A framework for user centred privacy and security in the cloud

Standardisation and interoperability

Type (distribution level)	Public
Contractual date of Delivery	31/07/2016
Actual date of delivery	02/08/2016
Deliverable number	D4.3
Deliverable name	Standardisation and interoperability
Version	Final
Number of pages	20
WP / Task related to the deliverable	WP4 / Task 4.2
WP / Task responsible	Trust-IT
Author(s) (in alphabetical order)	Roberto G. Cascella, Stephanie Parker, Niccolò Zazzeri (Trust-IT)
Partner(s) Contributing	TRUST-IT
Document ID	CLARUS-D4.3-Standardisation_interoperability-v1.3
Abstract	This deliverable analyses the CLARUS value proposition and provides the main results concerning standardisation and interoperability issues highlighting how they are addressed in the design of the CLARUS architecture. The objective of this document is to assess how CLARUS is aligned with the standardisation roadmap built in Deliverable D2.5. The analysis considers the architecture design and the definition of the APIs.

Disclaimer

Table of Contents

1 Introduction

1.1 Scope of the Document

This document analyses the CLARUS architecture and framework in terms of interoperability and standardisation. It leverages the work carried out in WP2 on the identification of relevant best practices in security, privacy, and data format in order to map the requirements that have driven the design of the CLARUS architectural solution, presented in Deliverable D4.2 [1]. Moreover, it analyses the security as a service infrastructure and concepts for the CLARUS framework proposed in WP4, specifically in Deliverable D4.4 [2]. The result is a thorough analysis of interoperability in the context of CLARUS, including the data types supporting the two use cases, and the approach that must be followed to pursue the objective of building an interoperable framework. While the output can help identify potential gaps in the standardisation landscape and drive the work for the implementation of CLARUS started with the definition of the APIs in Deliverable D5.1 [3], it is also relevant in the context of the EU Cloud Computing Strategy and actions related to ICT standardisation in the Digital Single Market Strategy.

1.2 Outline

This document is structured as follows:

- Section 2 summarises the CLARUS value proposition and provides a general understanding of the concepts used in the deliverable to justify the need for interoperable and standardized solutions in CLARUS.
- Section 3 defines the concepts of interoperability-by-design used in CLARUS and revises the analysis of the standards provided in Deliverable D2.5 [4]. Finally, it analyses the CLARUS architecture and provides useful insights for the implementation of the CLARUS framework.
- Section 4 indicates how CLARUS contributes to the Digital Single Market (DSM) strategy.
- Section 5 concludes the document.

1.3 Revision History

Version	Date	Author	Description
0.1	19/06/2016	Trust-IT	Initial ToC
0.2	04/07/2016	Trust-IT	Added Section 2 and Section 4

0.3	12/07/2016	Trust-IT	Finalised Section 4. Added Section 3 and integrated contribution from AKKA about standards for Geo-Reference use case
0.4	26/07/2016	Trust-IT	Added Section 5
0.5	28/07/2016	Trust-IT	General revision of the document
1.0	29/07/2016	Trust-IT	Release for review by consortium partners (RHUL, KUL)
1.1	30/07/2016	Trust-IT	Addressed comments from Stephanie Mihail (KUL)
1.2	01/08/2016	Trust-IT	Addressed comments from James Alderman (RHUL)
1.3	01/08/2016	Trust-IT	Final round of edits

Reviewers:

Stephanie Mihail (KUL) and James Alderman (RHUL)

2 CLARUS service proposition

The objective of CLARUS is to enhance trust in cloud computing services by developing a secure framework for storing and processing of data outsourced to the cloud. This model change will give control back to data owners and will also encourage cloud services based on standards that can be certified as compliant with security and privacy. Such an approach will increase transparency with regard to data management, privacy and security and thus improve levels of acceptance of cloud technology and create new business opportunities.
.

