



MEDINA

Deliverable D7.1

MEDINA brochure and public website

Editor(s):	Eva Salgado, Leire Orue-Echevarria
Responsible Partner:	TECNALIA
Status-Version:	Final – v1.0
Date:	28.02.2021
Distribution level (CO, PU):	PU

Project Number:	952633
Project Title:	MEDINA

Title of Deliverable:	MEDINA brochure and public website
Due Date of Delivery to the EC	28.02.2021

Workpackage responsible for the Deliverable:	WP7
Editor(s):	Eva Salgado, Leire Orue-Echevarria (TECNALIA)
Contributor(s):	Eva Salgado, Leire Orue-Echevarria (TECNALIA)
Reviewer(s):	Juncal Alonso (TECNALIA)
Approved by:	All Partners
Recommended/mandatory readers:	All WPs

Abstract:	The initial version of the brochure and project website will include at least project objectives and contact details. MEDINA website will be set-up and continuously enhanced by all partners to include public downloadable results and links to related news and initiatives.
Keyword List:	Website, brochure, communication
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

Document Description

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	20.12.2020	First draft version	Leire Orue-Echevarria, Eva Salgado (TECNALIA)
v0.2	15.02.2021	Sent for internal review	Leire Orue-Echevarria (TECNALIA)
V0.3	26.02.2021	Addressed comments from internal review	Leire Orue-Echevarria (TECNALIA)
V1.0	26.02.2021	Ready for submission	Leire Orue-Echevarria (TECNALIA)

Table of contents

Terms and abbreviations.....	6
Executive Summary.....	7
1 Introduction	8
1.1 About this deliverable	8
1.2 Document structure	8
2 Public website	9
2.1 Structure.....	9
2.2 Graphical appearance	9
2.2.1 Color palette.....	9
2.2.2 Menu	9
2.2.3 Body.....	10
2.2.4 Footer	10
2.3 Content.....	10
2.3.1 Homepage	10
2.3.2 About us	12
2.3.3 Use cases	15
2.3.4 Partners	17
2.3.5 Communication	19
2.3.6 Blog.....	20
3 Leaflet.....	21
3.1.1 Front of the leaflet	21
3.1.2 Inside of the leaflet	22
3.1.3 Back of the leaflet.....	23
3.1.4 Find us!	23
3.1.5 Project Key data	23
3.1.6 Contact information details	23
4 Conclusions	24
5 References.....	25

List of figures

FIGURE 1. LOCATION AND STRUCTURE OF THE MEDINA WEBSITE MENU	10
FIGURE 2. MEDINA FOOTER.....	10
FIGURE 3. CARROUSSEL IMAGE 1.....	11
FIGURE 4. CARROUSSEL IMAGE 2.....	11
FIGURE 5. MAIN ACTIVITIES AND RESULTS OF MEDINA	12
FIGURE 6. BLOG ENTRIES (PLACEHOLDER)	12
FIGURE 7. PAGE FOR THE MEDINA MISSION, VISION AND CORE VALUES.....	13

FIGURE 8. PAGE FOR THE MEDINA SOLUTION	13
FIGURE 9. PAGE FOR THE MEDINA APPROACH	14
FIGURE 10. PAGE FOR THE MEDINA OBJECTIVES	14
FIGURE 11. PAGE FOR THE MEDINA KEY RESULTS	15
FIGURE 12. AN EXAMPLE OF MORE DETAILS REGARDING A MEDINA KEY RESULT	15
FIGURE 13. PAGE FOR THE MEDINA BENEFITS	15
FIGURE 14. PAGE FOR THE USE CASE EUROPEAN CERTIFICATION OF MULTI-CLOUD BACKENDS FOR IOT SOLUTIONS	16
FIGURE 15. PAGE FOR THE USE CASE CONTINUOUS AUDIT OF SAAS SOLUTIONS FOR THE PUBLIC SECTOR.....	17
FIGURE 16. MAP SHOWING WHERE ALL PARTNERS COME FROM	18
FIGURE 17. DETAILS OF THE ORGANIZATIONS PARTICIPATING IN THE PROJECT AND THEY RESPONSIBLE PEOPLE OF SAID ORGANIZATIONS	19
FIGURE 18. PAGE FOR THE PUBLICATION OF MEDINA PUBLIC DELIVERABLES.....	20
FIGURE 19. MOCKUP FOR THE FRONT OF THE LEAFLET	22
FIGURE 20. MOCKUP FOR THE INSIDE OF THE LEAFLET.....	23

Terms and abbreviations

CSA or EU CSA	EU Cybersecurity Act
CSP	Cloud Service Provider
DoA	Description of Action
EC	European Commission
GA	Grant Agreement to the project
KPI	Key Performance Indicator
SW	Software

Executive Summary

This deliverable is a key aspect in the outreach strategy as it services to create the MEDINA brand.

