an online service for doctors; RC uses it for the medical examination of its employees.

Team 2 RP 2

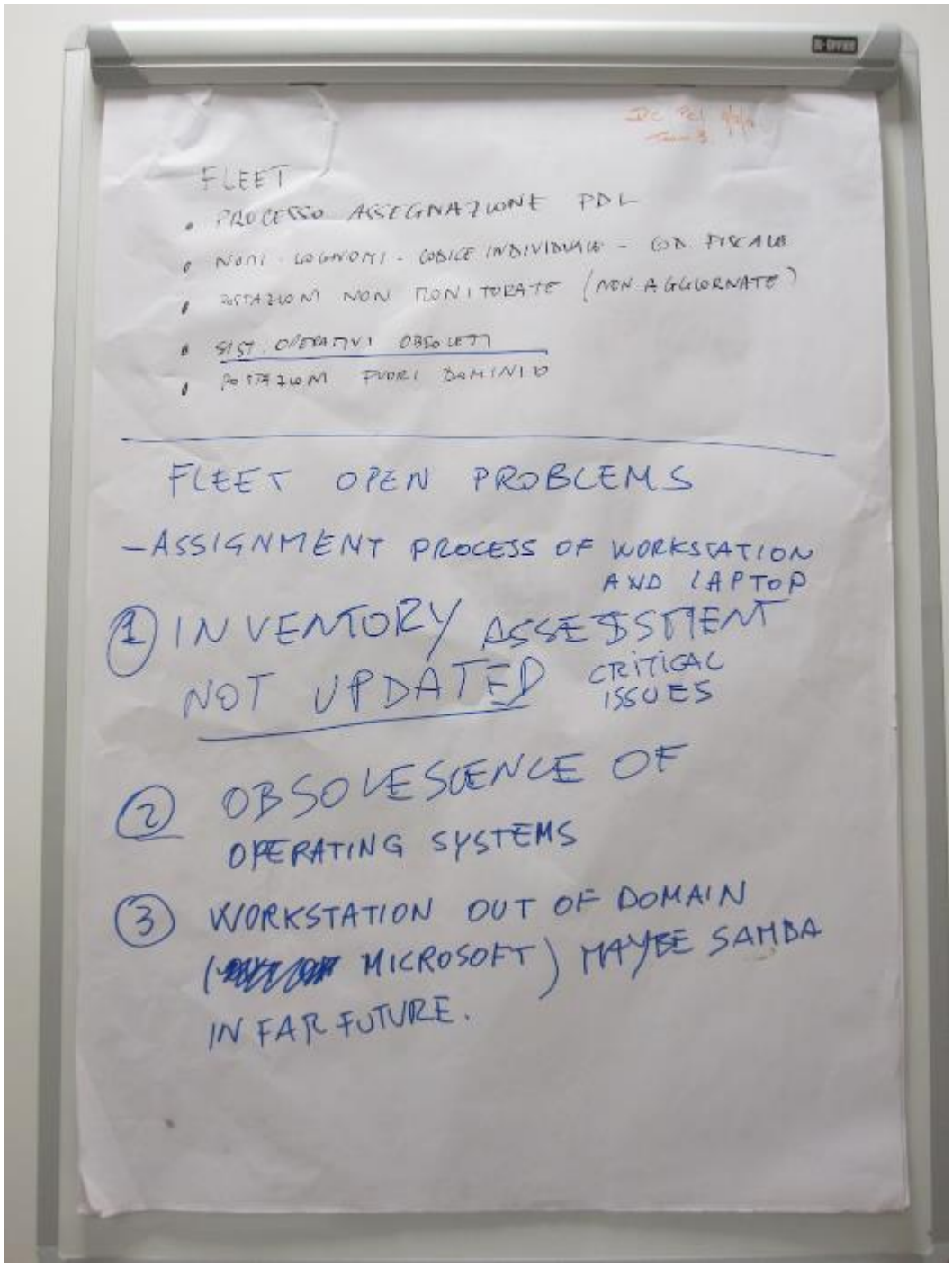

AUTH
SUET
CITIZEN
EMPLOYÉE
IAM
CIL
CILA
SCIA
ONLINE SERVICES
SUET
ONLINE SERVICES (B.O.)
+
INTRANET
CERTIFIER
PROFILING
FROM MUNICIPIO OR DEPARTMENT

RP IAM


IAM
CITIZENS
EMPLOYEES
MUNICIPAL DISTRICT AND POPULATION OFFICE
USER ON-LINE REGISTRATION
ON-LINE SELF-SERVICE MANAGEMENT FUNCTION
OPERATOR
IDM COUSCE
IDM IDENTITY MANAGER
OHS
OIM
OUD
ORACLE DB
ACCESS MANAGER
LOAD
PROXY SERVER
REVENUE OFFICE
HEALTH SURVEILLANCE
PORTAL
WEBMAIL
REVENUE OFFICE SERVICE
EMPLOYEE
DOCTOR
USER CITIZEN OR EMPLOYEE
EMPLOYEE
USER CITIZEN OR EMPLOYEE

