DOME

(Distributed Open Marketplace for Europe)

D4.2 Methodological framework for the continuous compliance of cloud services in DOME

Project full title

A Distributed Open Marketplace for Europe Cloud and Edge Services

Contract No.

101084071

Strategic Objective

DIGITAL-2021-CLOUD-AI-01-DS-MARKETPLACE-CLOUD

Project Document Number

DOME-D.4.2-V0.1

Project Document Date

30.06.2024

Deliverable Type and Security

DEM - PU

Main editor

TECNALIA

Contributors and reviewers

DEKRA, CSI, FIWARE Foundation,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101084071.

Log Table

Version	Date	Change	Author/partner
V0.1	02.11.2023	Table of content proposal and content in section 2.2 included	Juncal Alonso/TECNALIA
v0.2	29.05.2024	Initial content for the main sections	Juncal Alonso, Enrique Areizaga, Iñaki Etxaniz/TECNALIA Noelia Guerra, Juan Manuel Martinez /DEKRA
v0.3	05.06.2024	Content included in section 2	Juncal Alonso/ TECNALIA
v0.4	10.06.2024	Ready for internal review	Juncal Alonso, Enrique Areizaga, Iñaki Etxaniz/TECNALIA Noelia Guerra, Juan Manuel Martinez /DEKRA
v0.5	14.06.2024	Peer-review	Davide de Santis/CSI
v0.6	18.06.2024	Peer-review	Jesus Ruiz/FF
v0.7	26.06.2024	Addressed comments from internal reviewers	Juncal Alonso, Iñaki Etxaniz /TECNALIA
VFinal	1.07.2024	Final check and submission	Laura Pucci/ENG

Table of Contents

List of figures

Acronyms

Acronym	Definition
CAB	Conformity Assessment Body
CSP	Cloud Service Provider
EUCR	European Cloud Rule Book
M18	Month 18
VC	Verified Credential

1 Introduction

Cloud computing is identified as a central piece of Europe's digital future, giving European businesses and public organisations the data processing technology required to support their digital transformation. The European Commission thereby stepped up its efforts to support cloud uptake in Europe as part of its strategy, notably with the pledge to facilitate "the set-up of a cloud services marketplace for EU users from the private and public sector". DOME will materialise the envisioned online marketplace, providing the means for accessing trusted services, notably cloud and edge services, building blocks deployed under the Common Services Platform and more generally any software and data processing services developed under EU programmes such as the Digital Europe Programme, Horizon 2020 or Horizon Europe Relying on Gaia-X concepts and open standards, DOME will provide the finishing touch to the technical plant that the Digital Europe Program is creating for boosting the development and adoption of trusted Cloud and Edge services in Europe. It will provide the single point of trusted and federated CSPs to meet each other in a trustful manner. DOME will take the form of a federated collection of marketplaces connected to a shared digital catalogue of cloud and edge services. Each of the federated marketplaces will be independent or connected to the offering of a given cloud provider which, in turn, can be classified as cloud IaaS, PaaS or SaaS providers. The federated partners offering services have, in fact, the common goal of giving expertise to support the integration of data/services, to the management of the same in even specific domains such as may be smart cities or smart farming or, more generally, for the application of artificial intelligence in all domains like AI Services on demand. DOME will rely on the adoption of common open standards for the description of cloud and edge services and service offerings as well as their access through a shared catalogue.

1.1 Executive Summary

This document aims at presenting work related to the support for the Continuous Compliance of Cloud Services in DOME, performed in the context of T4.3 during the first 18 months. The deliverable has introduced the approach for Continuous Compliance in DOME which has been also aligned with current relevant initiatives, addressing similar compliance related challenges (i.e. Gaia-X, CISPE Cloud). The support to the Continuous Compliance in DOME is based on a mixed approach, including the methodological framework and the tools to support and automate this process. The current report describes both aspects of the solution available at M18.

In order to establish trust in the services provided by cloud suppliers within the DOME marketplace, these services must adhere to the EU Cloud Rulebook specifications [1], which is expected to include regulations, codes of conduct, standards and certification schemes. Compliance is required both prior to onboarding and while the services are available in the marketplace.

The primary goal of DOME is not to directly certify cloud services for inclusion in the marketplace. Instead, DOME relies on certifications issued by authorised Conformity Assessment Bodies (CABs) and third-party auditors. These certifications, along with other relevant aspects outlined in the EU Cloud Rulebook, undergo analysis during the onboarding process. During operation, DOME continuously verifies the ongoing validity of these certifications.

1.2 Intended audience

This document is meant to provide valuable information, guidance and references to:

- Owner of the DOME marketplace (a.k.a. DOME Operator) to gather information about the support to the all required software artefacts and documentation to support the validation of the certification through DOME services.
- DOME project partners, in particular cloud services providers and federated marketplaces , are willing to publish trustable services in the marketplace.
- Potential federated marketplaces and providers outside the consortium, wishing to gain knowledge on the open-source technical foundation of the DOME tool supported approach to EUCloud Rulebook compliance.
- Personnel of the company providing the compliance validation service. Currently this service is provided by DEKRA, partner of the DOME consortium.

1.3 Structure of the document

This document is divided into 5 chapters:

Chapter 1: Introduction - provides a summary of this document, and describes its content and structure.

Chapter 2: Continuous Compliance of Cloud services in DOME - describes the approach followed in DOME to assess the compliance of the services in the marketplace during their whole lifecycle. It also presents a set of relevant initiatives that might be considered and aligned with.

Chapter 3: Methodological framework for the continuous compliance of Cloud services in DOME - explains the tool supported methodology strategy adopted in DOME to address the compliance of the services. To this end , this chapter describes the process of service compliance in DOME and details the functional description and the technical specifications of the first implementation of the DOME component assessing such compliance.

Chapter 4: Conclusions - closes up the document and provides information about the next steps and following reports supporting the services compliance in DOME.

Chapter 5: references of the document.

1.4 Related documents and resources

Following is a list of valuable links to relevant documents and resources:

- D2.1 - DOME requirements V1_Final [4] , which provides the complete list of functional requirements, including the ones related to the compliance features.
- D3.1 - DOME reference architecture and specifications v1 [5] , providing an overall technical and functional description of the DOME components and the relationship between them

2 Continuous Compliance of Cloud Services in DOME

2.1 Initial considerations

EU Cloud Rulebook will comprise different types of schemes, regulations and standards. T4.3 will focus on certification schemes and standards which cover the most relevant schemes and frameworks to be included in the EU Cloud Rulebook (EUCR). By the time of writing this deliverable and developing the corresponding Compliance Component the EUCR was not available, therefore we adopted an incremental approach starting by supporting the certification compliance assessment to widely adopted schemes (ISO based in the first version) and incrementally supporting the rest of the schemes to be defined in the European Cloud Rule Book. The objective of T4.3 is to automate as much as possible the compliance assessment process so that no "human" intervention is needed. Nevertheless, and due to a number of limitations on the CABs and other stakeholders to support the automation of some parts of the process (i.e. lack of available APIs to check and assess the existence and correctness of the certificates in a form of automatically exposed Register of Adherence, lack of support to verifiable credentials approach from the certificates issuers, etc) DOME foresees to implement different levels of support to the automatic checking of the certificates. The initial approach is based on the manual assessment of the controls present in the certificates by experts (see the detail in section 3.2) , and the translation of "digital signed or unsigned document based certificates" into machine readable compliance evidences in the form of Verified Credentials of those certificates.

The main objectives of the compliance support in DOME are:

- Develop a **formal process to verify the compliance** against reference standards
- Develop a **methodological framework supported by tools** to verify the compliance against reference standards during the on-boarding process
- Develop tools to support the semi-**automatic assessment of the validity of the certificates**
- Develop tools to **continuously monitor that security requirements** are being fulfilled through the c**ontinuous assessment of the validity of the certificates**

To this end, DOME will guarantee that services in the platform are certified checking the validity of the related certificates through a process composed of 4 steps:

1. Initialisation: During this phase the Marketplace owners are able to choose the set of certifications to be assessed or considered. Initially, as introduced DOME will
2. Accreditation: This phase covers the activities to be performed by the CSP to provide the requested information about certifications. As explained lately in this report DOME proposes an extensible approach, supporting current and future needs with respect to the format of the certificates.
3. Assessment and endorsement: Once the certificates are provided by the CSPs DOME Trusted Service Provider for certifications (in the first stage of the project, this role is

played by DEKRA, partner of the DOME consortium) assesses the certificate and if successful creates the corresponding valid VC in DOME for the CSP.

4. Onboarding: With the VC issued the CSP can be on-boarded into DOME with a valid and trusted compliance profile.

It is worthy to note, that DOME won't certify services, but will rely on valid certificates from official certificates issuers.

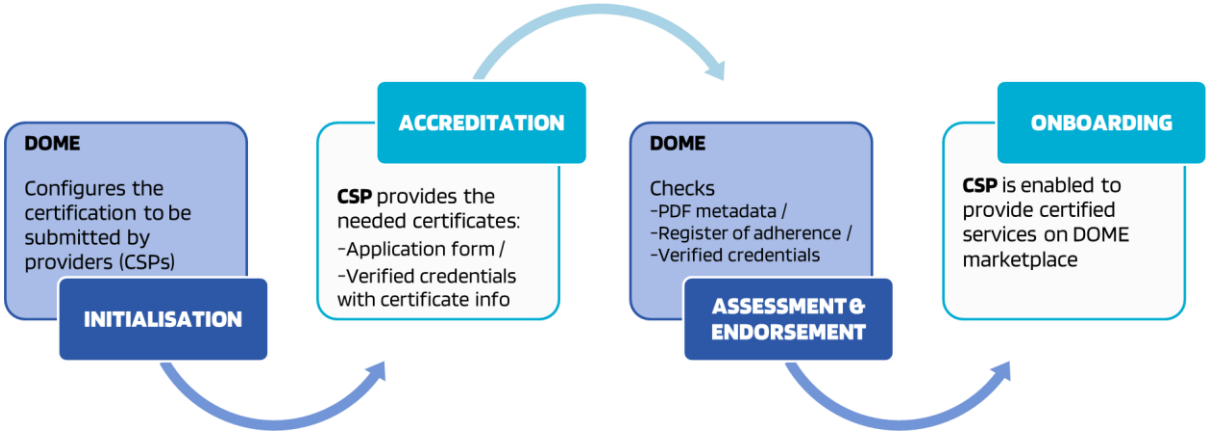


Figure 2.1.1 DOME certification compliance process

2.2 Link with relevant initiatives

This section reflects the analysis done on current practices related to the assessment of the compliance of cloud services. To this end 3 initiatives have been analysed and links have been established. This work has served to design a DOME compliance approach aligned and compatible with relevant current initiatives.

2.2.1 Gaia-X

Gaia-X compliance framework is based on the Gaia-X labels. The Gaia-X conformity Label is mandatory to endorse services in the framework. On the other hand, the optional Label levels define additional criteria and conformance-ensuring measures such as certificates, to achieve additional levels of assurance and trust, with a focus on European values and based on EU/EEA legislation. At this stage, the Gaia-X policy rules [2] list the normative high-level objectives for service offering providers in the following categories: contractual framework, data protection, cybersecurity, European control, and sustainability.

The Labelling Framework extends upon the Basic Conformity level and makes use of verifiable credentials to extend the Trust Framework. Thus, it is ensured that all information required to

make a qualified choice between different services is available in a consistent and standardised machine-readable form.

The Labels require consistency among the Gaia-X Ecosystem, scalability and extensibility, composability and modularity mapping, referencing of existing standards, self-assessment and CABs.

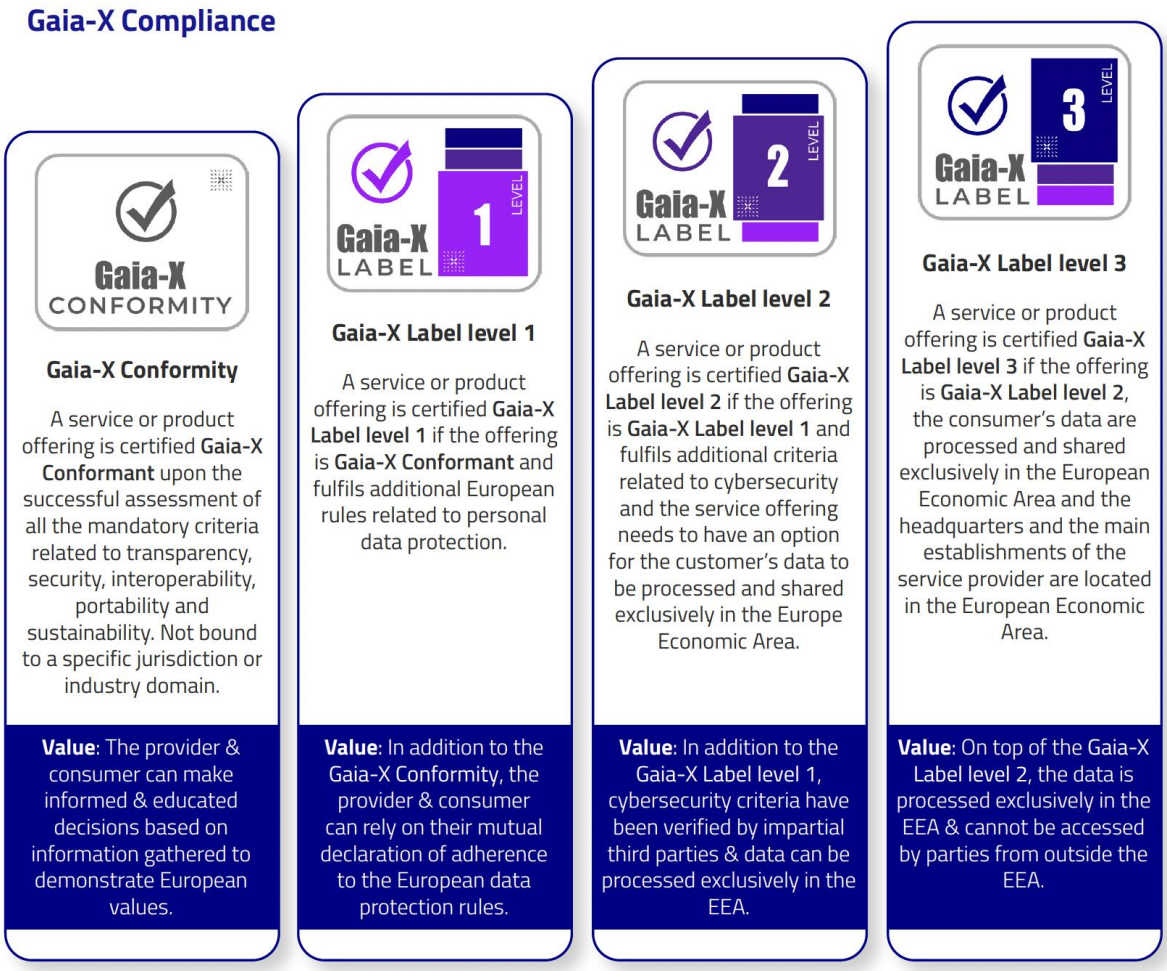


Figure 2.2.1.1. Gaia-X compliance levels. Source: [2]

	CONFORMITY	LEVEL 1	LEVEL 2	LEVEL 3
Declaration of Service or Product	✓	✓	✓	✓
Signed with verified method (e.g. eIDAS)	✓	✓	✓	✓
Automated validation by GXDCH	✓	✓	✓	✓
Automated verification by GXDCH*	✓	✓	+	+
Data Exchange Policies	✓	✓	✓	✓
Certified Label Logo		✓	✓	✓
Data protection by EU legislation		✓	✓	✓
Manual verification by CAB			✓	✓
Provider Headquarter within EU				✓

*not all criteria can be automated, "+" means automated verification if the evidence issuer (Standard & CAB)

Figure 2.2.1.2. Gaia-X criteria for the compliance levels. Source: [2]

Conformity with label criteria can be declared by self-assessment (declaration) or supported by external Conformity Assessment Bodies (CAB) (certification).

