SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D9.4
SYSTEM PROJECT WEBSITE

31 January 2019 **V3.0**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787128

Project title	SYnergy of integrated Sensors and Technologies for urban sEcured environment
Project acronym	SYSTEM
Project number	787128
Start date of the project	1st September, 2018
Duration	36 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D9.4
Deliverable title	SYSTEM PROJECT WEBSITE
Leading partner	FORMIT
Partners contributing	ALL
WP of reference	WP9
Title of the WP of reference	EXPLOITATION AND DISSEMINATION
Task of reference	T.9.3
Title of the task of reference	SYSTEM PROJECT WEBSITE
Deliverable type	Website, patents filling, etc.
Dissemination level	Public
Due date	M5 – January 2019. Foreseen in the DoA at M3 – November 2018. Extended by Mr. De Candido (DG HOME) with the email sent to Ms. Cavallini (FORMIT) on 10 December 2018.

Keywords	Website, Document Management System, Network Area Storage, Portal, Architecture
Abstract	D9.4 describes features and technical specifications of the project website. At this stage (submission date of this deliverable), the main focus will be on the architectural proposal of project web portal. During the project life, the SYSTEM public web portal will be regularly updated, taking into account that the SYSTEM project requires security and confidentiality of some information. For the same security and confidentiality reasons, the web platform available to SYSTEM partners in the back end of the web portal cannot be used for managing EU classified documents/deliverables at the level of EU_CON.

Editor	Edoardo Limone (FORMIT)
Contributors	Cristina d'Alessandro (FORMIT)
Reviewers	Fernando Solano (WUT), Martin Hedstrom (CSB)
Submission date of the draft to reviewers	21 January 2019

Submission date of the draft to the SAB (if required)	Not required. At the date of the submission of this deliverable, all the contents of the website were submitted and approved in form of other documents (e.g. press release) by the SAB.

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
FORMIT	V1.0	21/01/19	First draft (all.)	
WUT	V2.0	23/01/19	Executive Summary, 1. Main elements of this deliverable, 2 The architectural proposal of the document repository	
CSB	V2.1	29/01/19	None	None
FORMIT	V3.0	01/02/2019	Executive Summary, 1. Main elements of this deliverable, 2 The architectural proposal of the document repository	Re-arrangement of the order of some paragraphs.

Every information is updated to the date of issue of this document.

This document is composed by 12 pages

Table of Contents

EXECUTIVE SUMMARY 1

1 MAIN ELEMENTS OF THIS DELIVERABLE 2
- 1.1 INPUT FROM OTHER PROJECTS 2
- 1.2 INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES 2
- 1.3 APPLICABILITY 2
- 1.4 REFERENCE DOCUMENTS 2
- 1.5 PURPOSE OF THE DOCUMENT 2
- 1.6 STRUCTURE OF THE DOCUMENT 2

2 THE ARCHITECTURAL PROPOSAL OF THE DOCUMENT REPOSITORY 2
- 2.1 THE EXTERNAL PERIMETER 3
- 2.2 THE INTERNAL PERIMETER 3
- 2.3 SCHEMA OF THE ARCHITECTURE 3

3 THE SYSTEM PUBLIC WEB PORTAL 4
- 3.1 ACCESSIBILITY THE SYSTEM PUBLIC WEB PORTAL 6
- 3.2 SECURITY ASPECTS OF THE SYSTEM PUBLIC WEB PORTAL 7

4 BIBLIOGRAPHY 8

List of figures

Figure 1 Schema of the architecture 4
Figure 2 Mock-up of the portal on the left side and its first implementation on the right side 5
Figure 3 The SYSTEM project logo 5
Figure 4 Snapshot of the home page of the portal 6
Figure 5 Snapshot of the page with descriptions of the SYSTEM partners 6
Figure 6 Mock-up of the mobile version on the left side and its realization on the right side 7
Figure 7 The Aruba DB architecture 7

List of acronyms and abbreviations

CA	Consortium Agreement
DDoS	Distributed Denial of Service
EU_CON	EU Confidential
EU_RES	EU Restricted
GA	Grant Agreement
NAS	Network Area Storage
SAB	Security Advisory Board
SSL/TLS	Secure Sockets Layer/ Transport Layer Security
WP	Work Package

EXECUTIVE SUMMARY

The SYSTEM project requires visibility (as defined in WP9) as well as a proper security and confidentiality level for some information/other aspects. The balance between these two needs is obtained by submitting dissemination material and proposals for dissemination activities to the approval of the Security Advisory Board (SAB).