The objective of this deliverable is twofold. Firstly, it presents the initial content as well as the look and feel of the MEDINA website. The look and feel is supported by screenshots of the website at M4. The website will be regularly updated with the addition of new content, be them blog pots, news or deliverables. The second goal of this deliverable is to outline the content of the brochure / leaflet. Similarly, to the website, there will be subsequent versions in line with the progress of the project.

1 Introduction

1.1 About this deliverable

The objective of this deliverable is twofold. On one hand, it presents the look and feel requirements, the structure and main content of the MEDINA website. On the other hand, it presents 1) the outline of the leaflet and 2) its main content.

1.2 Document structure

Section 2 presents the look and feel of the website, as well as the content that has been included. It also states which keywords need to be stressed in each of the pages. Section 3 outlines the main aspects of the MEDINA brochure in terms of messages and content. The main target audience of this section is actually the graphical designers that will work in the creation of the brochure. Section 4 presents the conclusions of the deliverable.

2 Public website

2.1 Structure

Websites are a powerful communication and dissemination tool that is often used as the first entry point to get to know what the product or service is about. While websites are communication channels in one direction, the goal is to update the content as much as possible with interesting content in order to engage stakeholders.

A clear structure is therefore paramount for this. At this stage, this is the structure proposed:

- Home
- About
 - Mission and Vision
 - Solution
 - Approach
 - Objectives
 - Key Results
 - Benefits
- Use cases
 - European Certification of Multi-cloud backends for IoT Solutions
 - Continuous Audit of SaaS Solutions for the Public Sector
- Results:
 - Public deliverables
- Publications & Communication
 - Press Release
 - Newsletter
 - Brochure
 - Articles
- Partners: brief description of the partners.
- Blog
- Contact us

2.2 Graphical appearance

2.2.1 Color palette

The MEDINA Color palette in RGB format is as follows:

- Green: 0 – 153 - 160
- Black: 0 – 0 - 0

The website will use as baseline the following theme: <https://www.refaktor.org/drupal/porto7/one-page> (One-page site).

This template allows the website to be responsive and is automatically adapted to the device used.

2.2.2 Menu

The menu of the website is located in the upper side of the screen and with the following structure.



Figure 1. Location and structure of the MEDINA Website menu

2.2.3 Body

The content of the body is described in the next section (section 2.3)

2.2.4 Footer

The footer shall include:

- The acknowledgement to EC funding, compliant with the EC rules
- A Twitter widget
- Details of the coordinator, so anyone can get in touch with her
- Logos of the social networks where MEDINA is present

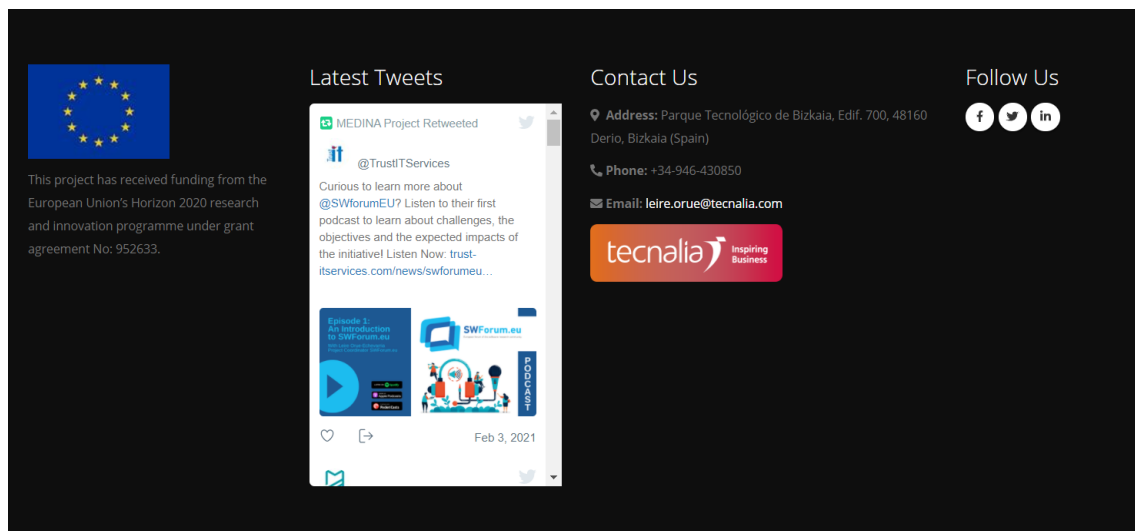


Figure 2. MEDINA Footer

2.3 Content

2.3.1 Homepage

When the user lands at the MEDINA homepage, the first thing he will see is the 'Home'.

2.3.1.1 Carrousel of images

The following images should appear in the moving carrousel of images that this template presents. The text is also detailed.