CLARUS service proposition is a proxy that will be installed in the trusted domain of the end-user to provide a transparent solution to preserve the confidentiality of sensitive data and guarantee data protection before data are outsourced to the cloud for storage and processing. The proxy relies on the assumption that the Cloud Service Provider is *honest but curious*, as such it will perform honestly the operations on the data as requested by the user, but it might also attempt to learn from the data. To address the need for privacy while leveraging the computational and storage capabilities of public Cloud Service Providers (CSPs), CLARUS proposes a set of privacy-preserving techniques (Deliverable D3.1 [5]) leading to the concept of security as a service (Deliverable D4.4 [2]). This service is implemented by the CLARUS proxy, which holds the keys and manages the knowledge to restore outsourced and secured data.

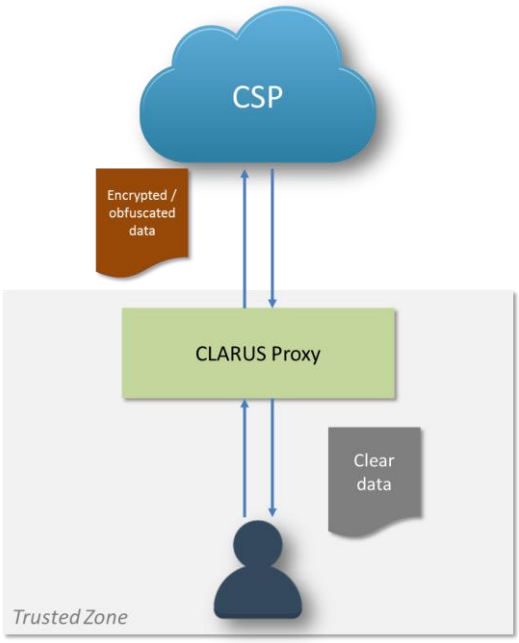

Figure 1 – Simple CLARUS scenario with one CSP and one user [Source D4.4 [2]]

Figure 1 depicts the CLARUS proxy solution. The cloud service provider (CSP) is considered untrusted. The provider may access the stored information for monitoring purposes or simply to provide the required services to its customers, such as processing data or returning results of queries to data stored in a database. This is the main justification of the need of the CLARUS solution. Customers reside in a trusted domain and access the CSP services via the CLARUS proxy, which encrypts or anonymises the data as required before accessing CSP.

The implementation of this scenario considers three different actors: the CLARUS end-users; the security manager that administers and manages the CLARUS proxy to grant access rights to users; and the Cloud Service Provider (CSP).

The CLARUS end-user registers and authenticates to the proxy. CLARUS foresees the use of standard authentication mechanisms implementing Single Sign-on (Deliverable D4.2 [1]) to provide a transparent access to end-users and allow *interoperability* of the CLARUS proxy with legacy authentication mechanisms already available at companies supporting and integrating CLARUS. It is

worth mentioning that multiple users of the same organisation can use the same CLARUS proxy and work on the same data.

The CLARUS proxy holds the encryption keys, information and metadata about the outsourced data in the cloud. The end-user delegates the management of the data to the proxy, including searching, processing, and updating the data stored at the CSP. The access to the CSP is completely transparent for the end-user who does not need to interact with the CSP.

The type of connection with the CSP depends on the type of operations that need to be performed on the cloud. CLARUS envisages the use of secure data transfers and, in some cases, requires the installation of dedicated modules on the CSP to handle a specific request, as is the case for the geo-data use case, see Deliverable D2.1 [6]) for details. The same CSP can be used to handle different types of operations on the data and different levels of protection (encrypted, anonymised, split data, or plaintext) as well as for the meta-data, used to enable search on encrypted data and to reconstruct the original information. The CLARUS proxy can use multiple Cloud Service Providers at the same time, e.g. to split sensitive parts of data across multiple CSPs or simply use multiple CSPs to create backups for reliability purposes.