Team 3 RP 1

This rich picture helped the team to identify open issues with the fleet management in Roma Capitale and was mainly drawn to help Team 3 to better understand the situation. Those thoughts are incorporated in the next version of the picture (Team 3 RP2) and are described there, if relevant. The design aims to highlight the fact that the fleet management office plays a transversal role for the entire organization. Feeling the needs of the local and central structures, it provides the necessary hardware and software resources both to the individual worker and to the structure that requests it. Software distribution and status is monitored by Microsoft sccm (service center configuration management).The knowledge of the instrumental equipment (understood as knowledge of location, user, ...) is of fundamental importance to avoid wastes as well as, in the security field, to be aware of the correct use of the tools available and monitor the deadlines of support for the various software.

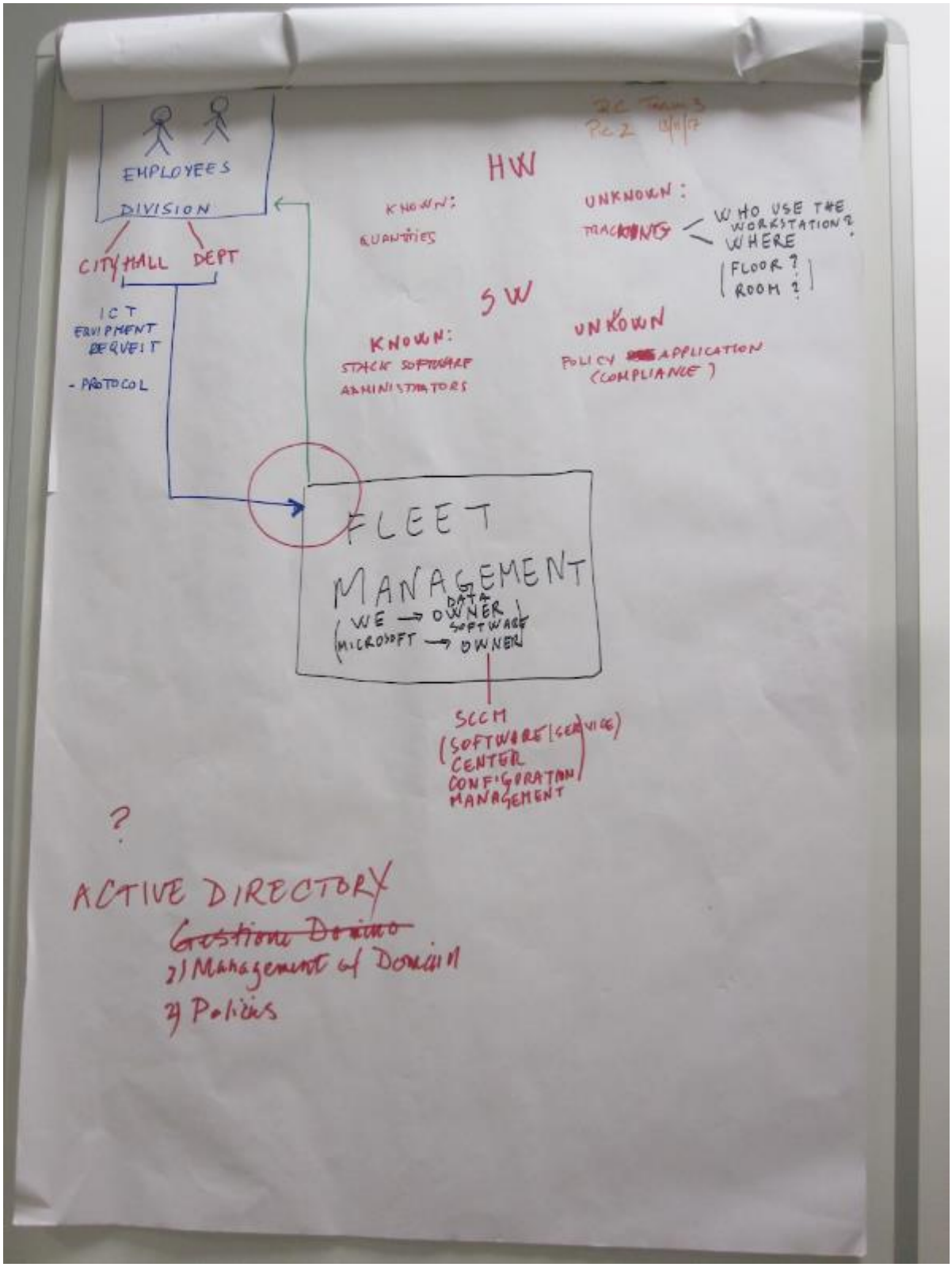


Team 3 RP 2

As part of the process on migration from proprietary systems to floss systems, the preliminary phase of study has highlighted a series of potentially dangerous aspects in the field of security. At present the Technological Innovation Department almost perfectly knows the exact location of the Administration of desktops, however only 10% of these are associated with the name of an assignee or user employee. Regardless of how much this lack of knowledge can affect the decision to limit Microsoft Office licenses in favour of other open source products, there are several technical problems that strongly limit the ability to be capillaries. Many workstations are not reachable because they are out of the domain or due to software problems that make them even if they are in domain.