Figure 3. Carroussel image 1

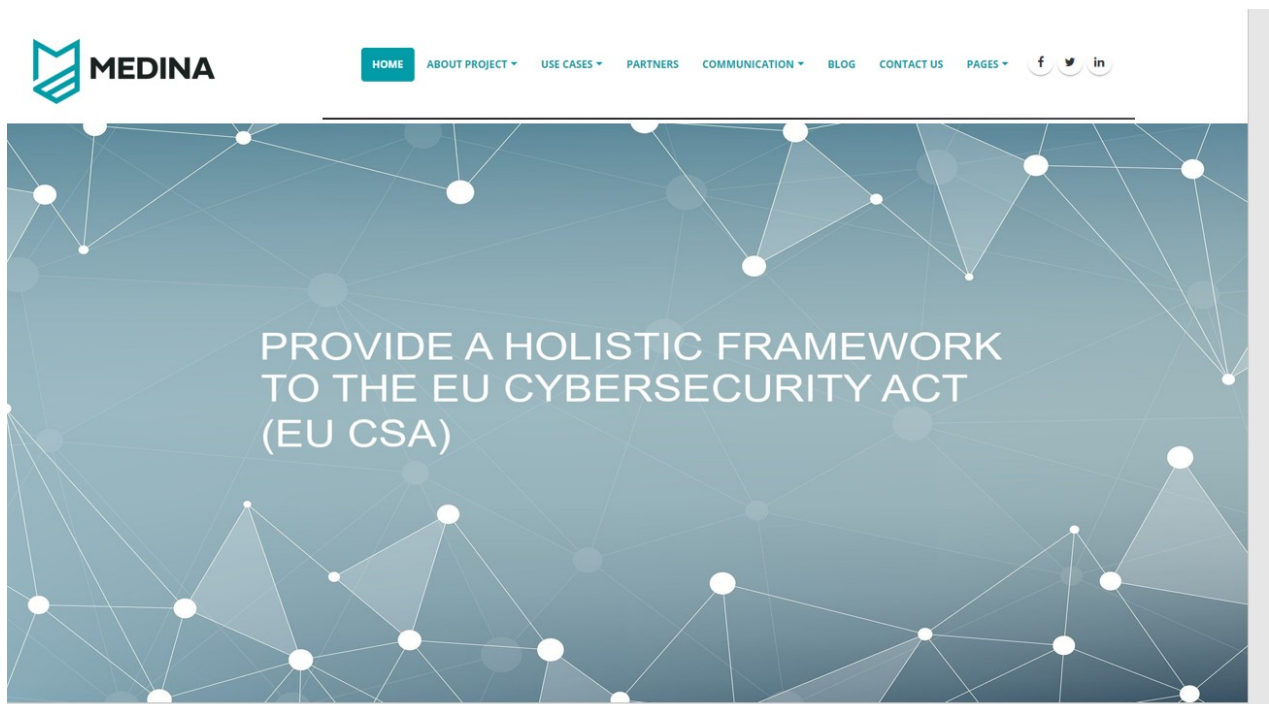
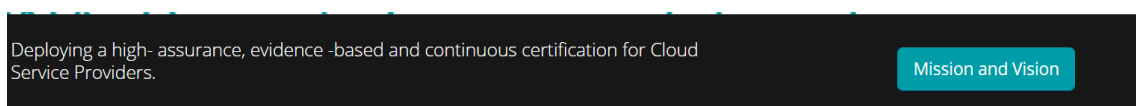


Figure 4. Carroussel image 2

In addition, the following image shall appear so the audience can get a faster understanding of the mission and vision of the project.



In order to show at a glance, which are the main results of MEDINA, the following images and texts shall be included:



Figure 5. Main activities and results of MEDINA

The next block is the blog posts. At M4 the project still does not have any entry, so a placeholder has been included.



Figure 6. Blog entries (placeholder)

2.3.2 About us

2.3.2.1 Mission and Vision

The goal of this site is to present a summary of the project with some of the project's core values.

The final version looks like this:

MEDINA project works on areas of cloud security performance and audit evidence management to create a Security Framework

Our core values: **Cloud security**

The MEDINA Project

The MEDINA project is an EU funded-research project working in the areas of cloud security performance and audit evidence management and its main goal is to create a **Security framework** for achieving a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme. of cyber-security and safety solutions which can be implemented by industrial and scientific users to increase their **resilience** to cyber threats, reduce safety **risks** and ensure the **compliance** of industrial standards.

MEDINA will tackle challenges in areas like:

- 🔍 Security validation.
- 🧪 Testing.
- 📄 Machine-readable certification language.
- 📊 Cloud security performance.
- 📁 Audit evidence management.

The main objective of the project is to provide:

- 🌐 A holistic **framework** that enhances cloud customers' control and trust in consumed cloud services, by supporting CSPs (IaaS, PaaS and SaaS providers) towards the **successful achievement of a continuous certification aligned to the EU Cybersecurity Act**(EU CSA).
- 🔧 The proposed framework will be comprised of **tools, techniques, and processes** supporting the **continuous auditing and certification of cloud services where security and accountability are measurable by design**.
- 🔄 As the **MEDINA** framework is leveraged into a cloud supply chain, it will support continuously assessing the efficiency and efficacy of security measures to ultimately achieve and maintain a certification.