Gaia-X Service Offerings are defined by Provider-generated attestations which include claims of adherence to the Labelling Criteria. The proof of validation of a claim will be technically realised through Verifiable Credentials. The **Verifiable Credential can either be issued by a Provider or a CAB** directly or it can be created by a trusted Verifiable Credential issuer based on existing documentation (**like a signed PDF or paper document**). Level 2 and Level 3 conformity schemes contain criteria requiring 3rd party impartial certification by Conformity Assessment Bodies (CAB). Labels are issued by Gaia-X AISBL-accredited Gaia-X Conformity and Gaia-X Label issuers.

The Verifiable Credential includes the entity asserting the validity of the claim; the list of trusted Verifiable Credentials issuers is maintained in the Gaia-X Registry.

Figure 2.2.1.3. Gaia-X compliance validation approach. Source: Gaia-X

The Gaia-X Conformity and Gaia-X Label attestations are issued for a period of **one year.** Upon expiration, a new submission must be made. They don't consider the continuous monitoring of the certificates.

Gaia-X Labels do not normatively reference external documents which are not yet approved (for example the current proposal of the Data Act or the EUCS). Whenever such external documents are approved, Gaia-X may consider adapting its labels in accordance with them.

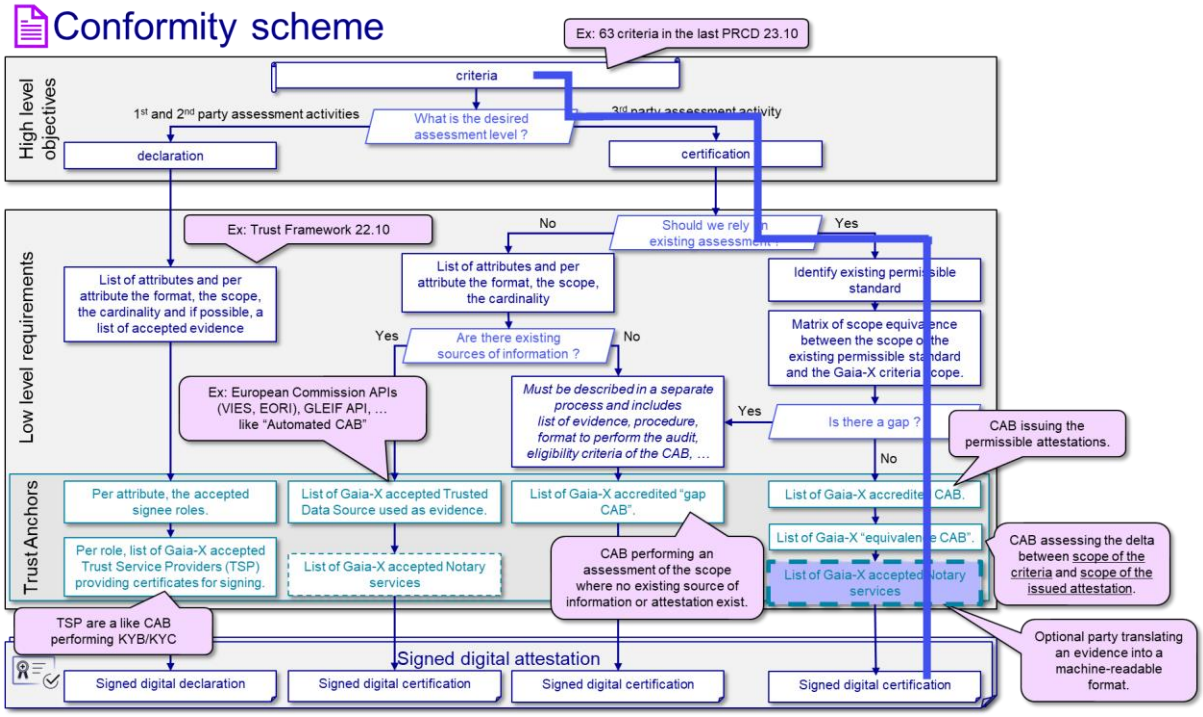


Figure 2.2.1.4. Gaia-X conformity validation process. Source: Gaia-X

After initial analysis and discussions with Gaia-X representatives we have established the following collaboration topics between DOME and Gaia-X in the compliance topic:

- DOME certification process (see details in section 3) fits within the NOTARY services of Gaia-X . In order to be compliant with both ecosystems it will need to be included within the list of Gaia-X Notary Services.
- Collaboration on a common and standard model for the characterization of the VCs corresponding to certifications. DOME proposes a preliminary model of the VCs at M18 that will be discussed with Gaia-X for complementarity and alignment.
- Cooperation on the establishment of a common recognizable compatibility between the two frameworks, DOME and Gaia-X, analysing the alignment between DOME compliance levels and Gaia-X labels.

All these aspects will be further worked out and followed up between the Gaia-X and the DOME teams towards future alignment and compatibility.

2.2.2 CISPE Cloud

The Cloud Infrastructure Services Providers in Europe (CISPE) is a non-profit association dedicated to fostering a greater understanding of, and promoting the use of, cloud infrastructure services across Europe. The association comprises 27 members, including small and medium-sized enterprises (SMEs) as well as large multinationals, headquartered in 14 EU Member States and serving customers throughout the European Union.

CISPE has developed the first dedicated Cloud Infrastructure Code of Conduct for Data Protection under the EU's General Data Protection Regulation (GDPR). This code adheres to the stringent requirements of the GDPR framework, aiding providers in achieving compliance and avoiding penalties while enabling customers and end users to select and trust cloud providers confidently. Additionally, CISPE co-chairs, alongside EuroCIO, the cloud infrastructure industry working group sponsored by the European Commission. This group is tasked with developing industry Codes of Conduct that facilitate data portability within the framework of the Free Flow of Non-Personal Data Regulation.

CISPE members were pioneers in declaring their services compliant with the SWIPO (Switching Cloud Providers and Porting Data) IaaS Code of Conduct for data portability. The ability to prevent lock-in and ensure seamless data portability is crucial to the GAIA-X vision.

As part of the first Data Protection Code of Conduct for Infrastructure-as-a-Service approved by EU Regulators (EDPB), CISPE introduced the option to store and process data exclusively within the European Economic Area (EEA) and guaranteed that customer data would not be monetized or used for any other purpose without consent.

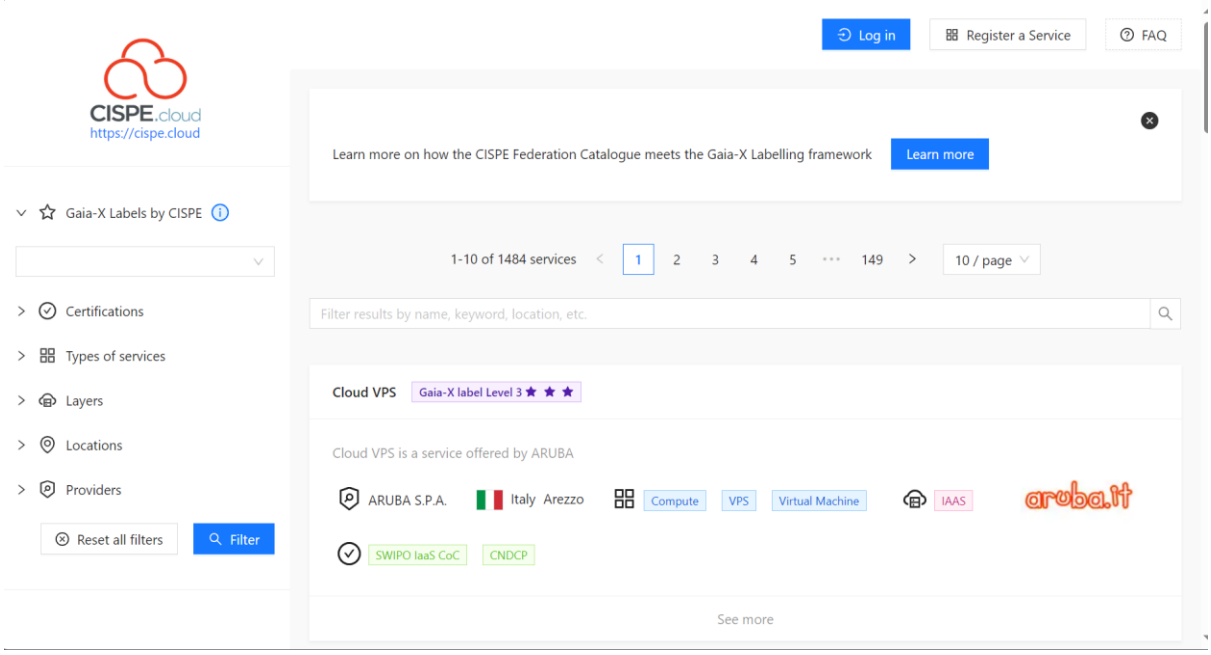


Figure 2.2.2.1. CISPE Cloud Labelling framework. Source: [3].

The CISPE Federation Catalogue is managed by Cloud Data Engine (CDE), an independent company specialising in technologies for managing Gaia-X catalogues. CDE ensures full compliance with all Gaia-X requirements and adheres to additional specific rules set by the CISPE governance.

The CISPE Federation Catalogue is the first operational catalogue adhering to Gaia-X project standards. It allows cloud service providers to demonstrate compliance with Gaia-X Labels, implementing the complete digital value chain of trust established by Gaia-X. The catalogue includes Gaia-X Compliance 22.10 offerings, complemented by a CISPE Label that extends the Gaia-X Label 22.11 criteria with the sustainability standards of Gaia-X Label 23.11 (PRCD 23.11). Where applicable, standards approved as "permissive" within Gaia-X PRCD 23.11 are utilised to demonstrate compliance, particularly regarding third-party audits on Data Protection and Cybersecurity, and declarations of adherence related to Data Portability and Sustainability criteria.

Only service offerings compliant with Gaia-X Policy Rules are listed in the CISPE Federation Catalogue. To be included, service providers must:

1. Be CISPE Members or Associate Members, who are invited to declare their service offerings.
2. Non-members can also declare their service offerings if they meet the following criteria:
    - Adherence to the Climate Neutral Data Centre Pact as a company.
    - Compliance with the Data Portability initiative supported by CISPE or the CISPE Data Protection Code of Conduct.

Declarations of service offerings in the CISPE Federation Catalogue are free of charge for CISPE members and associate members.

Labels are attributed based on compliance with Gaia-X Labelling Criteria, which cover a comprehensive set of standards developed by Gaia-X AISBL. Each service offering in the CISPE Federation Catalogue must comply with the mandatory Gaia-X Conformity scheme, based on Verifiable Credentials signed by the provider or trusted third parties. In this context, CISPE acts as an issuer of Verifiable Credentials for its members, based on information collected from members, associate members, or companies declaring services under one or several of the reference schemes supported by CISPE in terms of Data Protection, Data Portability, or Sustainability. Gaia-X Level 1 requires provider self-assessment, while Levels 2 and 3 currently mandate third-party audits for Data Protection and Cybersecurity schemes and mandatory declarations for Data Portability and Sustainability. Other criteria are included based on self-assessment in accordance with the relevant Gaia-X Labelling framework rules. By applying these rules, the CISPE Federation Catalogue can unequivocally establish and sign provider claims.

The approach adopted by CISPE concerning the Catalogue Federation, Cloud Rule Book, and Cloud Services Certification shares several commonalities with the selected deployment for the DOME Marketplace. Based on the analysis, the following actions will be undertaken to achieve alignment and interoperability:

1. The CISPE Federation Catalogue is Gaia-X compatible. Similarly, the DOME Federated Catalogue aims to be Gaia-X compliant. The ultimate goal is to enable Cloud Service Providers (CSPs) participating in CISPE to be accessible through the DOME Catalogue without undergoing an additional onboarding process.

2. CSPs in CISPE are required to adhere to the Data Protection Code of Conduct and the Climate Neutral Data Centre Pact, while in DOME, adherence to the EU Cloud

Rule Book is mandated. It is anticipated that once the EU Cloud Rule Book is approved, it will also be accepted by CISPE.

3. To be listed in the CISPE Federation Catalogue, service offerings must comply with Gaia-X Policy Rules. As DOME and Gaia-X are working on analysing the alignment between DOME compliance levels and Gaia-X labels, CISPE will consequently achieve compatibility as well.

3 Methodological framework for the continuous compliance of cloud services in DOME

This section presents the methodological approach for the continuous compliance of cloud services in DOME. The methodological approach and the related processes are supported by several tools, with the objective of automatizing them.

In the following figure 3.1, the general approach for the certification process of a single product or service in DOME is shown. This process description assumes that the organisation is already onboarded in DOME.

The process describes a single certification for the product/service and proposes a "certification" agnostic model for certification validity assessment. To this end, and while the main focus in the short term is to support the adherence to the EU Cloud Rulebook and the regulations, schemes and certifications included there, the envisioned approach supports the incorporation of future certifications such as the ones related to AI that are currently in the pipeline of several certification agencies (i.e. ENISA).