In our administration no user has administrator powers except for local contacts, who are in possession of the requirements and can therefore administer the entire structure in which they work. Obviously local contacts do not have the credentials to perform the domain administration. However, they are not prevented from adopting unofficial practices that are not entirely lawful and that can be perpetrated “in the friendship”, making it possible for those without administrative powers to install software without the prior authorisation. In a report for the month of April, it was highlighted that there are 15,000 non-authorised software installations in the City’s machine stock provided to employees, which may be running unlicensed software.

At present, around one thousand out of fifteen thousand workstations in City’s machine stock asset register that are not monitored and it is legitimate to assume that they do not receive centrally distributed updates of the operating system antivirus all security patch. The presence of unsupported operating systems, makes it particularly risky to use the machines that host these OS’s that can of course, gain access the Internet. Software updates are downloaded centrally and then distributed via SCCM (System Centre Configuration Manager), the verification of the machine stations compliance is carried out through SCOM (System Centre Operations Manager).


EMPLOYEES
DIVISION
CITY HALL
DEPT
ICT EQUIPMENT REQUEST
- PROTOCOL
HW
KNOWN:
QUANTITIES
UNKNOWN:
MACHINES
WHO USE THE WORKSTATION?
WHERE
(FLOOR?
ROOM?)
SW
KNOWN:
STACK SOFTWARE
ADMINISTRATORS
UNKOWN
POLICY APPLICATION
(COMPLIANCE)
FLEET
MANAGEMENT
(WE → DATA OWNER
MICROSOFT → SOFTWARE OWNER)
SCCM
(SOFTWARE CENTER CONFIGURATION MANAGEMENT)
?
ACTIVE DIRECTORY
Gestione Dominio
2) Management of Domain
3) Policies