Figure 7. Page for the MEDINA Mission, Vision and core values

The text behind “our core values” is a carousel with the following values: **Excellence – Cloud Security certification – continuous monitoring of compliance**

Key topics must also be stressed such as: **framework – tools, techniques and processes – MEDINA**

2.3.2.2 Solution

The goal of this page is to present the MEDINA Solution.

The term “**Modular framework**” must be stressed out.

At the core of the MEDINA project is a **Modular Framework** that allows CSPs to implement and manage continuous certification of their cloud supply chain aligned to the EU CSA requirements. Because of the myriad of different cloud service delivery model as well as the different provisions on the EU CSA certification scheme, the framework itself needs to be agnostic to the actual cloud service and offer abstractions through different components.

While MEDINA aims to provide a reference implementation of those components, it is important to note that the framework will also allow and guide a CSP to achieve continuous certification through their already established tool-chain (or a combination of both).

Additionally, the MEDINA framework aims to support seamless transition from existing, non-continuous-based certifications, by empirically validating it with respect to the steps required in a regular audit. In the following, the individual components, or rather their role in the framework, will be detailed.

MEDINA Framework

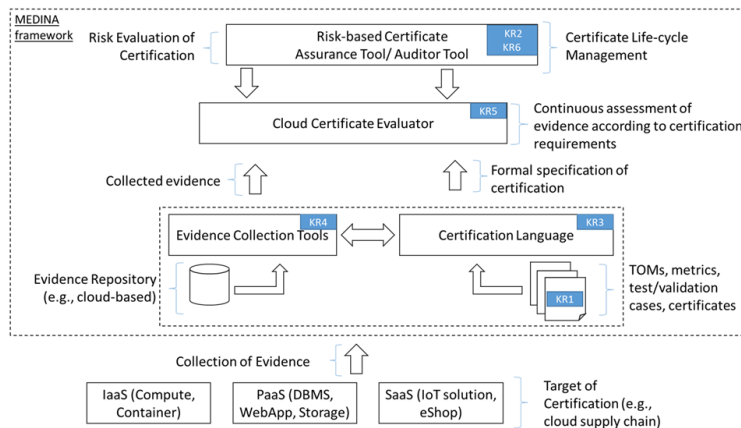







Figure 8. Page for the MEDINA Solution

2.3.2.3 Approach

The approach section briefly describes the main activities of MEDINA.

The word **approach** must be stressed, as well as the key elements of the explanation of the approach.

The MEDINA *approach* can be summarized as follows:

-  **Define a catalogue of metrics:** Associated to technical and organizational measures out of the MEDINA catalogue
-  **Select controls:** Taking into consideration the CSPs risk appetite and following a risk-based approach, the CSP shall select the security controls that are most convenient for it to certify. After that, assets of the cloud service and relevant IT threats shall be identified, and additional security controls proposed
-  **Specify the certification language:** Currently certification schemes are expressed using natural language. MEDINA proposes to transform this certification language into a machinereadable expression, by using NLP, including aspects such as scope of the certification, assurance level and conformity assessment method so it can be traced in an accountable manner with what is actually implemented (by using DLT / blockchain techniques).
-  **Collect and evaluate evidences.** Once the scope of the certification scheme is established, the evidences need to be collected at cloud service as well as code level, both at design and at operation time, that is, during the whole lifecycle of the cloud service.
-  **Continuously audit:** The collected evidences need to be continuously evaluated and the risks continuously monitored and updated, in order to have a secure operational service certifiable through the selected conformity assessment method. Furthermore, the lifecycle of the cloud security certificate shall be continuously managed and trailed through smart contracts using DLT