At the date of the submission of this deliverable, the SYSTEM public web portal (online at https://www.systemproject.eu) include information/contents approved by the SAB in other documents/deliverables (e.g. the first press release) and public information related to project partners. As the web portal should be also used to exchange information and documents between partners, a secured reserved area will be set up according to the architectural proposal described in this deliverable. For the security and confidentiality reasons connected to the SYSTEM project, the web platform available to the partners cannot be used for managing EU classified documents/deliverables at the level of EU_CON. It should be intended as an effective tool to share and store documents with at maximum the EU_RES classified level.

This deliverable must be considered as a "living document" as the SYSTEM public web portal will be enriched with information about the activities and outcomes of SYSTEM.
Accordingly, this deliverable will be regularly updated with the Dissemination Plan (D9.1).

1 MAIN ELEMENTS OF THIS DELIVERABLE

1.1 INPUT FROM OTHER PROJECTS

The deliverable D9.4 SYSTEM project website does not receive inputs from other projects.

1.2 INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES

SYSTEM Project Website (D9.4) receives no input from other WPs (at the date of the submission of this deliverable). The deliverable is related to the other outputs and deliverables of WP9 (e.g. visual identity) and with D9.1 (Dissemination Plan), D9.2 (Dissemination material) and D9.3 (Dissemination activities). It is linked to the Project Operational and Management Plan (D12.1) for timing of the activities of WP11 according to the work plan.

1.3 APPLICABILITY

The SYSTEM public web portal has to be intended as the "live" information point of SYSTEM for partners as well as the wide public during all the project life. Information and contents reported in public pages as well as the structure of the web portal itself will take into account limitations imposed by potential confidentiality and security issues.

1.4 REFERENCE DOCUMENTS

In order to set a framework in matter of a conflict between the SYSTEM project website and other documents such as the Description of Actions (DoA) in the Grant Agreement, the following hierarchy will be applied:

1. Grant Agreement (GA);
2. Consortium Agreement (CA);
3. The Project Operational and Management Plan (D12.1).

The hierarchy related to the documents above implies that the latter document needs to be consistent with the former. In case of issues, the hierarchy of the documents is mandatory.

1.5 PURPOSE OF THE DOCUMENT

SYSTYEM Project Website (D9.4) is set as a descriptive document of the architectural proposal related to the SYSTEM Project Web Portal (i.e. the repository of the documents/deliverables and the SYSTEM public web portal).

1.6 STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

1. **Main elements of this deliverable;**
2. The **Architectural Proposal** describes the web portal focusing on the Document Repository, external/internal perimeter, providing also a schema of the architecture;
3. The **SYSTEM Public Web Portal** illustrates the mock-up of the public pages.
4. **Bibliography**

2 THE ARCHITECTURAL PROPOSAL OF THE DOCUMENT REPOSITORY

The idea is to build an easy storage area for the management of the documents. This solution will be called **Document Repository** (hereafter the repository) and will be located inside a Network Area Storage (NAS) physically installed in FORMIT headquarters in Rome. The repository will be accessed only by authorized users and will represent a user-friendly space where to upload and download documents/deliverables and information. Each authorized user will be able to:

- **Browse folders**: users can navigate through folders such as Microsoft Windows Explorer or

Apple Mac Finder;
- **Create, edit and delete file and folders**
- **Upload/Download files**;
- **Zip/Unzip files** (useful to download an entire folder or upload a large number of files.

Security and confidentiality of some information and documents/deliverables is an essential requirement. As consequence, this repository will benefit from two different protection layers: the external perimeter and the internal perimeter.