As depicted in the figure 3.1 the certifications compliance can be demonstrated in DOME through 3 different cases, in which the evidence (the certificate or a digital equivalent of it) can be provided in different ways: Unsigned PDFs (case 1) , Signed PDFs (case 2) or VC of the certificate provided by certification agencies (case 3). Adopting this approach, DOME wants to support the different current and future needs from the providers and the certification agencies. The DOME compliance component assesses the validity of the evidence providing tools to support the validation activity (performed by qualified entities "Trusted Service Provider for Certifications - TSP"[1]) and delivering the valid electronic proof (VC of the certificate) to be able to certify the compliance in the DOME ecosystem.

[1] For the first version the DOME TSP is DEKRA, partner of the DOME project consortium.

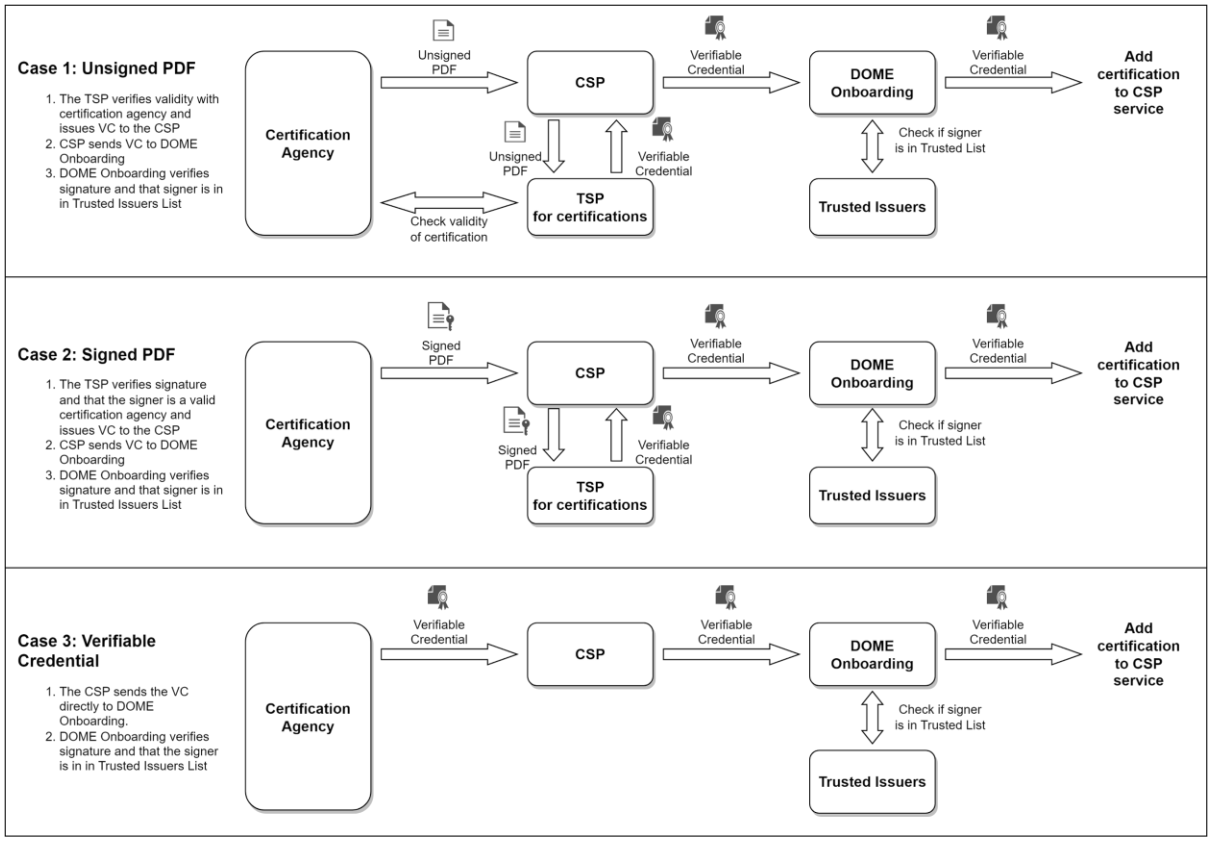


Figure 3.1 DOME general certification process and cases.

3.1 Continuous compliance processes in DOME

DOME marketplace will foster the adherence to the upcoming EU Cloud Rule Book [1]. As anticipated in the introductory section of the current document, EUCR is not publicly available by the time of writing this deliverable. The EU Cloud Rulebook it is envisioned as a “light” regulation with no strict obligation (based on voluntary adoption) and issued as a “Recommendation” but the Member States will have the power to enforce it in their jurisdictions, if they wish, or even make compulsory a subset or a superset of it . For more details please refer to the Cloud Rule Book [1].

Consistent with this approach, the DOME certification compliance functionality will allow the service providers to check which certification they own and to allow the customers to search/filter the catalogue upon the kind of qualification they aim to achieve. In the EU Cloud

Rulebook it is expected to have different compliance levels, i.e. Level 1, Level 2, Level 3. Similarly, DOME will also support the labelling strategy initially into 3 categories based on the number of verified certifications (from the supported ones). The services will be tagged (by different colours) accordingly into these categories: Red - Level 1 (No verified certifications), Yellow Level 2 - (Some supported certifications verified), and Green - Level 3 (All the certifications have been verified by a Certification Body[2] accepted in DOME).

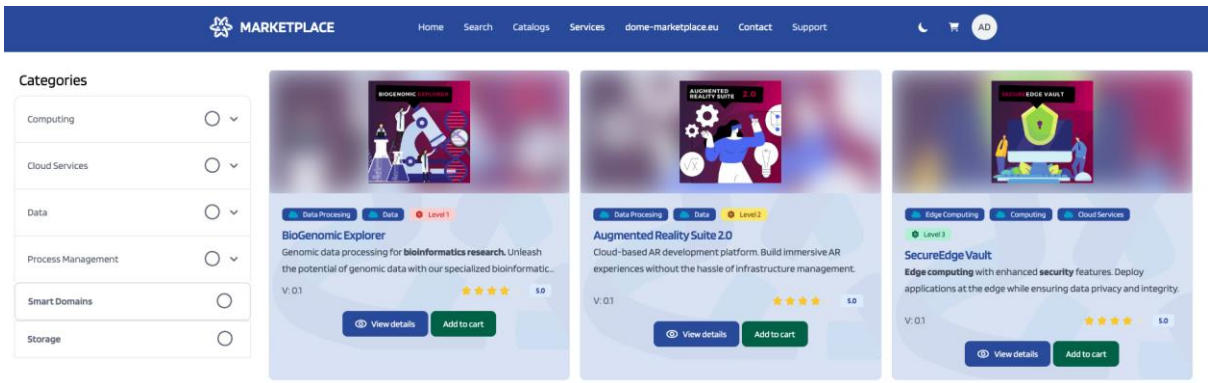


Figure 3.1.1 DOME compliance levels in the portal

This information will be also reflected at certification level, in the Compliance profile:

- DOME VERIFIED (verification passed)
- SELF-DECLARED (self-declaration of certification compliance, there is no assurance from DOME about the validity)
- EXPIRED (expired certificate)
- NOT ACHIEVED YET (no evidences provided)

[2] Authorised Certification Bodies in DOME: DEKRA

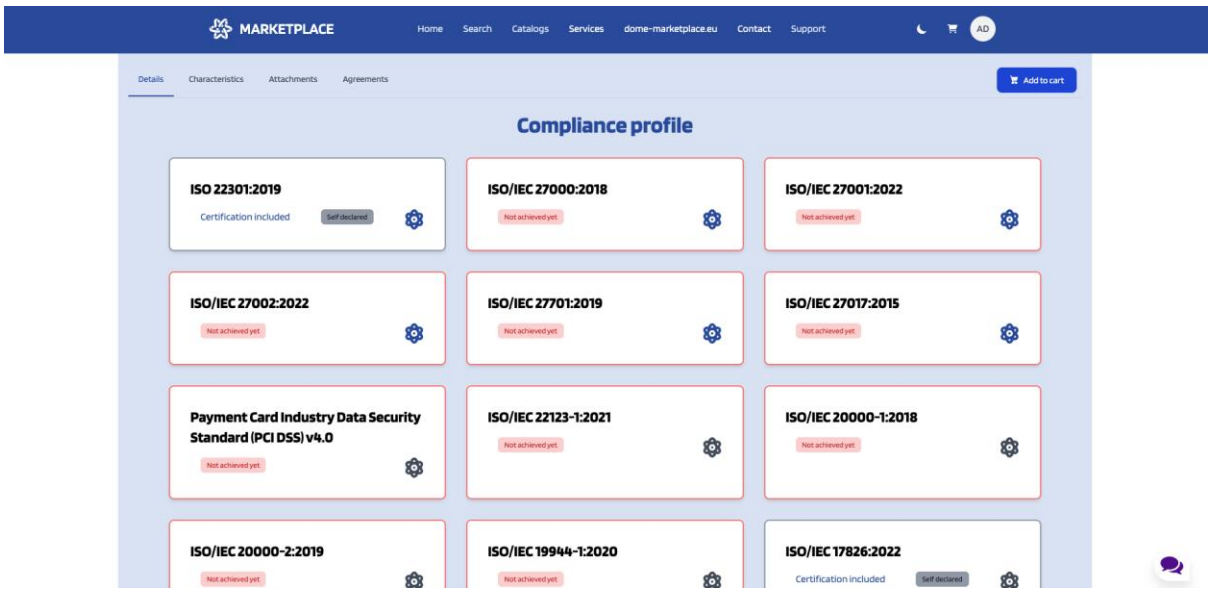


Figure 3.1.2 DOME compliance profile

For the first version of the platform the certifications supported[3] are the green ones in the following table:

[3] The current list is extracted from the draft version of EUCR to which the DOME team has had access, and will be increased following an incremental approach to support and extensive list of standards and schemas as they are being incorporated into the EUCR.

Table 3.1.1. DOME compliance supported schemes in the M18 version.

STANDARDS	Mandatory
General	
ISO/IEC 22123-1:2021	No
ISO/IEC 20000-1:2018	No
ISO/IEC 20000-2:2019	No
ISO/IEC 19944-1:2020	No
ISO/IEC 17826:2022	No
ISO/IEC 17788:2014	No
Interoperability and portability standards	
ISO/IEC 19941:2017	No
Information security standards	
ISO 22301:2019	No
ISO/IEC 27000:2018	No
ISO/IEC 27001:2022	No
ISO/IEC 27002:2022	No
ISO/IEC 27701:2019	No
ISO/IEC 27017:2015	No
Payment Card Industry Data Security Standard (PCI DSS) v4.0	No
Data protection and privacy standards	
ISO/IEC 29100:2011	No
ISO/IEC 29101:2018	No
ISO/IEC 19086-4:2019	No
ISO/IEC 27018:2019	No
Service level agreement standards	
ISO/IEC 19086-1:201	No
ISO/IEC 19086-2:2018	No
ISO/IEC 19086-3:2017	No

As presented previously the objective is to automate as much as possible the compliance assessment process, so that ideally no human intervention is needed, or otherwise the human intervention is minimised. To achieve this objective the DOME compliance process has been broken down into the following steps:

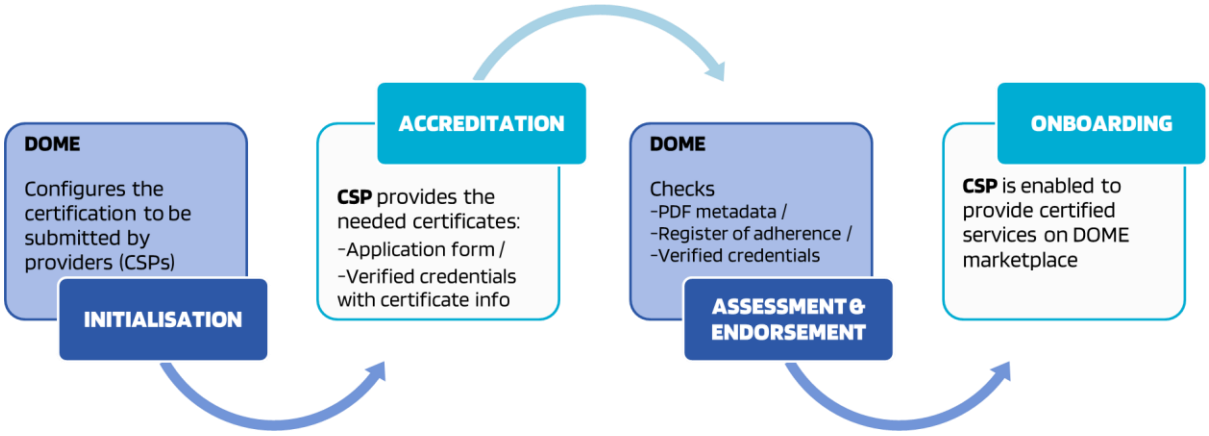
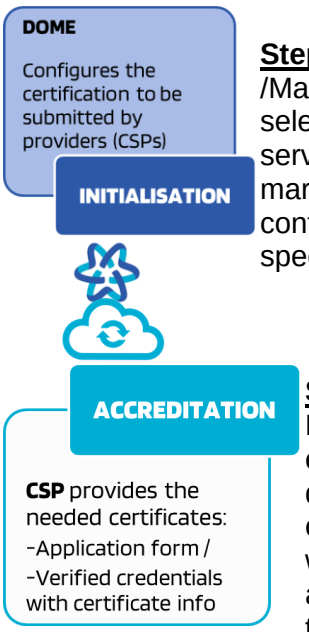


Figure 3.1.3 DOME compliance process steps



Step 1 - Certification initialisation: The DOME administrator /Marketplace administrator sets up the certification level for the services, selecting which certifications/frameworks need to be provided when a service is endorsed into the DOME/federated marketplace. Each marketplace federated in DOME can have specific additional configurations for compliance: EUCR , Others: AI related ones, financial specific, health specific, environmental specific, etc.

Step2 - Certification accreditation: A CSP that wants to be part of DOME provides the certificates, uploading the corresponding evidence (signed or not signed pdf files or VC of the certificate . As depicted in Figure 3.1.4, depending on the type of the provided evidence different methods need to be applied to validate it. DOME will accept the different certification types issued by the different agencies and authenticity will be assessed both in all the cases. When the evidence provided is a signed or unsigned pdf the authenticity will be assessed by the DOME Trust Service Provider for Certification, and the corresponding VC will be created for the CSP to be included in their DOME compliance profile.