Team 4 RP 1

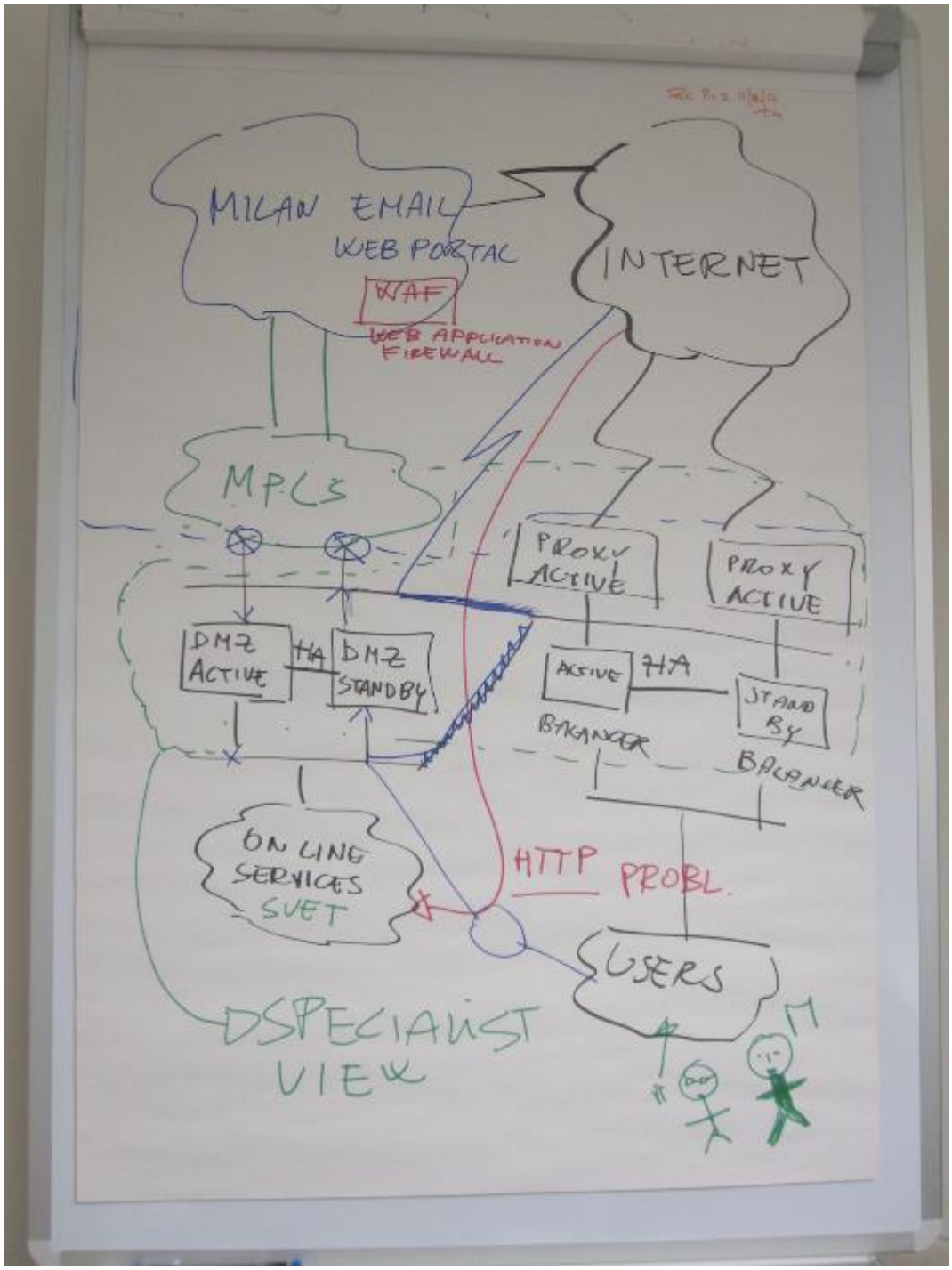
This picture represents the first rich picture of team one. This picture was re-drawn after the first round of presentations and discussion. A detailed description is provided in the enhanced version Team 4 RP 2. This rich picture describes parts of Roma Capitale's architecture. CRC architecture is very complex and in this picture we are describing a simplified model but with enough detail within the scope of CS-AWARE project. Regarding the user's data flow, there are two possible data flows for portal web services access:

- **Internal users (employees) data flow:** For accessing web portal services, the employee authenticates herself/himself passing from border/perimeter firewall, and then accessing to the web portal. After s/he authenticates and then s/he can access the services for which s/he has been authenticated for (depending on his/her role/profile) i.e. SUET.
- **External user (common citizens) data flow:** Common citizens access the portal that is in Milan and passes through Fastweb's MPLS network and Rome perimeter firewall. Then s/he can access the services located in Rome data centre.