2.1 THE EXTERNAL PERIMETER

The external perimeter is the entry point to the repository from the web. The web access will be protected by web certificate (SSL/TLS) that will encrypt the entire communication flows with the repository. The network devices will examine inbound/outbound data packets in terms of risks. In particular, to block any kind of DDoS (Distributed Denial of Service) attacks, various protection approaches can be combined among the ones listed below:

- SYN flood defense;
- UDP flood defense;
- ICMP flood defense;
- Port Scan detection;
- Block IP;
- Block Land;
- Block Tear Drop;
- Block Smurf;
- Block Ping of Death;
- Block trace route;
- Block ICMP fragment;
- Block SYN fragment;
- Block Unassigned Numbers;
- Block Fraggle Attack.

2.2 THE INTERNAL PERIMETER

Access to the repository will be protected with some redundant security measures installed on a UNIX architecture based on Linux OS. Other security rules will be enabled to guarantee “lock & ban” actions for bad users and fake connections. Each authorized user will be able to activate the “second-step-factor” log-in that adds a security layer to the login process. In addition to a common login method (i.e. based on username and password) a one-time-password (OTP) will be generated by Google Authenticator. Algorithms are specified in RFC 6238[1] and RFC 4226[2] created by the IETF (https://www.ietf.org/).

2.3 SCHEMA OF THE ARCHITECTURE

The figure below (Figure 1 Schema of the architecture) describes the architecture proposed for the repository, including the link between the repository itself and the SYSTEM Public Web Portal. A specific link will be generated every time a document will be uploaded into the repository. The link

[1] Internet Engineering Task Force (IETF) - Request for Comments: 6238 (https://tools.ietf.org/html/rfc6238)

[2] Internet Engineering Task Force (IETF) - Request for Comments: 4226 (https://www.ietf.org/rfc/rfc4226)

to such document (a flyer, for example) will be available also to visitors of the SYSTEM public Web Portal. Some features/restrictions can be added to this document:

- **The date and time of availability**. After which the document is available for downloading;
- **The date and time of expiration**. After which any download of the document is no more possible;
- **The password for downloading.** Users have to enter a password to open/download the document;
- **The maximum number of accesses to the resource**. After the maximum number of downloads, the link will be unavailable for further downloads.

Obviously, the link to public documents can be generated without any kind of these features/restrictions.