MEDINA framework approach overview

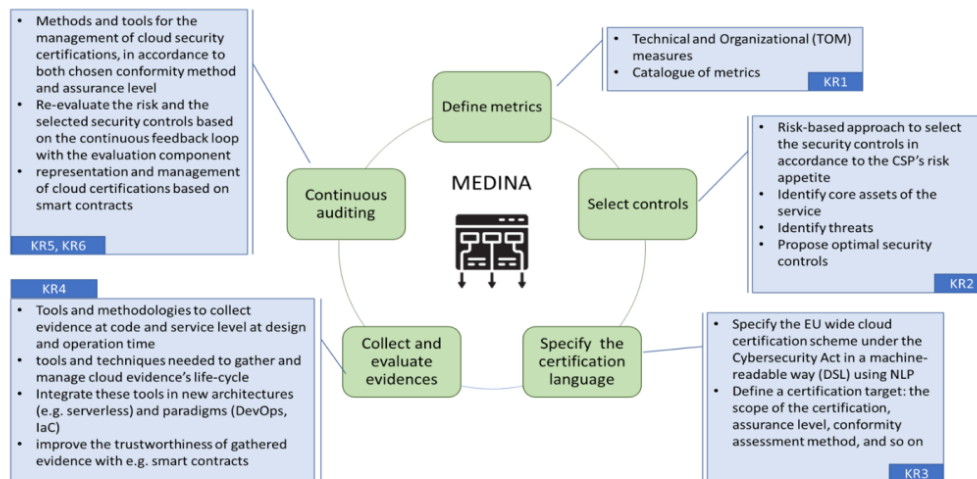


Figure 9. Page for the MEDINA Approach

2.3.2.4 Objectives

The page for the objectives looks like this:

The creation of this holistic framework, is supported by the following *objectives*:






-  **To provide Technical and Organizational Measures, TOMs**
Associated quantitative/qualitative security metrics³, machine-readable certification languages, and risk-based techniques to support security certification of cloud supply chains.
-  **To Provide Security Validation Techniques, Processes and Tools**
Allowing cloud providers to gather trustworthy evidences of implemented TOMs¹, in accordance to defined assurance levels in the EU Cybersecurity Act;
-  **To Implement and Integrate the Software Tools and Mechanisms to manage the life-cycle of cloud security certifications.**
Achieving the highest assurance level defined by the EU Cybersecurity Act (e.g., continuous monitoring-based certification).
-  **To Validate the outcomes in real use cases.**
Covering the three cloud service layers (IaaS, PaaS and SaaS).
-  **To Raise the awareness on the benefits of the contributed framework in the context of the EU Cybersecurity Act**
Supporting activities related to European training, awareness and relevant standardization activities.

Figure 10. Page for the MEDINA Objectives

2.3.2.5 Key Results

This page will show the main outcomes of the MEDINA project.



Figure 11. Page for the MEDINA Key Results

When clicking on each of the green boxes, more information about the key results can be seen.

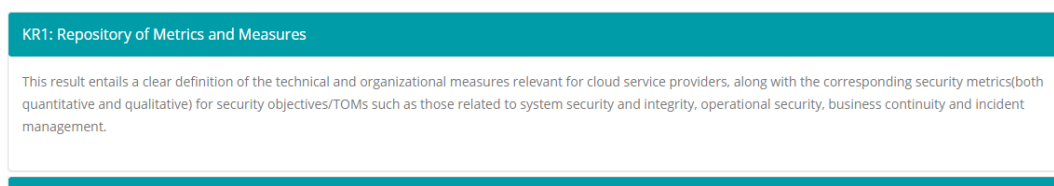


Figure 12. An example of more details regarding a MEDINA Key Result

2.3.2.6 Benefits

This page shall include the main benefits expected thanks to the application of MEDINA.

The MEDINA consortium is composed of academic and industrial partners, which play key roles in the EU cloud security certification ecosystem (e.g., research, cloud providers/customers, and auditors).

The MEDINA expected Benefits are:

- Guidance on the implementation of the controls, measures to be applied and evidences to be collected, reducing the time
- Support for an automatic compliance of the controls of existing certification schemes, reducing the effort, cost and risk of achieving and maintaining a certification
- Ease the effort in the collection and evaluation of evidences
- Ensure the Audit Trail of the evidences, and that no one has tampered with them

Figure 13. Page for the MEDINA Benefits

2.3.3 Use cases

MEDINA will be implemented in two real use cases, namely:

- European Certification of Multi-cloud backends for IoT Solutions
- Continuous Audit of SaaS Solutions for the Public Sector

Each use case shall have a distinct page. The text and images are taken directly from the DoA [1].

For the use case [European Certification of Multi-cloud backends for IoT Solutions](#) the page looks like this:

This validation scenario will solve the following issues:

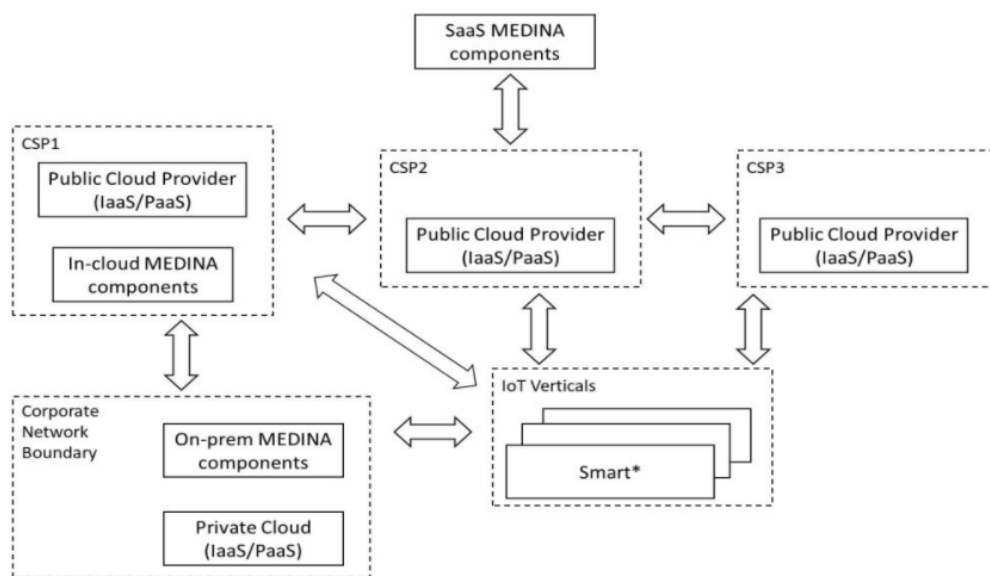


- Identify the technical and organizational measures to certify in a complex cloud supply chain for the three EU CSA's levels of assurance (basic, substantial, and high). Elicited TOMs will be derived from international standards and real-world IoT verticals like Smart Home, Smart Mobility and Industry 4.0.
- Perform the empirical validation of the continuous certification scheme (i.e. high assurance in the EU CSA), including the gathering of relevant evidence, in a real-world cloud ecosystem.
- Identify the gaps, which need to be solved in order to adapt existing audit practices to fulfil the requirements of the EU CSA (for assurance levels basic and high).
- Develop a set of reference architectures for the deployment of MEDINA's components e.g., SaaS based, Onpremises based, Hybrid-deployment based.
- Realize the real-world security requirements for onboarding MEDINA into a corporate environment.

Application where MEDINA will be used:

This use case will deploy a set of IaaS and PaaS services, commonly used for IoT backends, in at least three public CSPs. We refer to managed Kubernetes clusters, transactional SQL databases, raw virtual storage, virtual networks, virtual machines (e.g., as jump hosts), and serverless PaaS (e.g., functions).

The proposed system model looks like the one shown in the figure below.



Expected benefits/ improvements using MEDINA tools

- Provision of empirical feedback to international working groups/standardization activities on continuous certification (e.g., ENISA, DigitalEurope, ANSSI, US NIST, and BSI).
- Support the digital transformation of European SMEs by contributing with a blueprint to deploy the MEDINA framework (tools, techniques), in its different certification

Figure 14. Page for the use case [European Certification of Multi-cloud backends for IoT Solutions](#)

For the use case [Continuous Audit of SaaS Solutions for the Public Sector](#) the page looks like this:

Continuous Audit of SaaS Solutions for the Public Sector



This validation scenario will solve the following issue:

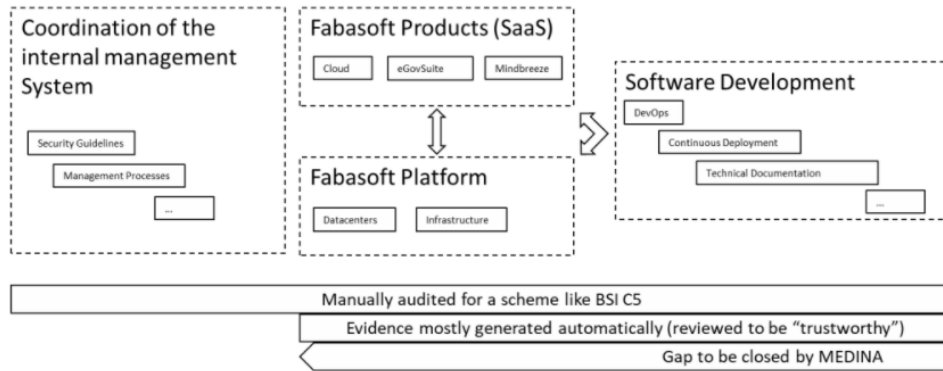
- Provide a high level of automation to the current audit process of a SaaS provider in alignment to the EU CSA, with particular focus on continuous audit-based certification.

At the state of practice, for a good number of requirements in current certification schemes (e.g., BSI C5, SOC2, ISO 20017, etc.), several CSPs already collect evidence automatically by using monitoring tools, log files, internal versioning and the likes. However, this generated evidence cannot, to date, be evaluated and audited automatically (continuously) due to the lack of standardized processes and tool chains. Furthermore, there is no clear definition of what "real evidence" is (i.e., evidence that auditors consider trustworthy for certification purposes), when it is automatically produced. Severing this problem is the fact that requirements of certification schemes change over time (more rapidly than slowly), and the effort to translate them into technical implementations for automatic collection of evidence is too expensive for most European CSPs.

Application where MEDINA will be used:

This SaaS Use Case will follow and validate the MEDINA's cloud security certificate life-cycle by making use of the risk-based auditor tool:

- Set the scope of the desired continuous audit process for the SaaS provider
- Continuously collect and evaluate evidence from a holistic perspective
- Monitor continuous compliance within the SaaS provider



Expected benefits/ improvements using MEDINA tools

- A standardized way to technically approach the requirements of a compliance scheme.
- A framework and working language to translate requirements into automatically observable controls.
- Ultimately reducing the operation workload for developers and technical staff related to certification processes.