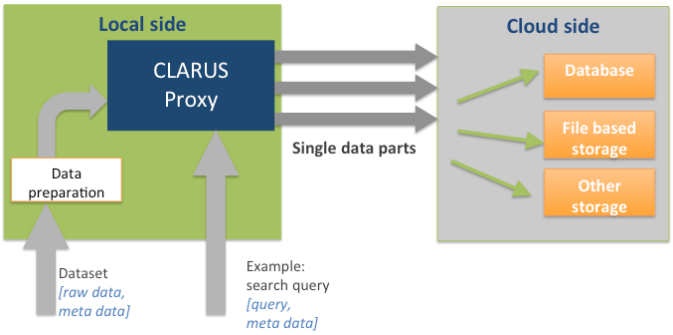

Figure 2 - Data splitting across different cloud services [Source D2.5 [4]]

Deliverable D4.2 analyses the possible scenarios where multiple CLARUS proxies cooperate and share access to data. This scenario requires an inter-proxy communication to be established between the two CLARUS proxies. The solution that CLARUS will implement consists of the Proxy 2 (in Figure 3), i.e., the data owner, which needs to establish a secure connection and data routing service with the Proxy 1. This solution guarantees that the data owner controls the access to the data at the cost of managing potentially resource-demanding requests, thus increasing the utilisation of the proxy.

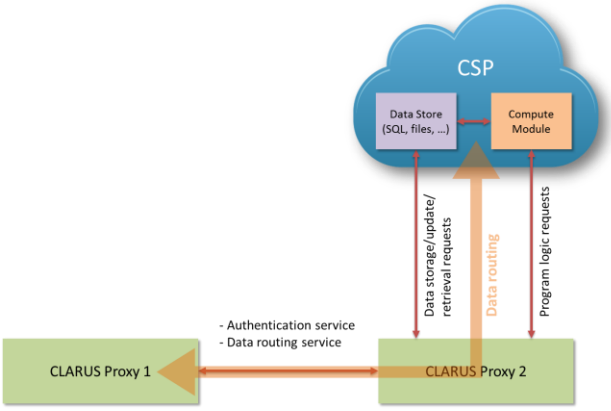

Figure 3 - Inter-proxy communication between multiple CLARUS proxies [Source D4.2 [3]]

The CLARUS service proposition to have a potential wide acceptance on the market calls for the use of standardised solutions for the service interfaces and data format. Moreover, the CLARUS solution should be applicable across different administrative domains, e.g. different CSPs using different types of storage, and serve multiple organisations and their end-users.

CLARUS will be demonstrated in two use cases: the publication of geo-reference data on the Internet and the eHealth scenario, described in Deliverable D2.1 [6].

The first use case addresses the secure publication and processing of geospatial data, that requires limiting access to some of spatial datasets and data services, due to public security or commercial reasons. These functionalities will be provided via a set of security tools working on anonymised and encrypted data that are exploited commercially by private companies, analysts or by other institutions in the public sector. Geo-data information in the environmental domain is characterised by the large size of the data and the rich metadata descriptions (mostly according to the European Directive INSPIRE [7]).

The second case study is related to eHealth and concerns a distributed e-health scenario that requires immediate access to medical data outsourced to cloud providers. The main actor in this use case is the hospital that is responsible to treat the Electronic Medical Records (EMRs) of the patients, which contain information that is highly identifying or confidential. A series of functionalities are needed, like creating, managing and updating medical histories, including results of clinical visits, searching for specific patients/histories and also a shared and cooperative access to these data according to access policies. The CLARUS solution will be applied to obfuscated data to provide security-aware access to functionalities, which should be backed up by a series of auditing tools.

3 Interoperability and standards

Cloud computing is a continuously developing ecosystem with many players bringing to the market new products and solutions that need to coexist with existing systems and be integrated with current solutions to preserve privacy and implement security at all levels. Interoperability is one of the major challenges and is identified as a cornerstone of the Digital Single Market[1] to guarantee that the technologies work reliably together while keeping the integration of new ones a smooth process.