DOME compliance approach is prepared to support the acceptance of VCs of the certificates issued by certification agencies as depicted in Figure 3.1.4.

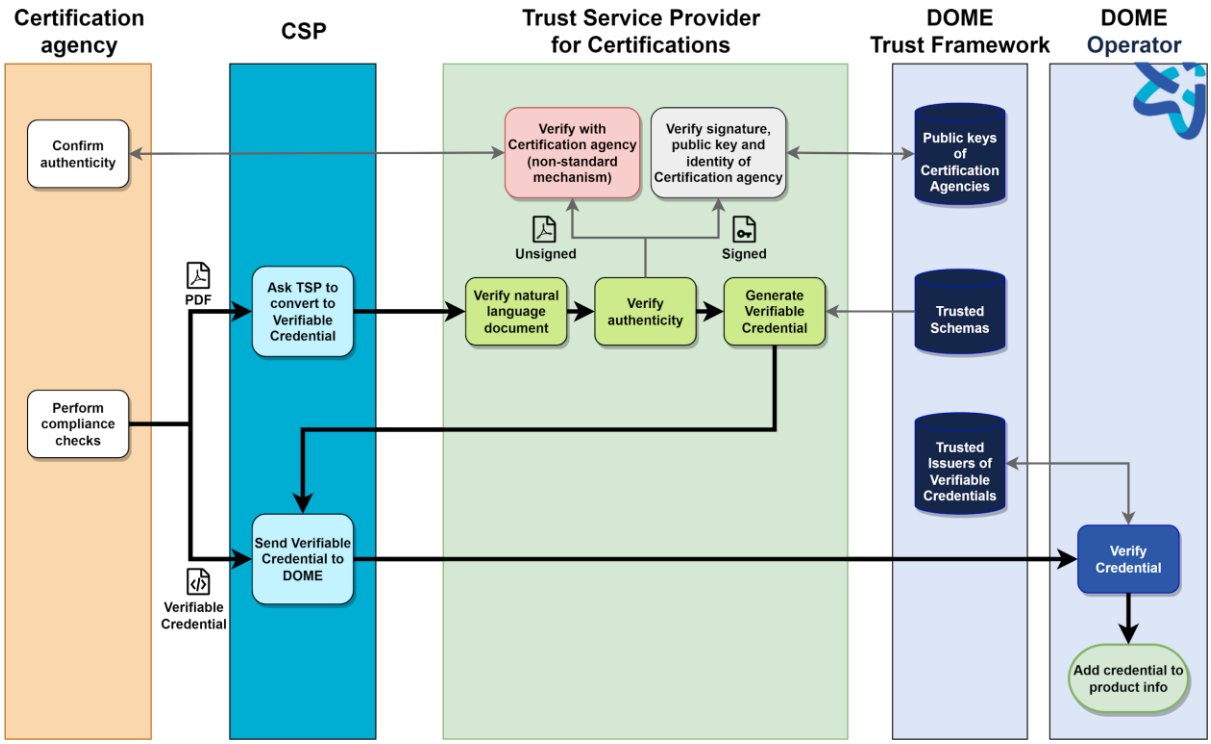
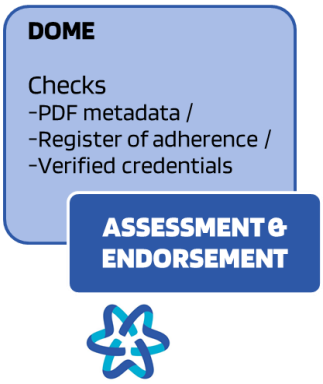
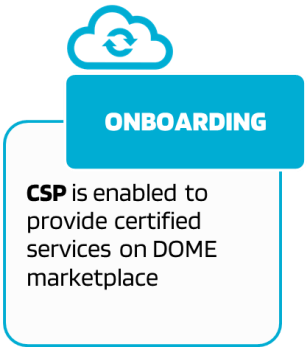


Figure 3.1.4 Certification accreditation cases in DOME.



Step 3 - Certification assessment: DOME assesses the validity of the certificate and if valid generates the related Verified Credential for the CSP to be stored in the wallet. The validation is done through the assessment of specific controls (see 3.2.4.6 for detailed information) and when available checking the inclusion of the presented certificates in EUCR registry of adherence or other relevant databases. The certification assessment activity will be done in a continuous basis process.



Step 4- Service qualification and onboarding: The service is qualified in the DOME marketplace based on the valid certificates and the information is updated in the catalogue. Once the product receives the validation it will be visible in the marketplace pages including the Certification profile achieved through the validation.There are 3 compliance levels based on the types of evidence provided for the supported certifications. These are the different compliance levels a service can be qualified to:

DOME Level 1 - No certifications provided/achieved
DOME Level 2 - Some supported certifications have been verified
DOME Level 3 - All the supported certifications have been verified by DOME

3.2 Tool supported methodological framework

This section presents the tools and software components supporting the processes described in section 3.1.

3.2.1 Continuous compliance supporting framework

Currently the compliance component is a web application to be accessed by a) the CSP to upload the certificates and complete specific information about the certifications b) the validators of the certifications, to access the requested information and manually assess the validity of the certifications. Once the validity of the certificate is assessed, the Certification Validator through the compliance component requests the issuance of the corresponding VC, to the VC issuer. The CSP receives the issued VC and stores it on his/her wallet. To end the process, the CSP uploads the valid VC with information about the validity of the certificates to the DOME marketplace, which updates the Compliance profile of the product, based on the information inside the VC. This process is depicted in the following picture (figure 3.2.1) :

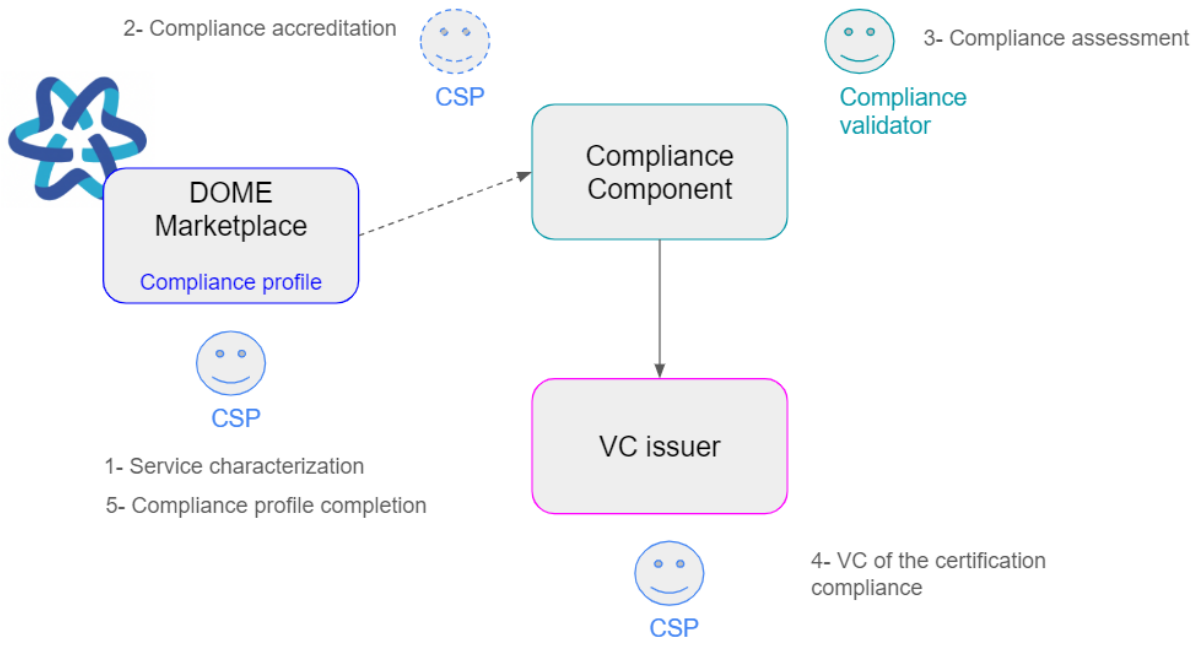


Figure 3.2.1.1. DOME compliance tool supported validation process at M18.

As explained, some of the steps of the figure above will be automatized or made transparent for the CSP in the next version of the Compliance Component at M36, such as the connection to the Compliance component or the automatization of the validation of the certificates. In the current version, the CSP is redirected from the Marketplace to the compliance form, while in the next version it is planned to be done directly in the compliance profile tab of the DOME Marketplace. Moreover, in the current version the validity of the certification is manually assessed by the experts. In the next version, the process will be automated as much as possible.

In the following text, the controls that have been identified as part of the process of the generation of the verified credentials once the manual process validation has been done, are presented. The list of controls proposed for the verified credentials is listed below. Additionally, in the table these fields are further detailed:

Controls considered:

- Issue date. The date when the certificate was issued. This marks the beginning of the Verified Credentials validity period.
- Expiration date. The date when the VC expires. After this date, the VC is no longer valid and needs to be renewed.
- Type of standard accreditation. The specific standard or framework the organisation is accredited for. This indicates the type of certification achieved, such as ISO/IEC standards.
- Scope. The extent and boundaries of the certification. It defines what parts of the organisation or which services are covered by the certificate.
- Certificate Number/ Certification ID. It is a unique and univocal code to identify the certificate issued.

- Issuer of the certificate. The name of the entity or authority that issued the VC. This organisation will validate that the information provided by the CSP is correct.
- Website of the issuer. The official website of the issuer.
- Name of the organisation (CSP). The name of the Cloud Service Provider (CSP) that received the VC. This is the entity being accredited
- Legal Address. The official registered address of the CSP, typically used for legal and official correspondence.
- ISO Country code. The ISO 3166-1 alpha-2 country code for the country where the CSP is legally registered.
- Website of the organisation (CSP). The official website of the CSP, included for providing more information about the services and background of the company
- Organization´s (CSP) email contact. The primary contact email address for the CSP. This can be used for inquiries and official communications.
- Product specification. A detailed description of the product or service that has been accredited. This includes the features and capabilities of the product.
- Version of the product *, The specific version of the product or service that has been accredited. It is important to mention that this field is relevant for distinguishing between different iterations of the product.

In section 3.2.4.6 a detailed table includes a description of the indicated controls.

3.2.2 Functional and technical description

3.2.2.1 Requirements covered by this prototype

As reported in D2.1 [4], the compliance validation features are related to several requirements of the DOME platform. In the next table the coverage of the requirements by the current prototype are presented. The advances and details of the current implementation is described in the Coverage column.

Table 3.2.2.1.1. DOME compliance component requirements coverage at M18

Req ID.	Requirement coverage at M18
RQ-21	Not yet Covered - Currently the compliance customization has not been developed. Nevertheless it is envisioned at process level (i.e.) but not supported by the Marketplace at M18.
RQ-63	Satisfied - The marketplace can flag each service with respect to compliance through the assessment of the certificates and the related information.
RQ-34	Satisfied- Users can manage their certificates through the Compliance component, including the uploading of certificates.

3.2.2.2 Prototype architecture and Components description

The architecture of the DOME compliance component is depicted in the following figure.

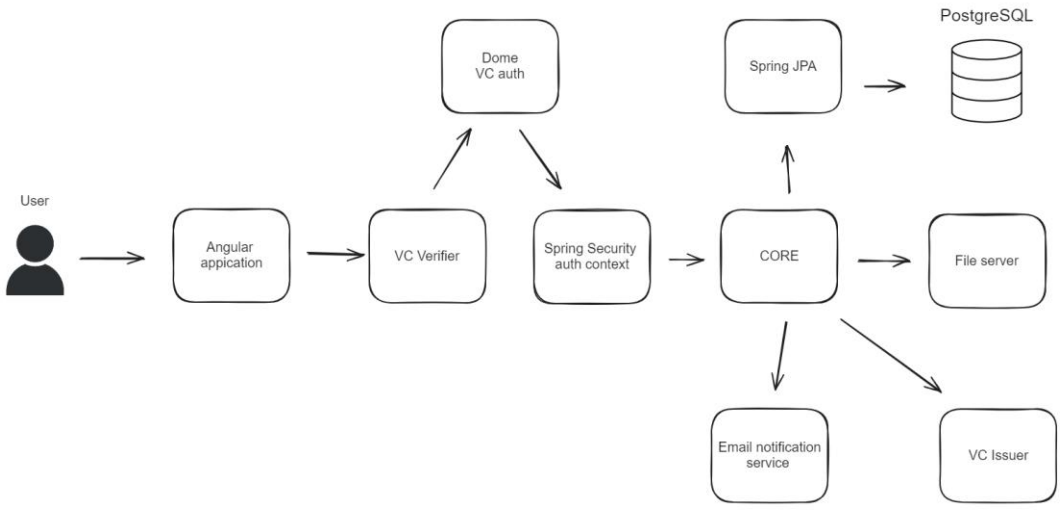


Figure 3.2.2.2.1 DOME compliance component architecture

- Angular application: This subcomponent is the entry point of the user as it is the user interface of the DOME compliance component from which the user can execute the necessary actions. In the case of the cloud service provider users, this interface allows them to fill in the necessary information for subsequent validation. In the case of the Certification Validator user, the interface allows the review of the data already entered by the cloud service provider.
- VC Verifier: This subcomponent is in charge of obtaining the verified credentials of the user and verifying that they are correct.
- DOME VC auth: This subcomponent has been developed by DOME WP3 and is responsible for authenticating users within the DOME marketplace. This subcomponent obtains the user information from the verified credentials and checks if the user has permissions or not to access the system.
- Spring Security auth context: It is the sub-component that stores the details of who is authenticated in the system.
- Core: It is the main subcomponent, being responsible for orchestrating all communication with the database, with the user interface and with the rest of the subcomponents.
- Spring JPA: It implements the database access layer.
- PostgreSQL: It is the database in which the persistent data is stored.
- File server: This subcomponent is in charge of managing the files, it allows the users to upload and download files with different formats.
- Email notification: It is responsible for managing the sending of emails to the user to notify them the updates that happen during the compliance process
- VC Issuer: This subcomponent has been developed by DOME WP3 and is responsible for the generation of the verified credentials of the product specification which indicates the standards for which it is accredited

3.2.2.3 Technical specifications

This section details the programming language, libraries and databases required for the implementation of the DOME compliance component.

The web application has been implemented in Angular. Angular is a robust platform and framework designed for building single-page client applications using HTML and TypeScript, maintained by Google. It is known for its modular architecture, where applications are divided into modules and components. Each component consists of a TypeScript class, an HTML template, and optional CSS styles, enabling developers to build reusable and maintainable code blocks.