Figure 15. Page for the use case Continuous Audit of SaaS Solutions for the Public Sector

2.3.4 Partners

This page has the goal of showing who is implementing the MEDINA solution.

Initially a map of Europe shall appear, showing the country where each partner comes from.

MEDINA is composed of eight partners from six different countries, representing Northern, Southern and Eastern Europe:

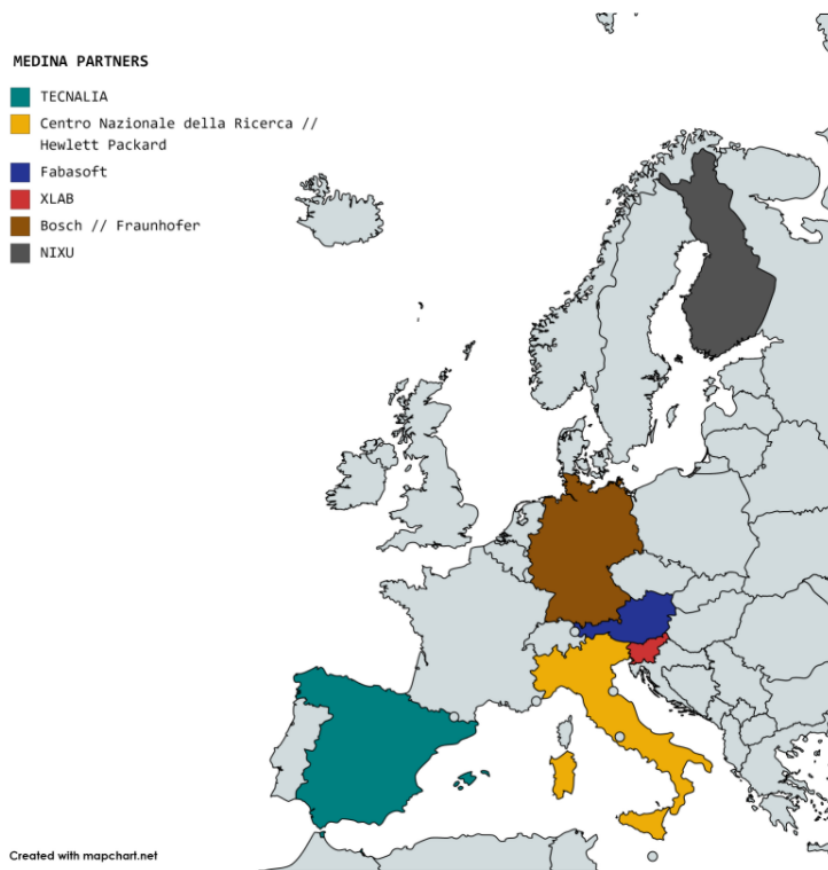


Figure 16. Map showing where all partners come from

The second part of this page is devoted to information about the partners and the leaders of each organization in the project:

Team Members






		
Leire Orue-Echevarria Project Manager	Jesús Luna García Cloud security and certification expert	Christian Banse Head of Department "Service and Application Security"
		
Björn Fanta Head of Research Alliances	Claudio Caimi Program Manager IT security	Anže Žitnik Project Manager at XLAB
		
Fabio Martinelli Senior Researcher	Niki Klaus Busines Leader certification services	

Figure 17. Details of the organizations participating in the project and they responsible people of said organizations

2.3.5 Communication

At this stage, the menu related to communication only contains a menu item, namely “Public Deliverables”, which will contain the public deliverables released in MEDINA. These will be published as soon as they are submitted to the EC, even before they are approved by the EC.