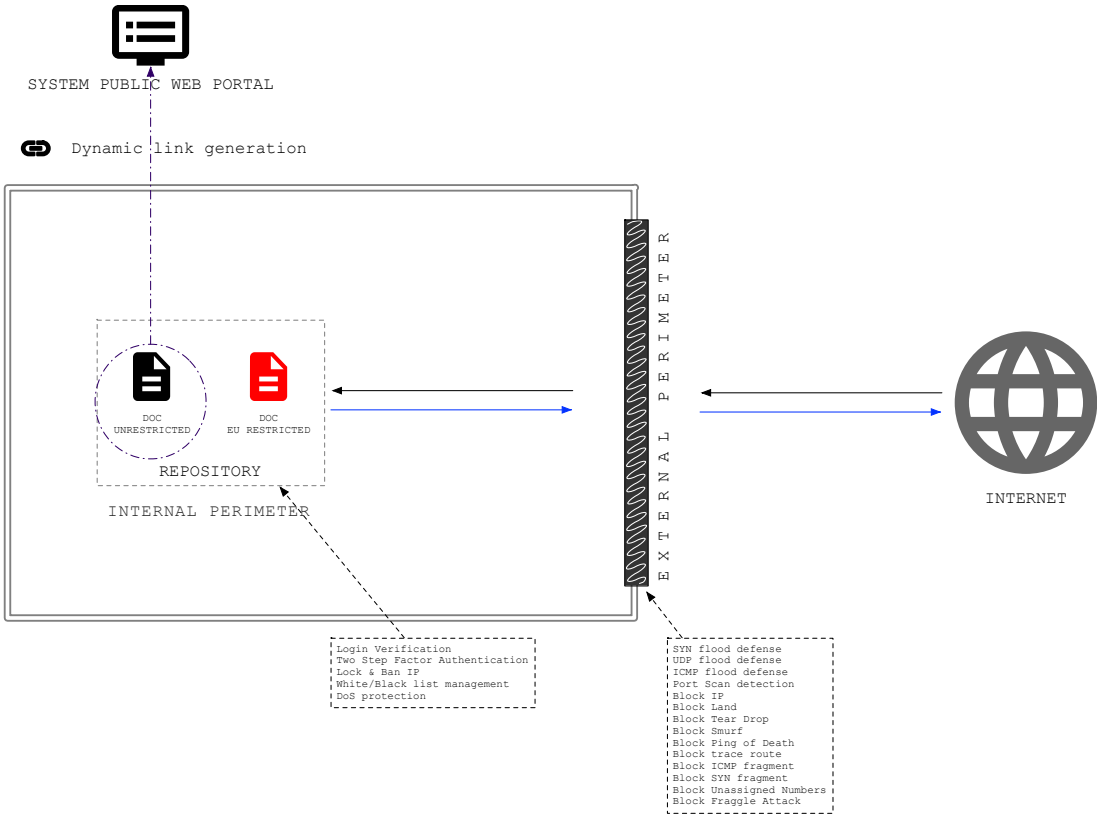

Figure 1 Schema of the architecture

In addition, different links can be generated in the repository for a single file: some with restrictions and others without restrictions. Links could be created/deleted by the administrator. This solution allows:

1) the non-redundancy of documents in repository and in SYSTEM public web portal;
2) a physical separation between repository and SYSTEM public web portal;
3) the monitoring of the activities on documents.

3 THE SYSTEM PUBLIC WEB PORTAL

Information for public related to SYSTEM will be disseminated by means of the SYSTEM public web portal (hereafter the portal) based on Joomla platform (https://www.joomla.org). The version

used for Joomla at the date of submission of this deliverable is the 3.9.2. All plug-ins and extensions are updated to the last available version[3].
The portal will contain two kinds of information of the project:

- contents directly created, edited and published into the Joomla platform.
- external contents such as documents linked from the repository to the portal.

With this approach, the portal, being empty of documents, will be maintained lightweight and much more secure.
The design of the portal started with the creation of a mock-up identifying the key information to be shared as well as the graphics elements to be inserted (Figure 2).

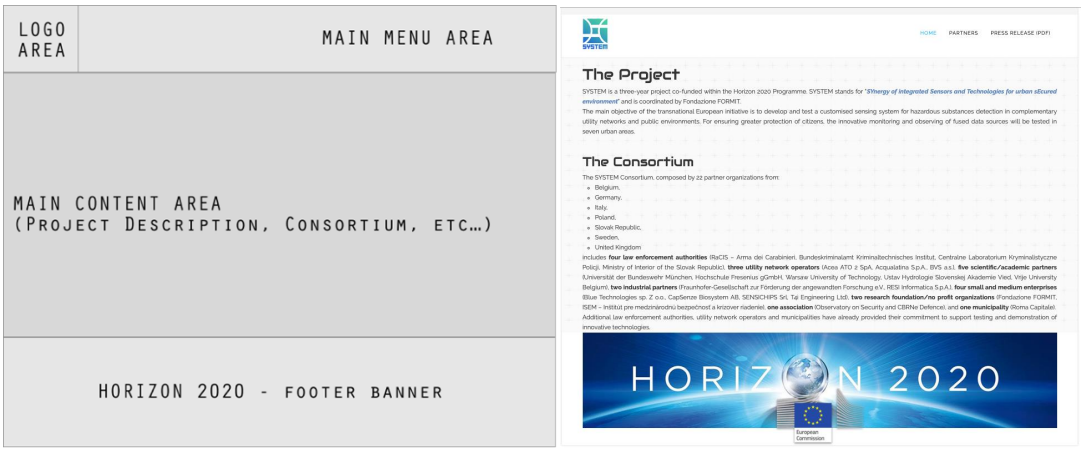

Figure 2 Mock-up of the portal on the left side and its first implementation on the right side

The portal will follow the project visibility rules described in the Dissemination Plan (D9.1). Key element of the project visibility is the SYSTEM logo (Figure 3).