Angular applications are structured in:

- Modules organise the application into cohesive blocks of functionality.
- Components are the fundamental building blocks, each with its own logic, view, and styles.
- Services encapsulate business logic and data access, leveraging Angular's powerful dependency injection system.
- Directives and Pipes enhance the functionality and appearance of the application, allowing for dynamic and formatted content.

One of the advantages of Angular is that it includes two-way data binding, which ensures synchronisation between the model and view, reducing boilerplate code. Its dependency injection system enhances code manageability and testability. Angular's extensive ecosystem

and strong community support, backed by Google, provide developers with a wealth of resources and integrations.

The backend subcomponents have been implemented in Spring Boot. Spring Boot is a framework for building production-ready applications quickly and with minimal configuration using Java. Part of the larger Spring ecosystem, it simplifies the development of stand-alone, production-grade Spring applications by offering convention over configuration. Spring Boot is built on top of the Spring Framework and provides a range of out-of-the-box features that helps streamline the development process.

Spring Boot applications are structured in the following components:

- Starters are dependency descriptors that simplify Maven or Gradle configuration. They provide a set of commonly used dependencies for various functionalities, such as web development or data access.
- Auto-Configuration automatically configures Spring applications based on the dependencies present in the project, reducing the need for manual setup.
- Embedded Servers allow Spring Boot applications to be run as stand-alone applications without needing an external server, using embedded servers like Tomcat, Jetty, or Undertow.

The main advantages of Spring Boot are:

- Rapid development: With its convention over configuration approach and auto-configuration features, Spring Boot reduces the time required to set up and develop applications.
- Microservices friendly: Spring Boot is ideal for building microservices due to its lightweight nature and support for embedding servers, making it easy to create self-contained units of functionality.
- Production-ready: It includes various production-ready features, such as metrics, health checks, and externalised configuration, ensuring that applications are ready for deployment.
- Wide ecosystem: Being part of the Spring ecosystem, it integrates seamlessly with other Spring projects, such as Spring Data, Spring Security, and Spring Cloud, providing a comprehensive suite of tools for enterprise application development.

Finally, for the database, PostgreSQL has been chosen. PostgreSQL is a powerful, open-source relational database management system (RDBMS) known for its robustness, extensibility, and compliance with SQL standards. It supports complex queries, ACID transactions, and a variety of data types and indexing techniques. PostgreSQL is highly extensible, allowing users to create custom data types, functions, and operators, making it ideal for a wide range of applications, from web services to large-scale data warehousing.

3.2.3 Delivery and usage

This section provides the details of the delivery package. First, the structure of the repositories and the instructions for the installation are described. Then, how to use the application depending on the role is detailed. Finally, licensing information and downloading instructions are provided.

3.2.3.1 Package information

The delivery package is composed of two projects, one for the frontend and another one for the backend. See below the structure of each project and the description of the main folders and files.

Backend

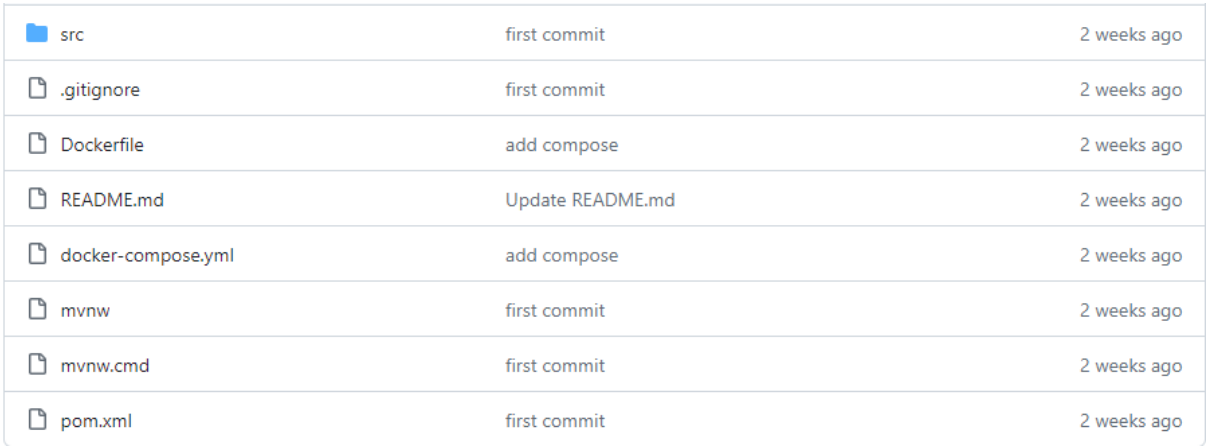
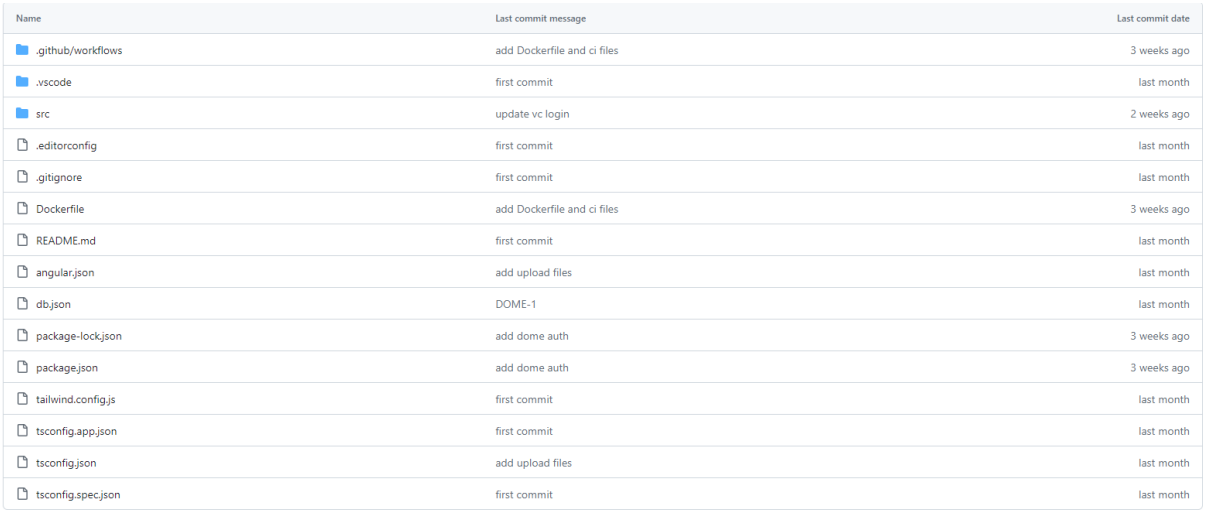


Figure 3.2.3.1.1 DOME compliance Backend component package information

- README.md provides an overview and documentation for the Angular project, including setup instructions.
- pom.xml defines the project's dependencies and builds configuration for Maven.
- mvnw.cmd is a script to run Maven commands without a pre-installed Maven on Windows.
- Dockerfile contains instructions to build a docker image for the Spring Boot application.
- docker-compose.yml: configures and runs multi-container docker applications, managing services like the app and database.
- src folder contains the source code, configuration files, and resources for the Spring Boot application.
- test folder contains test code for running unit tests

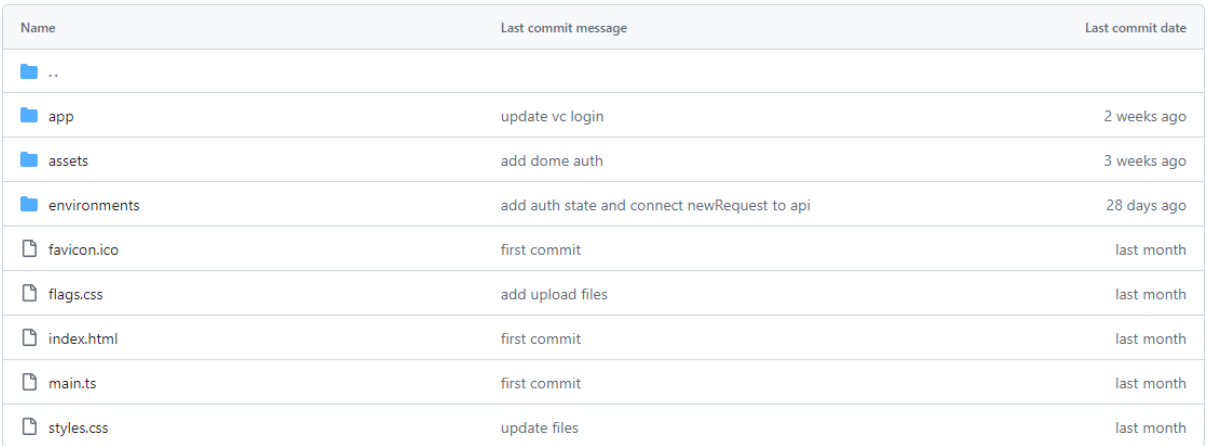
Frontend



Name	Last commit message	Last commit date
.github/workflows	add Dockerfile and ci files	3 weeks ago
.vscode	first commit	last month
src	update vc login	2 weeks ago
.editorconfig	first commit	last month
.gitignore	first commit	last month
Dockerfile	add Dockerfile and ci files	3 weeks ago
README.md	first commit	last month
angular.json	add upload files	last month
db.json	DOME-1	last month
package-lock.json	add dome auth	3 weeks ago
package.json	add dome auth	3 weeks ago
tailwind.config.js	first commit	last month
tsconfig.app.json	first commit	last month
tsconfig.json	add upload files	last month
tsconfig.spec.json	first commit	last month

Figure 3.2.3.1.2 DOME compliance Frontend component package information

- Angular.json defines the configuration and settings for the Angular project, including build and serve options.
- Package.json specifies the project's metadata, dependencies, and scripts for building and running the Angular application.
- tsconfig.json configures the TypeScript compiler options for the Angular project.
- dockerfile contains instructions to build a docker image for the Angular application.
- README.md provides an overview and documentation for the Angular project, including setup instructions
- src folder contains the source code, including components, services, modules, and assets for the Angular application.
    - app folder contains the source code, including components, services, modules, and assets for the Angular application.
    - assets folder contains static assets like images and PDFs.
    - environments folder contains environment-specific configuration files.
    - index.html is the main HTML file for the Angular application.
    - main.ts is the main entry point for the Angular application.
    - styles.css is the global CSS file for the Angular application



Name	Last commit message	Last commit date
..		
app	update vc login	2 weeks ago
assets	add dome auth	3 weeks ago
environments	add auth state and connect newRequest to api	28 days ago
favicon.ico	first commit	last month
flags.css	add upload files	last month
index.html	first commit	last month
main.ts	first commit	last month
styles.css	update files	last month

Figure 3.2.3.1.3 DOME compliance src folder

3.2.3.2 Installation instructions

This section provides the steps to follow to run the component. They are also detailed in the Readme.md file of each repository.

To run the application in a local environment, follow these steps:

1. Clone the repository to your local machine.
2. Navigate to the project directory.
3. Add the application.properties file for dev environment
4. Install dependencies using mvn, (PostgreSQL, structure will be created automatically)

```
mvn clean install
```

5. Start the API in PROD server:

```
mvn spring-boot:run -P prod
```

6. The server starts automatically on http://localhost:8080/

Application.properties contains all the configuration of the differents services examples:

```
#DB_POSTGRES
spring.datasource.url=jdbc:postgresql://localhost:5432/dome
spring.datasource.username=root
spring.datasource.password=root
spring.jpa.properties.hibernate.format_sql=true
spring.jpa.show-sql=true
spring.jpa.hibernate.ddl-auto=update

# PROPERTIES
spring.mvc.converters.preferred-json-mapper=jackson
file.upload-dir=C:/dome-upload
spring.servlet.multipart.max-file-size=10MB
spring.servlet.multipart.max-request-size=10MB

#SWAGGER_UI
springdoc.api-docs.path=/api-docs
springdoc.swagger-ui.path=/api-docs.html

#SPRING-MAIL
spring.mail.host=sandbox.smtp.mailtrap.io
spring.mail.port=25
spring.mail.username=b3c98a594c9ae2
spring.mail.password=490029367a0d9b
spring.mail.properties.mail.smtp.starttls.enable=true
spring.mail.properties.mail.smtp.auth=true
spring.mail.properties.mail.smtp.connectiontimeout=5000
spring.mail.properties.mail.smtp.timeout=5000
spring.mail.properties.mail.smtp.writetimeout=5000

#LOGS
logging.file.name=dome-certification.log
logging.level.root=INFO

jwt.secret.key= YOUR-SECRET-KEY-HERE
server.port=8080
```

Figure 3.2.3.2.1 Application.properties content

Frontend

To run application in a local environment:

1. Clone the repository to your local machine
2. Install dependencies using npm

```
npm install
```

3. Start server using Angular CLI command

```
ng s -o
```

4. Web application will open automatically at http://localhost:4200/

3.2.3.3 User Manual

This section describes how to use the DOME compliance application. The user can have different roles, cloud service provider or Certification Validator, depending on the role, the user is able to execute a set of actions so different use cases are detailed.