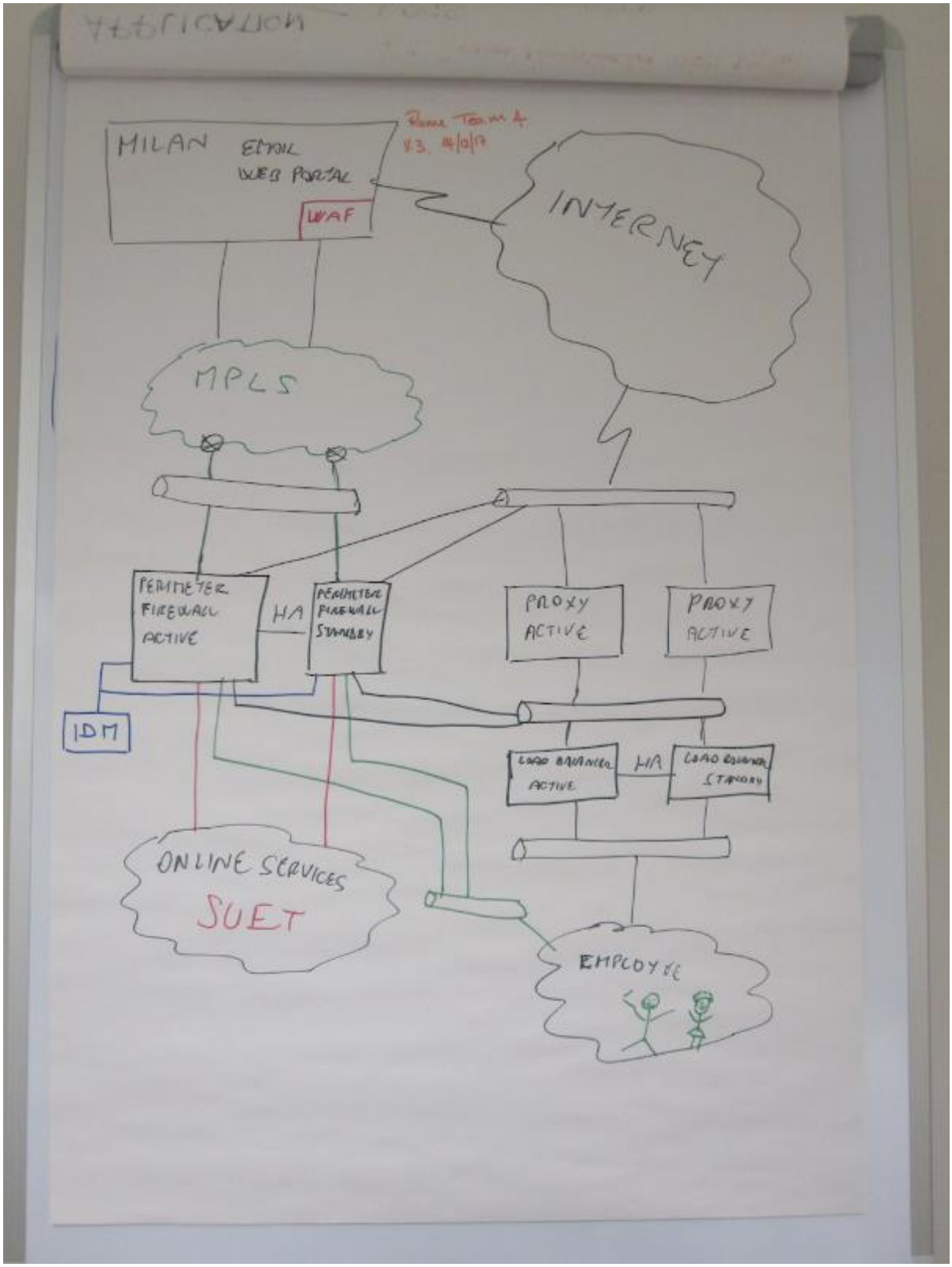
Team 4 RP 2

Team 4 RP 2 and a redrawn version Team 4 RP 2-V3 are two enhanced versions of Team 4 RP1, containing the input from workshop participants after the first round of presentations. After the second round of presentations the picture was even further detailed with the direct input from the Team 1 - Networks resulting in two iterations of Team 4 RP 3. A detailed description covering Team 4 RP 2 and Team 4 RP 3 can be found in the Team 4 RP 3 Section.

Version Team 4 RP 2



Version Team 4 RP 2-V3



Team 4 RP 3

This rich picture can be seen in two versions Team 4 RP2 and Team 4 RP 2-V3, and results from the analysis done in Team 4 RP 1 and Team 4 RP 2. It describes traffic flow when there is a request from the users both citizens and the internal users (employees) with an intended destination of either Internet or online services. Essentially, there are two paths, one for the citizen that starts from the Internet and goes through the MPLS-DMZ- Online-Services and another for internal users (employees) that goes through Proxy- ONLINE SERVICES. In the following we analyse each component. The CRC network, is composed principally by two principal branches:

- The device chain dedicated to the Internet connection for the internal CRC users (employees), is composed of a proxy (cache) system, two load balancers in high-availability mode that distribute the session to two separated proxy fire walls in active passive mode.
- The two DMZ perimeter firewalls are in high-availability mode and are the core of the CRC network. They guarantee the Rome-Milan datacentre, the IAM (Identity Management) farm and the service datacentres like SUET. All the data flow controlled by policy.
- MPLS the secure network that connects the Rome and Milan data centres.
- The two routers above the MPLS are border routers to the connection also for the Rome-Milan datacentre.
- Specialist view: manages the configurations of routing, VPN policy, Logs, Proxy rules.
- It is not HTTPS by default.

In the Milan datacentre, there are web-services like a web-portal and the services access.

- Online services (Rome): for example, SUET.
- WAF: Web application firewall is a firewall security at the application layer

The diagram describes to Data Centre infrastructures. All the components in the picture are detailed below:

Milan Data Center Infrastructure:

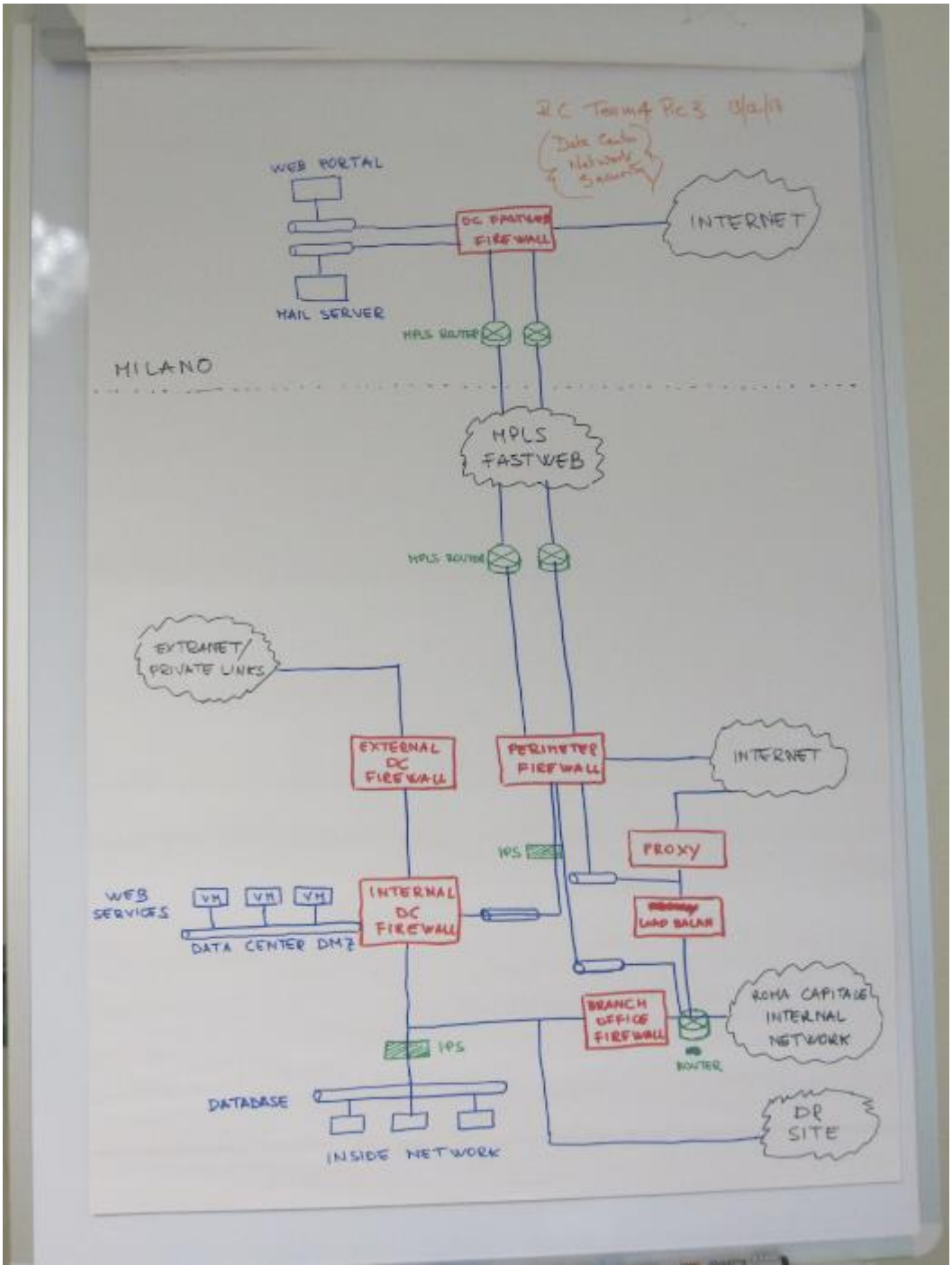
- DC Fastweb Firewall: is not a single appliance, but a firewall infrastructure that protects the web portal and the Mail infrastructure:
- The Internet connection is the main path to reach all the services hosted by the web portal.
- The site hosts the IAM access components that is part of the whole IAM architecture.
- There are two routers, part of the MPLS private link used to connect to Rome Data Centre.