Public Deliverables

Del. No.	Deliverable name	File
D7.1	MEDINA brochure and public website	
D7.2	Dissemination and Communication Strategy	
D7.3	Market, Innovation and Applicability Analysis	
D2.1	Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v1	
D2.3	Specification of the Cloud Security Certification Language-v1	
D3.1	Tools and techniques for the management of trustworthy evidence-v1	
D3.4	Tools and techniques for collecting evidence of technical and organisational measures-v1	
D4.1	Tools and techniques for the management and evaluation of cloud security certifications-v1	
D4.4	Methodology and tools for risk-based assessment and security control reconfiguration-v1	
D5.1	MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v1	
D2.6	Risk-based techniques and tools for Cloud Security Certification-v1	
D5.3	MEDINA integrated solution-v1	
D7.4	Dissemination and Communication Report-v1	
D7.8	Standardization Roadmap-v1	
D2.4	Specification of the Cloud Security Certification Language-v2	
D2.7	Risk-based techniques and tools for Cloud Security Certification-v2	
D3.2	Tools and techniques for the management of trustworthy evidence-v2	
D3.5	Tools and techniques for collecting evidence of technical and organisational measures-v2	
D4.2	Tools and techniques for the management and evaluation of cloud security certifications-v2	
D4.5	Methodology and tools for risk-based assessment and security control reconfiguration-v2	
D5.2	MEDINA Requirements, Detailed architecture, DevOps infrastructure and CI/CD and verification strategy-v2	
D2.2	Continuously certifiable technical and organizational measures and catalogue of cloud security metrics-v2	
D5.4	MEDINA integrated solution-v2	
D2.5	Specification of the Cloud Security Certification Language-v3	
D2.8	Risk-based techniques and tools for Cloud Security Certification-v3	
D3.3	Tools and techniques for the management of trustworthy evidence-v3	
D3.6	Tools and techniques for collecting evidence of technical and organisational measures-v3	
D4.3	Tools and techniques for the management and evaluation of cloud security certifications-v3	
D4.6	Methodology and tools for risk-based assessment and security control reconfiguration-v3	
D5.5	MEDINA integrated solution-v3	
D7.10	Training materials	

Figure 18. Page for the publication of MEDINA public deliverables

This menu will be extended with the following items:

- Press Release: with the different press releases published in MEDINA, in the different languages.
- Newsletter: it will show the different releases of the newsletters.
- Brochure: it will hold the files for the different versions of the brochure.
- Articles: references to the published articles in journals and conferences.

2.3.6 Blog

This section will include the different blog entries posted in accordance with the communication strategy defined in D7.2.

3 Leaflet

3.1.1 Front of the leaflet

The aim of this first version of the leaflet is to create awareness of the project and present the key aspects of MEDINA. Subsequent versions of the leaflet will have other goals, such as the presentation of the pilots with a later version focused on the presentation of the results delivered.

The information that the first version of the leaflet will contain is as follows:

- Logo of the project, acronym and title of the project
- EC Disclaimer: This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 952633
- EU flag: the EU emblem must have appropriate prominence. Graphics guide to the European emblem to be accessed at: <http://publications.europa.eu/code/en/en-5000100.htm>
- Partner logos

The end result shall look similar to this:



Security framework to achieve a **continuous audit-based certification** in compliance with the EU-wide cloud security certification scheme



This project has received funding from the European Union's Horizon 2020 research and Innovation programme under grant agreement No 952633

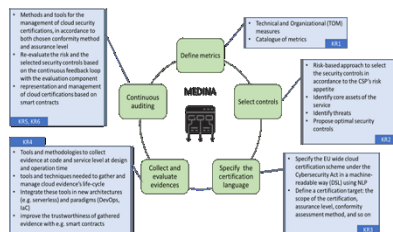
Figure 19. Mockup for the front of the leaflet

3.1.2 Inside of the leaflet

Project Objective

To create a **Security framework** for achieving a **continuous audit-based certification** in compliance with the EU-wide cloud security certification scheme.

Approach



Use cases

1. European Certification of **Multi-cloud backends for IoT Solutions**
2. Continuous Audit of **SaaS Solutions for the Public Sector**

Key Results

- KR1: Repository of Metrics** and Measures
KR2: Risk-Based Selection of Controls to reach the certification assurance levels
KR3: Certification Language
KR4: Continuous Evidence Management Tools
KR5: Cloud Certificate Evaluator
KR6: Risk-Based auditor tool

Benefits

1. **Guidance** on the implementation of the controls, measures to be applied and evidences to be collected, **reducing the time**
2. **Support** for an **automatic compliance** of the controls of existing certification schemes, **reducing the effort, cost and risk** of achieving and maintaining a certification
3. **Ease the effort** in the **collection and evaluation of evidences**
4. **Ensure the Audit Trail** of the evidences, and that no one has tampered with them

Figure 20. Mockup for the inside of the leaflet

3.1.3 Back of the leaflet

The back of the leaflet shall include the following items.

3.1.4 Find us!

<https://medina-project.eu/>

Twitter: @medinaprojecteu

3.1.5 Project Key data

Project Duration: November 2020 – October 2023

Budget: € 4 480 308,75

3.1.6 Contact information details

Project Coordinator:

Leire Orue-Echevarria (TECNALIA)

Leire.Orue-Echevarria@tecnalia.com

+34 664103005

4 Conclusions

This document has presented on one hand, the main aspects of the MEDINA website that will be used as entry point to get to know the project, and on the other, the main content that the first version of the brochure / leaflet should present.

Both the website and the leaflet will be continuously updated along the project timeframe. In the case of the website, as results are attained, these will be published on the website. This includes also blog entries, deliverables, presentations, videos and source code. Also, as mentioned beforehand, the leaflet will also have several iterations, with different foci, goal and target audience.

5 References

- [1] MEDINA Consortium, "Description of Action - Annex 1 - GA 952633.," 2020.