Figure 3 The SYSTEM project logo

The portal is hosted on a service provider located in Italy (Aruba, http://www.aruba.it). The selected domain name is **systemproject.eu**.
The link to the SYSTEM public web portal (Figure 4) is https://www.systemproject.eu.

[3] For any update of components/plug-inns as well as for any structural change a backup of the entire portal will be saved on a FORMIT server.

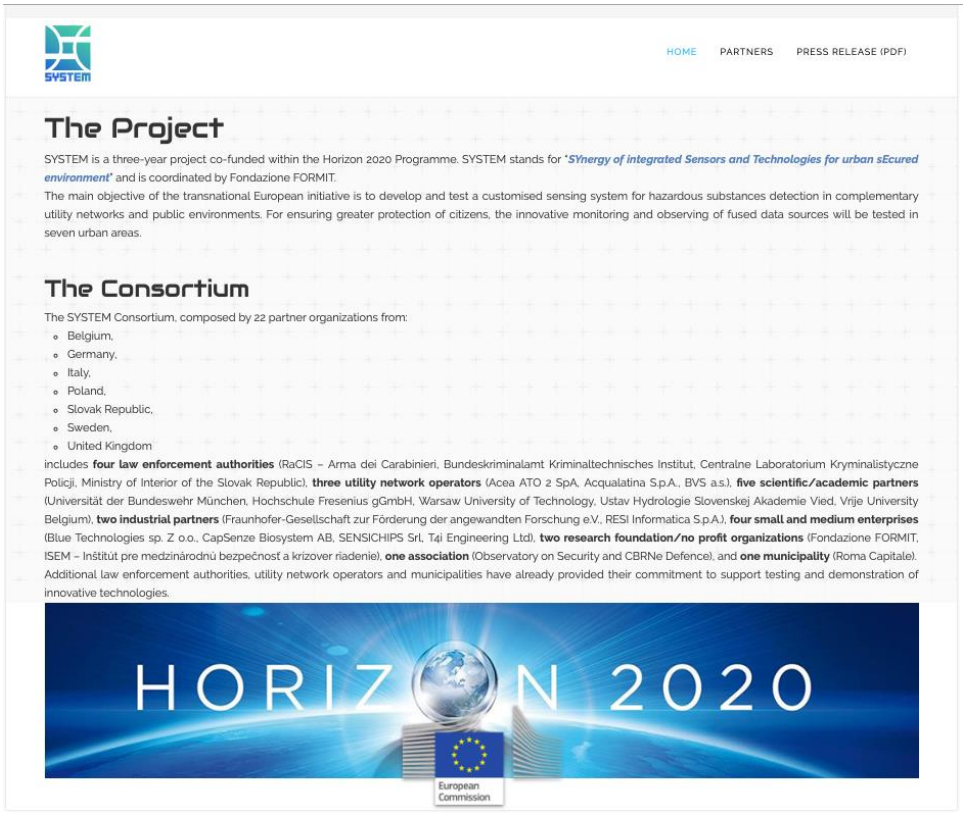

Figure 4 Snapshot of the home page of the portal

At the date of the submission of this deliverable, main information about the SYSTEM project is directly reported in the home page. A brief description about each partner is contained in a web page through a link in the main menu at the top of the page (Figure 5).

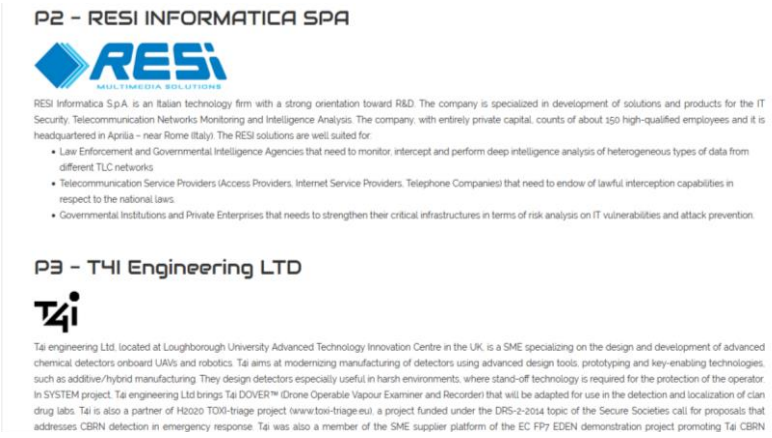

Figure 5 Snapshot of the page with descriptions of the SYSTEM partners

3.1 ACCESSIBILITY THE SYSTEM PUBLIC WEB PORTAL

The selected graphic template of the SYSTEM public web portal is fully compliant also in mobile version (i.e. responsive graphic). Figure 6 shows the mock-up design for mobile applications and a snapshot of its realization.