Rome Data Centre Infrastructure

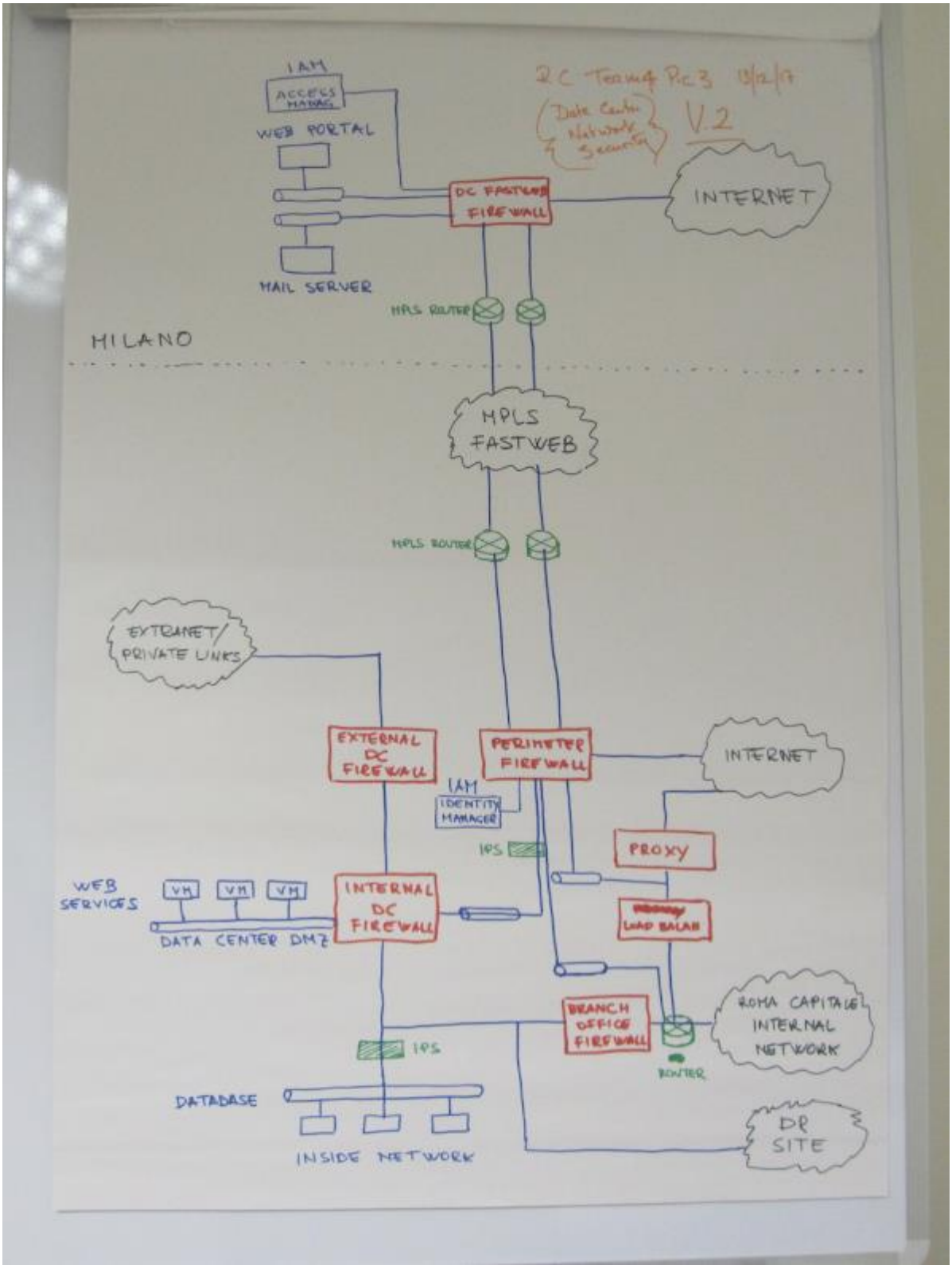
- There are two routers, part of the MPLS private link used to connect to Rome Data Centre.
- Extranet/Private links: are group of private links used to connect the datacentre to other private and public companies.
- External DC firewall: protects data centre from the traffic originated from the Extranet/Private links.
- Internal DC firewall: controls the access to the DMZ subnets
- Datacentre DMZ: group of subnets hosting various Hosts and Services that must be accessed by the outside (from Web Portal, directly from DC Internet access, from internal RC network and branch offices).
- Inside network: group of subnets posting various hosts and services that must be accessed only by specific servers and users (e.g.: databases, Microsoft infrastructure servers, ...)
- Branch office firewall: protects Rome Data Centre infrastructure against connections originated from RC internal network.

- RC Internal Network: connects all branch offices using private links.
- Load balancer: distributes traffic to the two nodes of the proxy
- Proxy: appliance in HA reconfiguration that allow and controls Web access of all RC workstations and servers.
- Perimeter firewall: connects Internet e secures Rome Data Centre infrastructure from connections originating in Milan datacentre
- The Internet connection: is an alternative path to reach the services hosted in DNZ. This path is used in specific situations.
- The site hosts the IAM identity component that is part of the whole IAM architecture.