Use Case 1 - Login of Cloud Service Provider or Certification Validator

1. Log in with DOME verified credentials

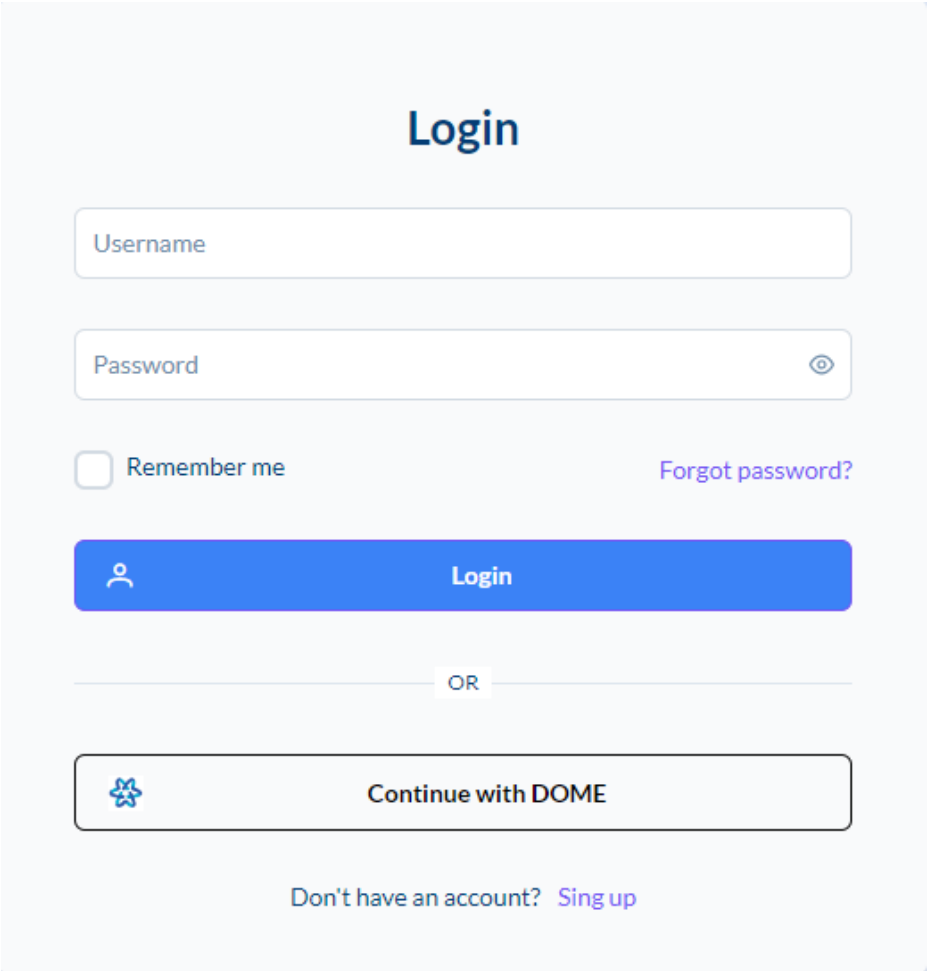


Figure 3.2.3.3.1 DOME compliance application login

a. Click on “Continue with DOME” button
b. Scan QR code with a mobile phone and select the verified credential store in your wallet

Figure 3.2.3.3.2 DOME VC

Once the VC has been authorised the user will be able to log into the application.

Use Case 2 - Cloud Service Provider Request a compliance verification

Once the user is logged in, a form is displayed to fill in the information about the product specification and to upload the certificates

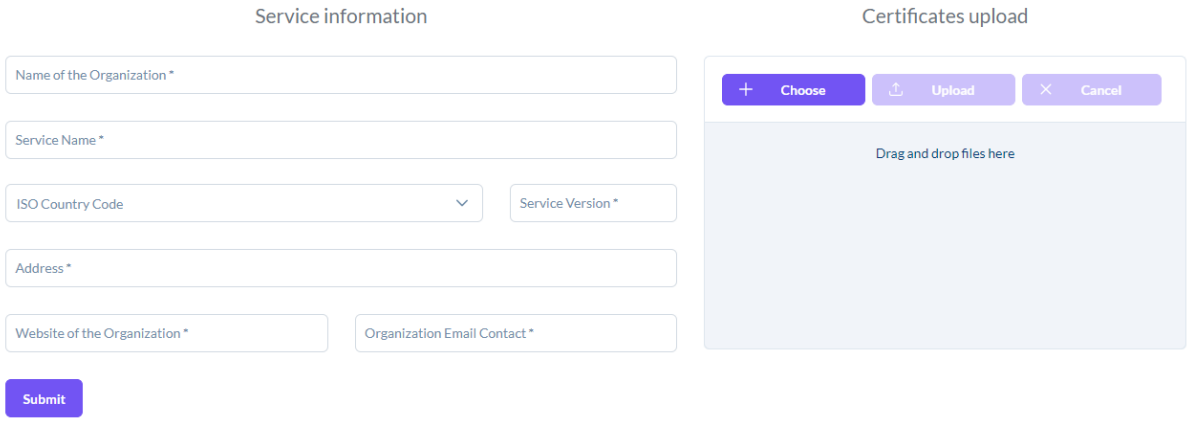


Figure 3.2.3.3.3 DOME compliance form

1. Cloud Service Provider has to fill in the requested information: Name of the organisation, service name and version, country, ISO country code, address, website of the organisation and email contact

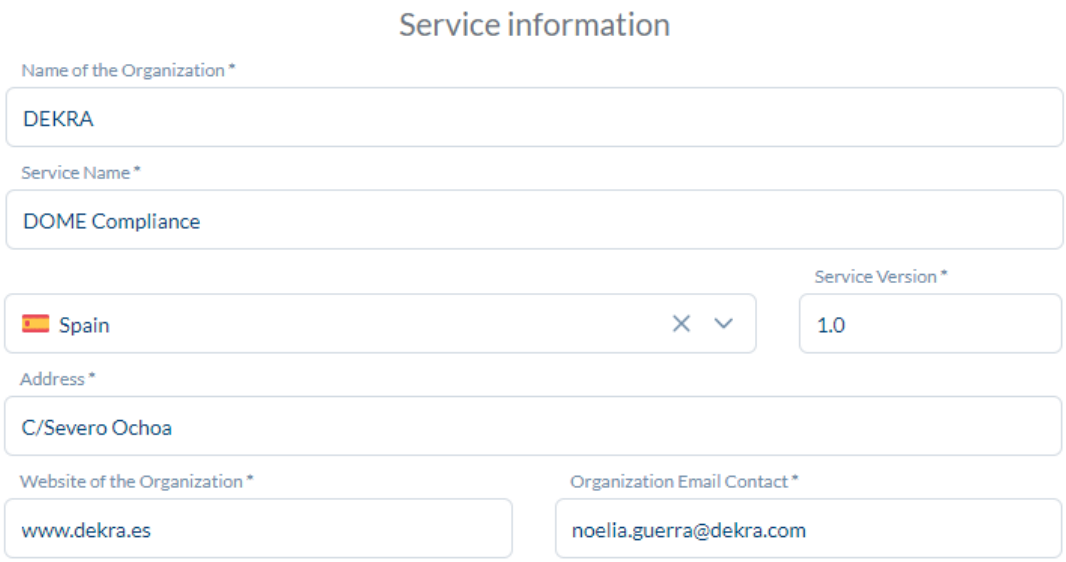


Figure 3.2.3.3.4 DOME compliance form fields

2. Then, he/she has to upload the certificates of the service

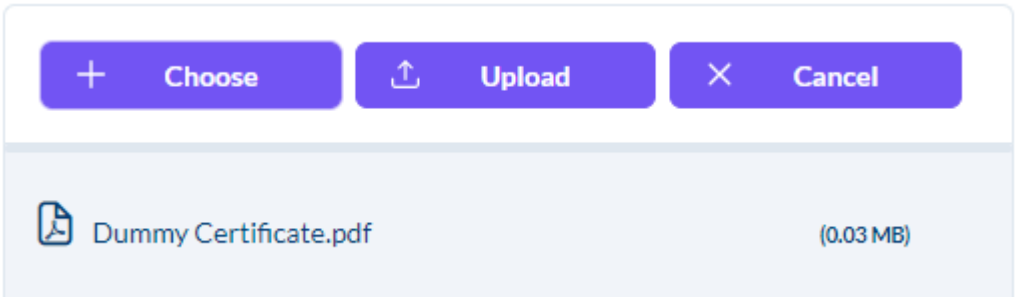


Figure 3.2.3.3.5 DOME compliance form certificates upload

3. Then click on “Submit” button
4. CSP will receive an email indicating that the process is in progress

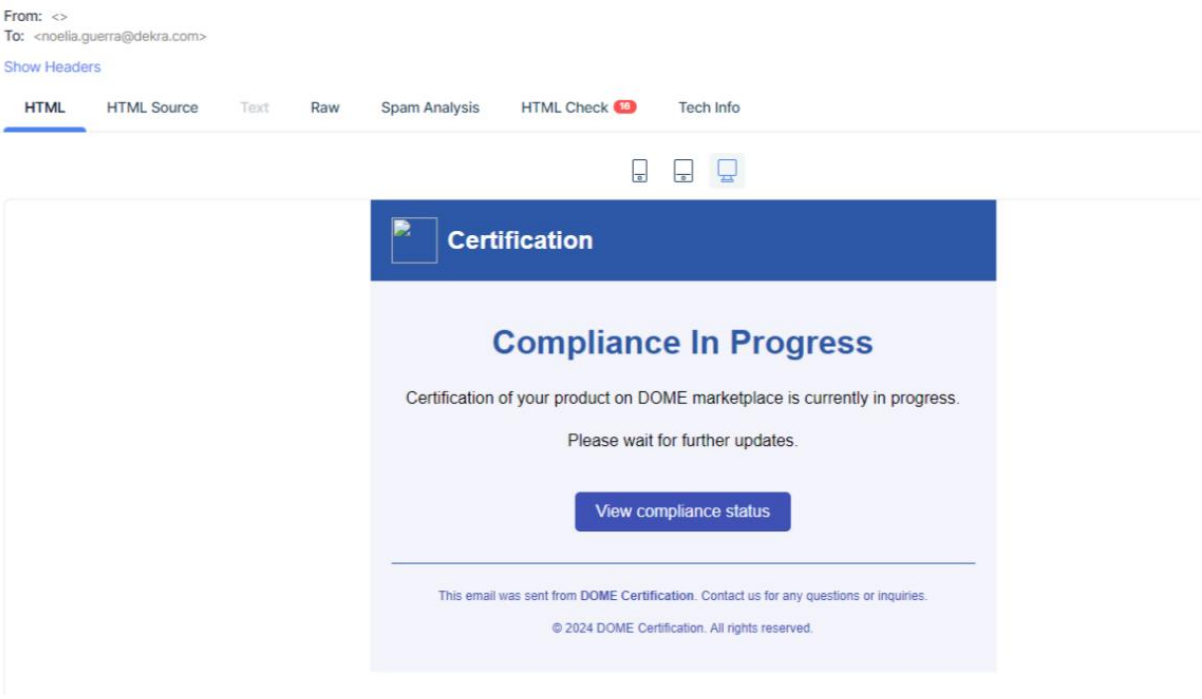


Figure 3.2.3.3.6 DOME compliance status: In progress.

Use Case 3 - Cloud Service Provider check the status of the requests

After log in, CSP can check the status of all their requests clicking on Dashboard tab

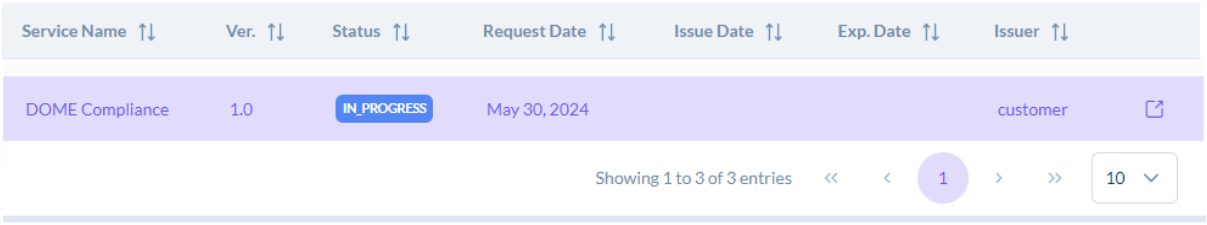


Figure 3.2.3.3.7 DOME compliance application Dashboard for CSPs.

Use Case 5 - Certification Validator validates the certificates

After logging in, the Certification Validator will see the list of pending validations.

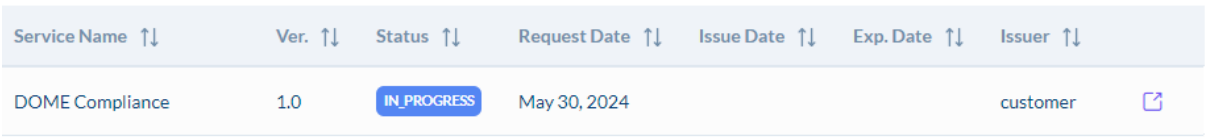


Figure 3.2.3.3.8 DOME compliance application Dashboard for Certification Validator.

1. The Certification Validator reviews the information provided by the CSP clicking on 

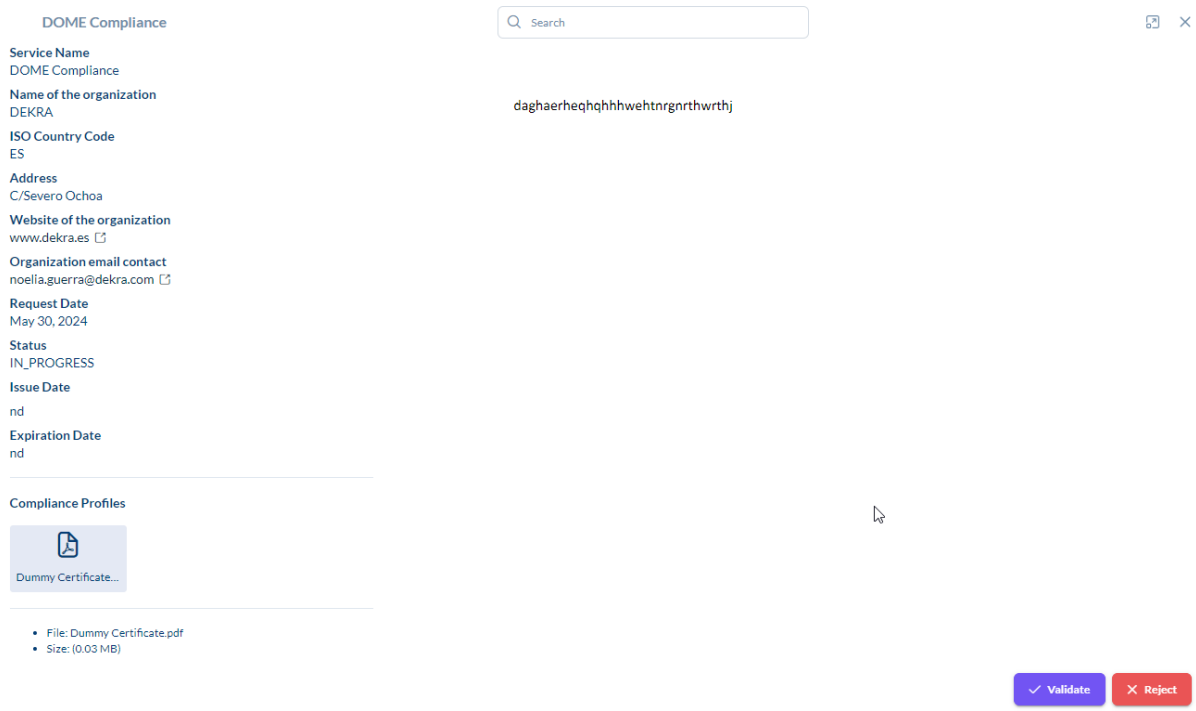


Figure 3.2.3.3.9 Information about the Certificate

2. After the information is reviewed, the Certification Validator validates the request clicking on “Validation” button
3. Then, the Certification Validator selects the compliance profiles