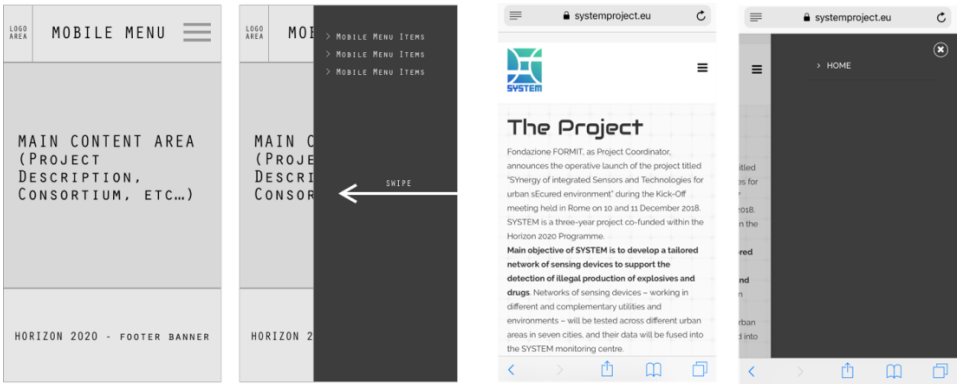

Figure 6 Mock-up of the mobile version on the left side and its realization on the right side

3.2 SECURITY ASPECTS OF THE SYSTEM PUBLIC WEB PORTAL

Selected hosting on Aruba will also add resilience to the SYSTEM public web portal through:
An additional security layer (

- Figure 7) with a firewall, an intrusion prevention system and a web application firewall;
- A restricted access to the MySQL database (DB). The access is possible only from the server used for the presentation layer and only from the Aruba's intranet.

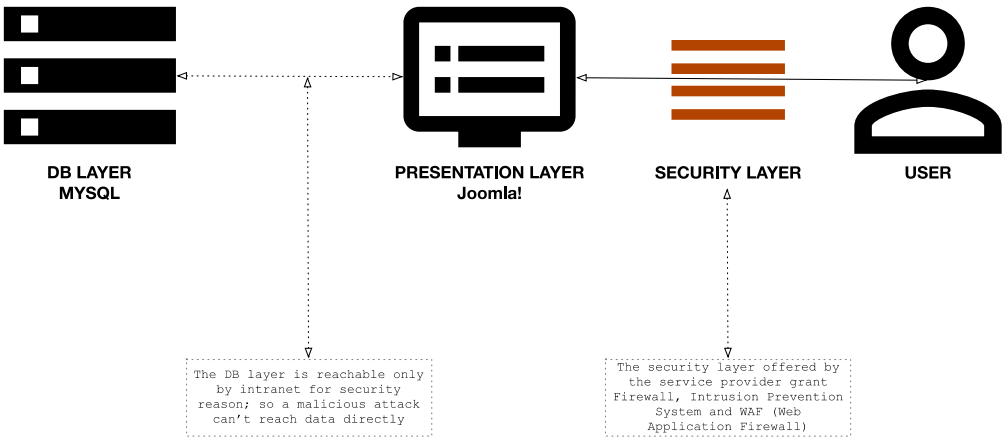

Figure 7 The Aruba DB architecture

4 BIBLIOGRAPHY

- Internet Engineering Task Force (IETF), "Request for Comments: 6238", https://tools.ietf.org/html/rfc6238
- Internet Engineering Task Force (IETF), "Request for Comments: 4226", https://www.ietf.org/rfc/rfc4226