Version Team 4 RP 3



Version Team 4 RP 3-V2

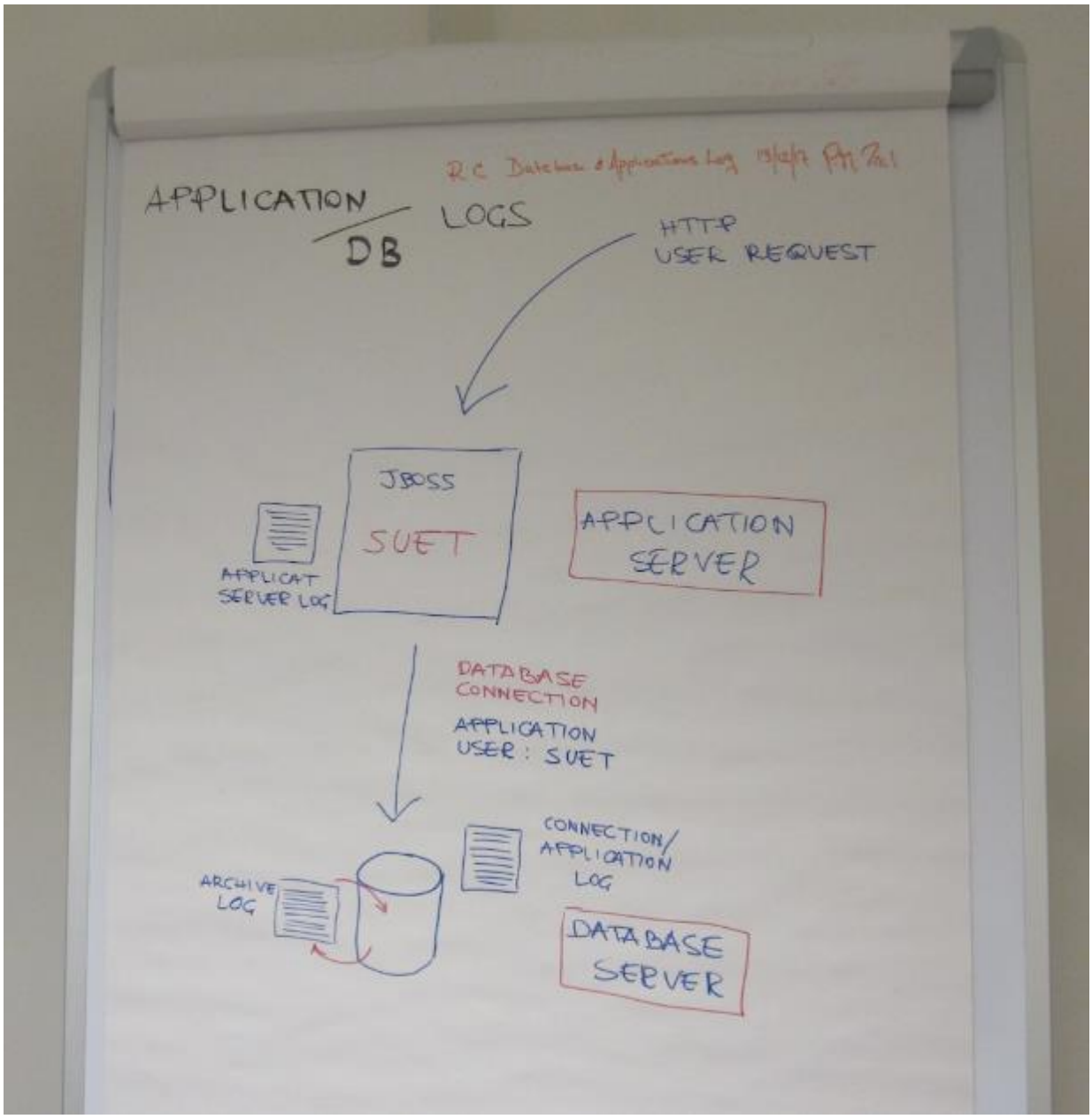


RP Database/Application log

In this rich picture, we describe the different levels of log used in SUET architecture. There are three kinds of log:

- Jboss/Debug Application Server logs
- DB application Logs
- Archive Logs

Jboss application logs trace every http request that an application server receives. Here we can find application debug logs and user access logs that are saved in application server file system. DB application logs are stored in a database table that traces every state change of all practices. This table contains different fields that identify practice and users that make changes practice's data. These types of logs contain sensibility information. All database connection from the application server is created by only one application that have grant to read/write in a database table. The last kind of log is DBMS SYS logs that are created directly by the DBMS. Archive logs are stored in the database file system and trace every operation in the database.



RP DMZ detail

There are two possible to interference and services access:

- Internal user (employee) data flow
- External user (common citizen) data flow

The diagram describes DMZ common traffic flow when there is a request originated from the Web Portal with a destination target located inside the DMZ. The entire process can be represented by seven different steps, each involving specific Network and security components

1. Request from portal: the end user, after being authenticated to the Web Portal, make an URL request for a specific service.
2. The connection comes from Milan to the Rome Data Centre Perimeter Firewall that redirects traffic to the internal DC Firewall
3. The URL request is processed by Reverse Proxy to be translated to the correct Web Server IP address.
4. If the service Front-End is made by multiple Web Servers, the request is redirected to load balancer.
5. Load Balancer distributes traffic to the nodes.
6. Web/Application Server ask for Database connection: the request is processed by internal DC Firewall Policies list.
7. The request is allowed to reach the Database host