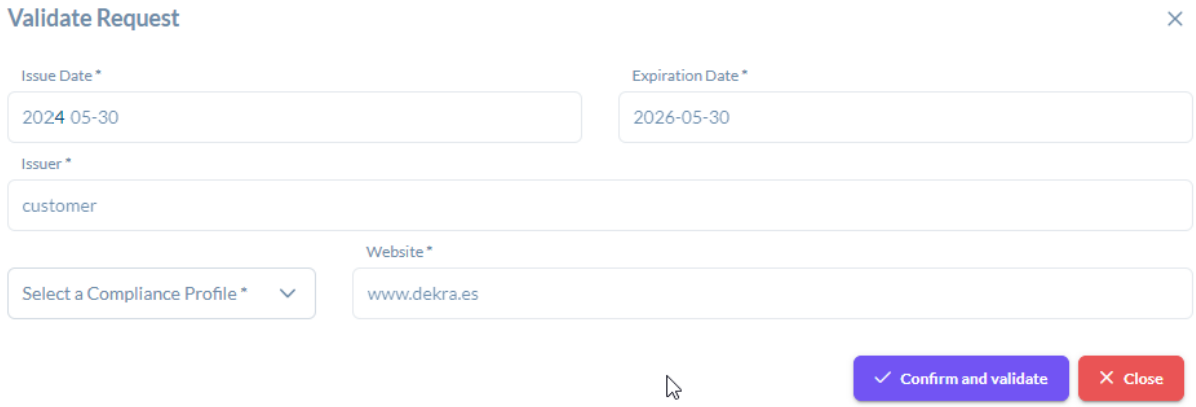


Figure 3.2.3.3.10 Compliance validation

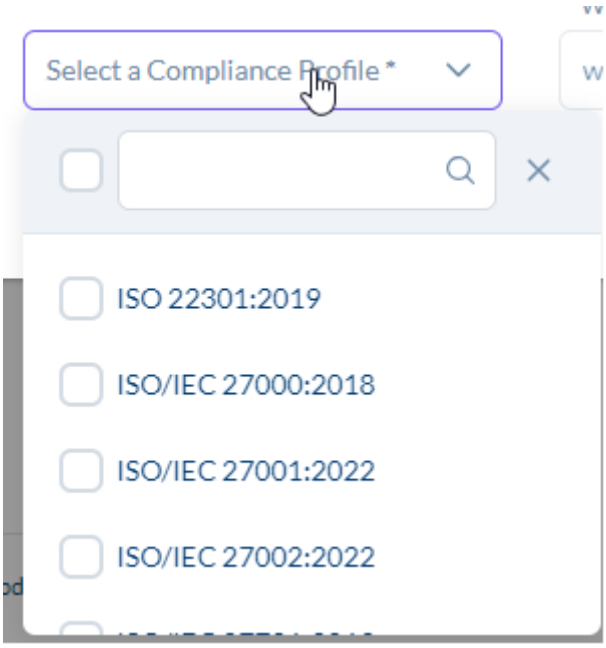


Figure 3.2.3.3.11 Compliance profile selection

4. And click on “Confirm and validate”
5. The VC of the product is automatically generated and sent to CSP in an email

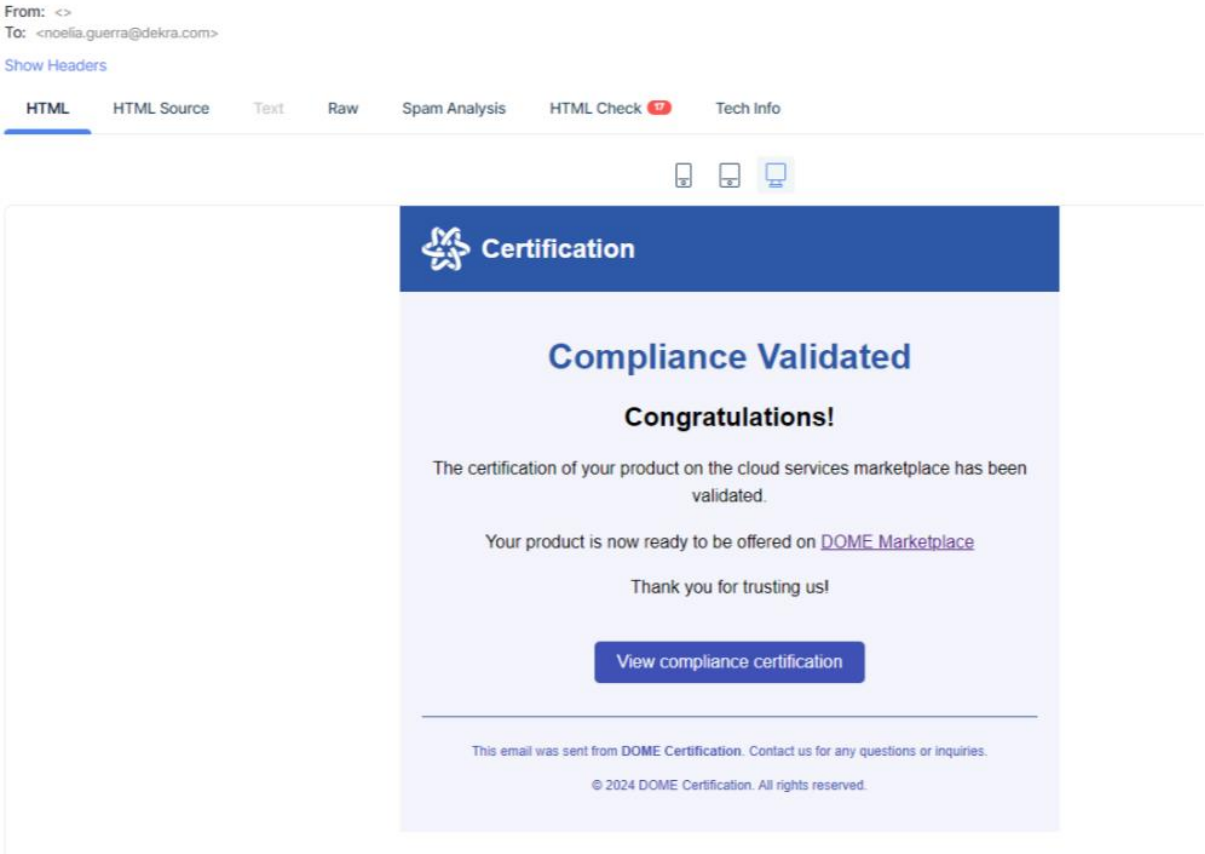


Figure 3.2.3.3.12 Compliance validation notification

6. CSP and Certification Validator can also check that the status of the request has been changed to validated in the “Dashboard” tab.

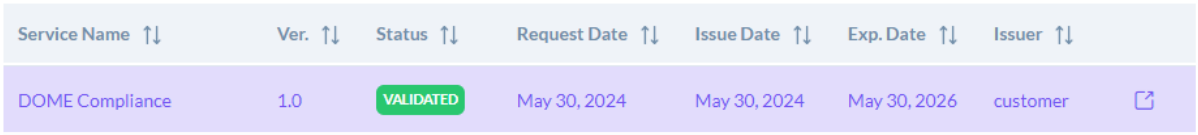


Figure 3.2.3.3.13 Compliance validation in the CSP dashboard

Use Case 5 - Certification Validator rejects the certificates

After log in, the Certification Validator will see the list of pending validations.

7. The Certification Validator review the information provided by the CSP
8. After the information is reviewed, the Certification Validator rejects the request clicking on “Reject” button
9. CSP is notified via email that the request has been rejected

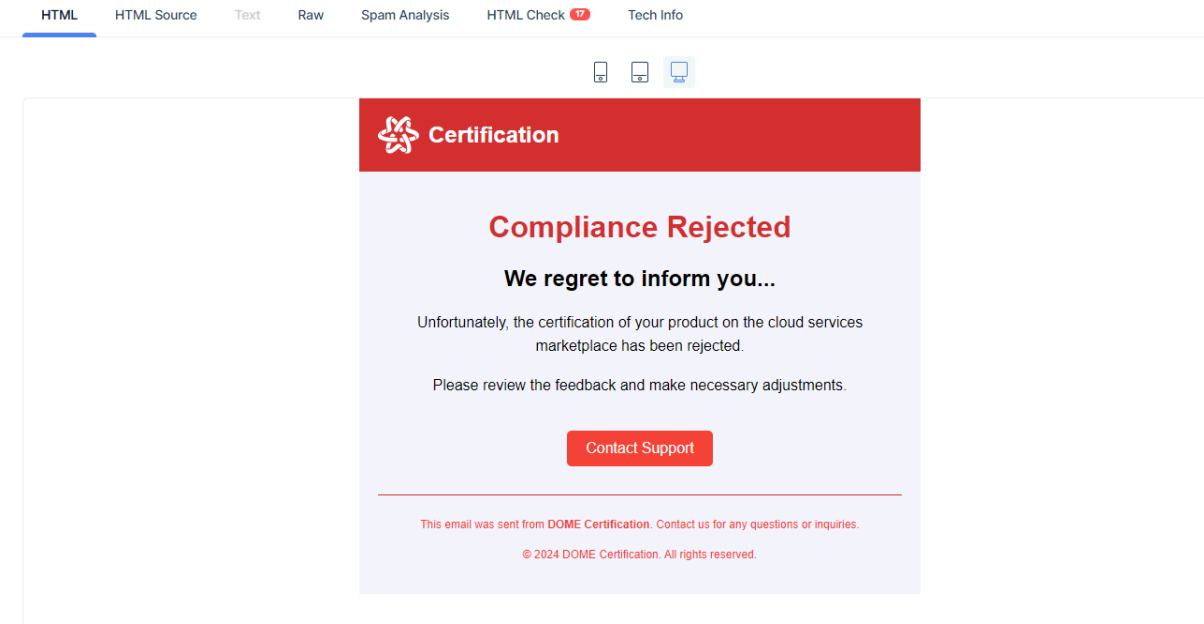


Figure 3.2.3.3.14 Compliance rejection notification

10. CSP and Certification Validator can also check that the status of the request has been changed to rejected in the “Dashboard” tab.

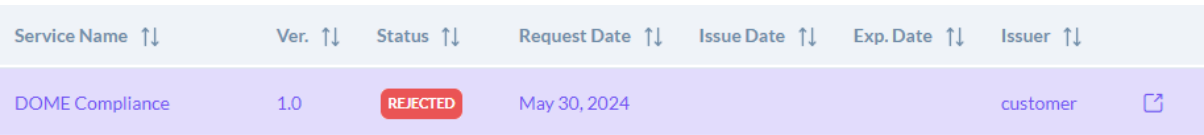


Figure 3.2.3.3.15 Compliance rejection in the CSP dashboard

Use Case 6 - VC of the product expires

The VC of the products expires in two years, so the CSP will receive a notification indicating that the VC expires in 2 months to initiate a new request.

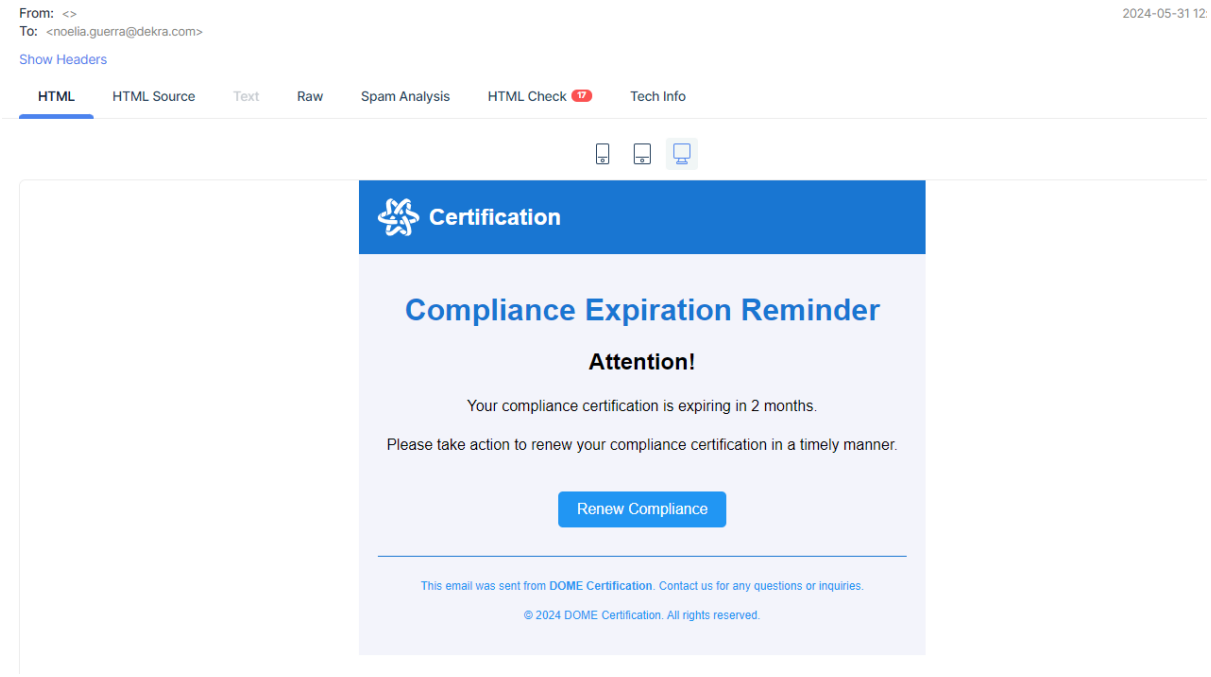


Figure 3.2.3.3.16 Compliance expiration reminder

Once the VC has expired, CSP will receive an additional notification.

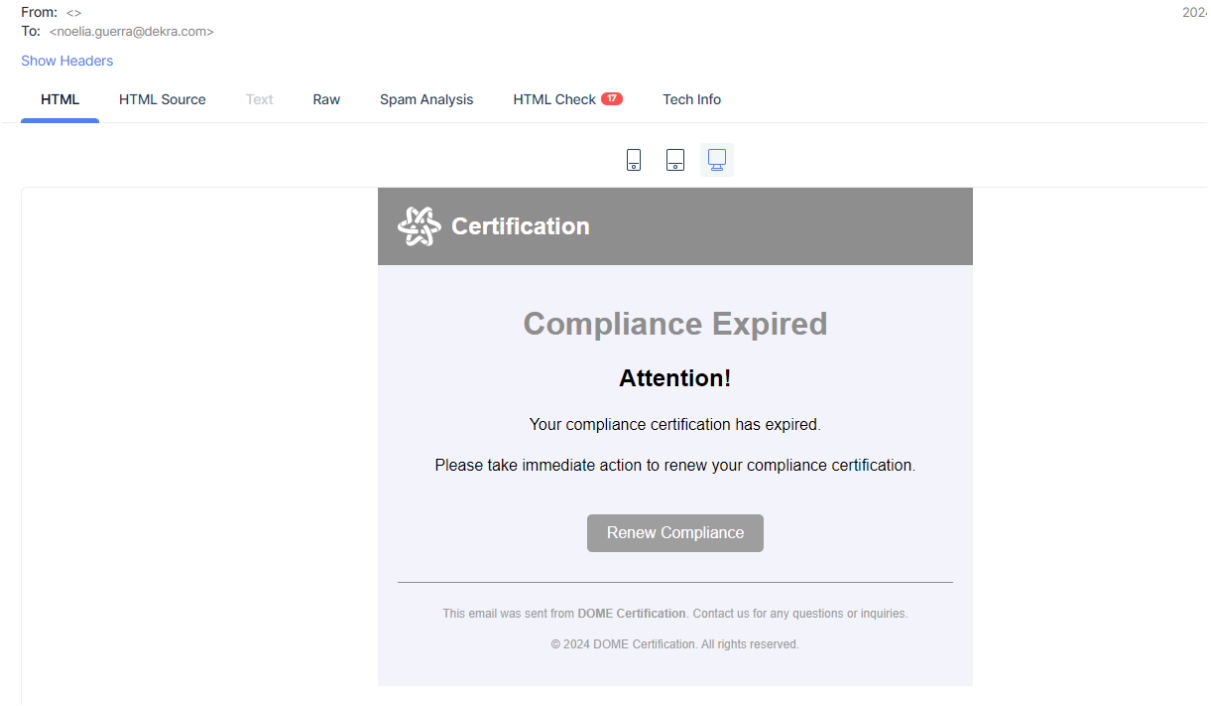


Figure 3.2.3.3.17 Compliance expiration notification

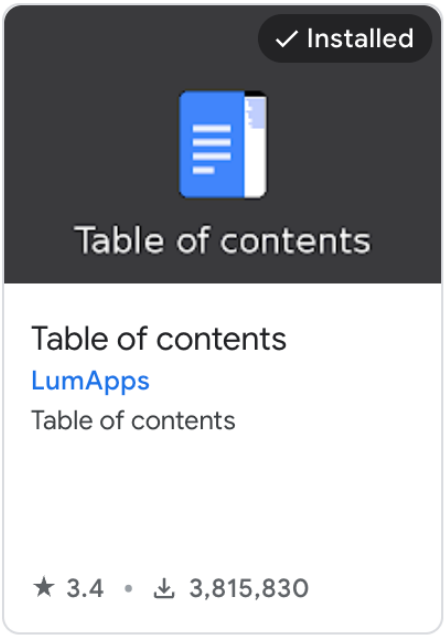
3.2.3.4 Licensing information

This component is offered under Apache 2.0 license. Detailed information can be found in the GitHub repository.

3.2.3.5 Download

The source code of the component is available in public DOME GitHub repository

- Backend: https://github.com/DOME-Marketplace/dome-certification-backend
- Frontend: https://github.com/DOME-Marketplace/dome-certification-frontend



3.2.3.6 Table of controls and examples

Controls to be assessed	Description	Example	How to assess the control
Issue date	The date when the certificate was issued. This marks the beginning of the Verified Credentials validity period	January 21, 2024	This control does not require assessment
Expiration date	The date when the VC expires. After this date, the VC is no longer valid and needs to be renewed	January 21, 2025	This control is not assessed, it is just monitorized when the expiration date gets closer
Type of standard accreditation	The specific standard or framework the organisation is accredited for. This indicates the type of certification achieved, such as ISO/IEC standards	ISO/IEC 27001	This control requires manual validation
Scope	The extent and boundaries of the certification. It defines what parts of the organisation or which services are covered by the certificate	Information Security Management System (ISMS)	This control requires manual validation
Certificate Number/ Certification ID	It is a unique and univocal code to identify the certificate issued	114272-2012-AE-ITA-ACCREDIA-CC4	This control requires manual validation
Issuer of the certificate	The name of the entity or authority that issued the VC. This organisation will validate that the information provided	DEKRA Testing and Certification S.A.U.	This control does not require assessment

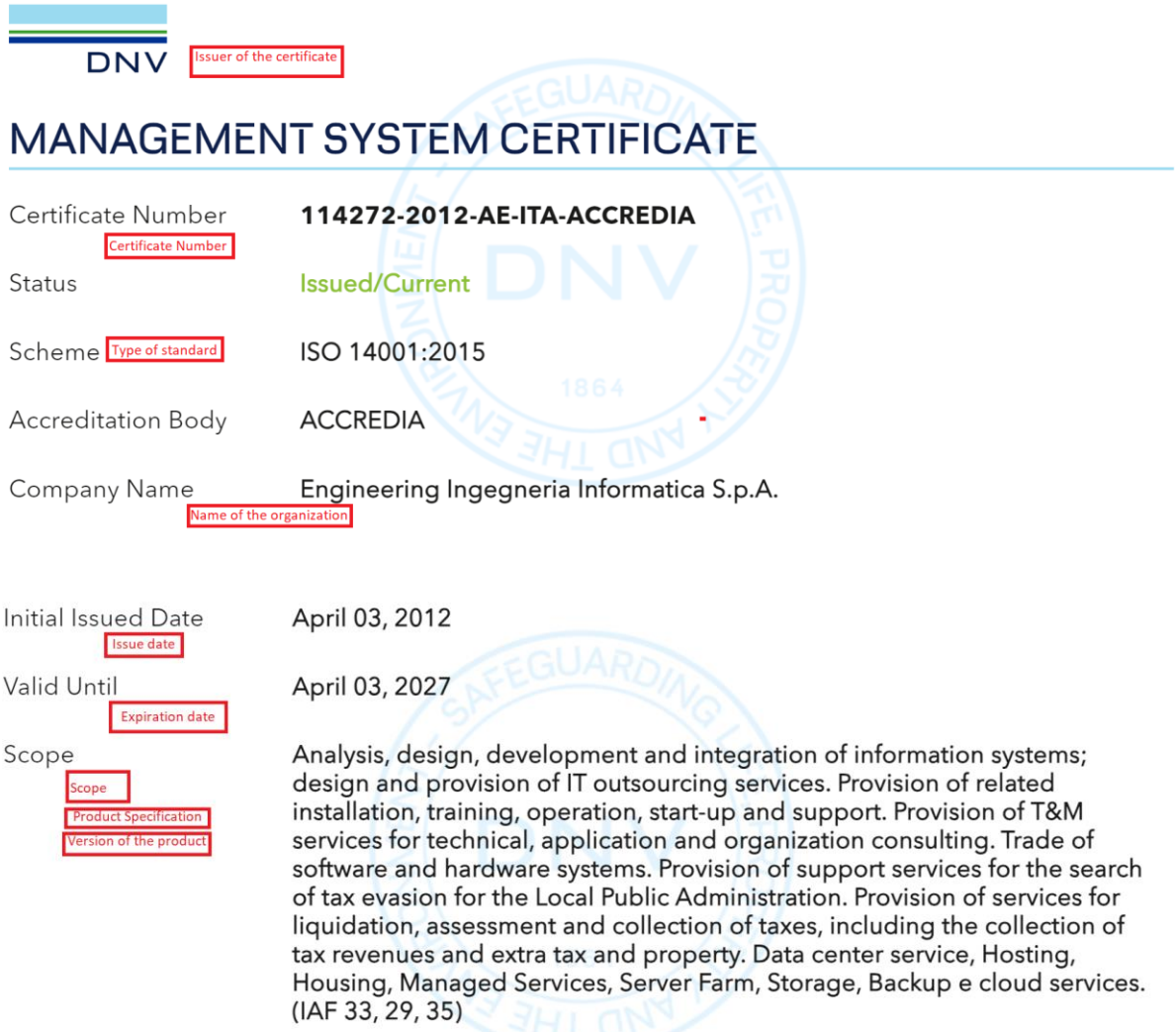
Controls to be assessed	Description	Example	How to assess the control
	by the CSP is correct		
Website of the issuer	The official website of issuer	https://www.dekra.com	This control does not require assessment
Name of the organisation (CSP)	The name of the Cloud Service Provider (CSP) that received the VC. This is the entity being accredited	Cloud Service Provider Test Inc.	This controls requires manual validation
Legal Address	The official registered address of the CSP, typically used for legal and official correspondence	Annaplein 254a, 1e verdieping, 2089, Oostkerkegem, Oost-Vlaanderen	This controls requires manual validation
ISO Country Code	The ISO 3166-1 alpha-2 country code for the country where the CSP is legally registered	BE	This controls requires manual validation
Website of the organisation (CSP)	The official website of the CSP, included for providing more information about the services and background of the company	https://csp-test.com	This control requires manual validation
Organization´s (CSP) Email Contact	The primary contact email address for the CSP. This can be used for inquiries and official communications	support@csp-test.com	This control requires manual validation
Product Specification	A detailed description of the product or service that has been accredited. This	Service x: A services that incorporated several interaction between systems to provide	This control does not require assessment

Controls to be assessed	Description	Example	How to assess the control
	includes the features and capabilities of the product	more flexibility and interoperability	
Version of the product *	The specific version of the product or service that has been accredited. It is important to mention that this field is relevant for distinguishing between different iterations of the product	Version 2.0	This control does not require assessment

* It is important to note that if a product that is already certified and uploaded in DOME releases a new version, some considerations should be taken into account.

It will be necessary to consider the differences between the current version with which the certificate has been held and the new one. It will be the CSP´s responsibility to identify whether the differences between the version with which the original certificate was obtained and the new version that the product may have are relevant from the point of view of the cybersecurity certificate that appears in DOME. If these differences are relevant with respect to the Cybersecurity requirements evaluated and validated in the first version, it will be necessary to review the compliance process completely.

In order to clarify how to use these specific controls, an example has been setup, considering one real certificate:



DNV Issuer of the certificate

MANAGEMENT SYSTEM CERTIFICATE

Certificate Number **114272-2012-AE-ITA-ACCREDIA**
Certificate Number

Status Issued/Current

Scheme Type of standard ISO 14001:2015

Accreditation Body ACCREDIA

Company Name Engineering Ingegneria Informatica S.p.A.
Name of the organization

Initial Issued Date April 03, 2012
Issue date

Valid Until April 03, 2027
Expiration date

Scope
Scope
Product Specification
Version of the product

Analysis, design, development and integration of information systems; design and provision of IT outsourcing services. Provision of related installation, training, operation, start-up and support. Provision of T&M services for technical, application and organization consulting. Trade of software and hardware systems. Provision of support services for the search of tax evasion for the Local Public Administration. Provision of services for liquidation, assessment and collection of taxes, including the collection of tax revenues and extra tax and property. Data center service, Hosting, Housing, Managed Services, Server Farm, Storage, Backup e cloud services. (IAF 33, 29, 35)

Certificate : 114272-2012-AE-ITA-ACCREDIA (dnv.com)

Controls to be assessed	Example
Issue date	April 03, 2012
Expiration date	April 03, 2027
Type of standard accreditation	ISO 14001:2015
Scope	Analysis, design, development and integration of information systems; design and

Controls to be assessed	Example
	provision of IT outsourcing services. Provision of related installation, training, operation, start-up and support. Provision of T&M services for technical, application and organization consulting. Trade of software and hardware systems. Data center service, Hosting, Housing, Managed Services, Server Farm, Storage, Backup e cloud services. (IAF: 33, 29, 35) Evaluated according to the requirements of Technical Regulations RT-09
Certificate Number/ Certification ID	114272-2012-AE-ITA-ACCREDIA-CC4
Issuer of the certificate	ACCREDITED UNIT: DNV Business Assurance Italy S.r.l., Via Energy Park, 14 - 20871 Vimercate (MB) - Italy - TEL: +39 68 99 905. www.dnv.it
Website of the issuer	www.dnv.it
Name of the organisation (CSP)	Engineering DHUB S.p.A.
Legal Address	Viale Carlo Viola, 76 - 11026 Pont-Saint-Martin (AO) - Italy
ISO Country Code	BE
Website of the organisation (CSP)	It is not included in the certificate
Organization´s (CSP) Email Contact	It is not included in the certificate
Organization´s (CSP) Email Contact	It is not included in the certificate
Product Specification	QuantumCloud Pro
Version of the product	It is not included in the certificate

4 Conclusions

This document revolves around the first prototype of the DOME Compliance Component delivered at M18. The goal of this component is to establish the compliance framework in DOME and provide the supporting tools to assess such compliance against relevant frameworks like the Cloud Rulebook.

In this first prototype the DOME compliance component allows the CSPs to provide the certificates and related information about them, and supports the Certification Validators to assess the validity of a first set of certificates (the ISO related ones). Part of the activities carried out in the context of the compliance framework have included the design of a new type of VC to represent the valid certificates. At M18, the VC issuer is able to create this special type of VC for the DOME user to be able to upload it to the portal. Moreover, the DOME marketplace is able to characterise the products based on the information about the compliance assessment, both at product level and at certificate level.

Future iterations of this prototype will include 1) the connection via API of the DOME catalogue and the Compliance component enhancing the user experience and simplifying the compliance process, 2) the coverage of the complete list of the certifications and (actionable) schemes to be included in the future Cloud Rulebook and, 3) the automation increasement in the assessment of the validity of the certificates.

\

5 References

[1] European Commission, Cloud Computing policies, 2024 https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

[2] Gaia-X Policy Rules Conformity Document (PRC). Gaia-X_Policy_Rules_Conformity Document - prc_document_2023 Release

[3] CISPE Cloud https://cispe.cloud/

[4] D2.1- DOME requirements v1, DOME consortium, 2023.

[5] D3.1 - DOME reference architecture and specifications v1, DOME consortium, 2023