One of the objectives of CLARUS is ***interoperability***, which ensures that the actors and systems providing cloud computing services, implementing the CLARUS solution, and using the proxy can communicate, e.g. are able to authenticate and exchange data, without requiring additional proxies. Moreover, interoperability will reduce the risk of vendor lock-in for customers, which is one of the major obstacles to the adoption of cloud computing along with legal issues related to data protection and security, all aspects addressed by the CLARUS solution.

Open ***standards*** have been recognised to ensure interoperability and facilitate the market growth. Despite the clear advantage of adopting standardised solutions, the main obstacle towards the definition of fully interoperable systems lies in the existence of many organisations and standards that could slow down the convergence process. Standardisation is of major interest for CLARUS, the project being committed to design and develop a standardised solution and to contribute to the European standards landscape with use cases and guidelines to fill in the current gap in standards for security and privacy in cloud services. In the rest of the document we analyse the concepts of interoperability and standards in CLARUS. We revise the content already provided in Deliverable D2.5, which we have updated based on the latest results accordingly.

3.1 Relevance of interoperability in CLARUS

In the context of CLARUS, several aspects related to interoperability are considered so that the CLARUS solution is able to interoperate and work without requiring further development with existing or future systems. Interoperability demands common technical APIs, protocols and data/message format, which can be achieved by following best practices and common guidelines or in its more general form, i.e., by design, adopting open or de-facto standards. Since the beginning of the project, CLARUS follows an ***interoperability by design*** approach by investigating the use of open standards in the architecture design and later in the implementation of the CLARUS components.

The first step is the analysis of the *Application Programming Interfaces (APIs)* of the components and tools developed as part of the CLARUS solution. Interoperability achieved via standardised APIs refers to the cloud computing domain and components of the CLARUS solution that need to interoperate among each other and

[1] ICT Standardisation Priorities for the Digital Single Market, COM(2016) 176.

with the existing cloud infrastructure to facilitate the integration with and the reuse of existing tools, and ease the penetration of the technology to a large set of applications and cloud infrastructures.

Deliverable D5.1 [3] defines the interfaces of the CLARUS platform with external actors. Three different APIs have been defined, each one with a different degree of interoperability:

- CLARUS-CSP interface allows the CLARUS proxy to connect to new cloud services and to integrate some protection primitives in the cloud.
- CLARUS end-user interface allows the end-user to authenticate to the CLARUS proxy and manage his/her sensitive data.
- CLARUS-CLARUS interface allows secure communication between different trusted CLARUS proxies.

CLARUS requires interoperability for the CLARUS-CSP and CLARUS end-user interfaces, as the CLARUS-CLARUS interface will naturally inherit the characteristics of the former, while integrating specific security primitives to ensure that a secure channel is established.

Interoperability will be implemented with a set of open standard protocols and the protocols supported by CLARUS should be *de facto* or popular standards. The first set of protocols that will be natively supported by CLARUS are defined by the two use case demonstrators, thus including the support of OGC standardised web services and consortium (WMS, WPS, WFS) and PostgreSQL and S3 protocols [3]. The result will be a CLARUS proxy transparent for the end-user, thus not implying modification of the client application code nor of the CSP services.

The second step is to ensure wide consensus about the *security solutions* that will be implemented to secure the communications, authenticate the users, and provide access to CLARUS cloud services. The intent is to provide compatibility with well-known protocols and best practices to ensure that the CLARUS solution can leverage existing authentication frameworks to facilitate the authentication of the users while, at the same time, ensuring that the secure exchange of information between users, services, and components is done in a standardised way. Interoperability for security is needed to enable cooperative access to data from different CLARUS platforms, and according to policies set by the data owner.

Finally, the *format of data* processed by web services. The CLARUS proxy operates on data applied to different transformation modes. Anonymisation and encryption are performed directly within the CLARUS proxy and do not require any specific add-on installed on the CSP or knowledge of the data type. Splitting, homomorphic encryption, and searchable encryption require the deployment of specific add-ons on the cloud and might depend on the nature of data [3]. The data and metadata stored and processed by CLARUS need to follow predetermined standards to allow the application of the CLARUS solution to a large set of applications. In the context of the two CLARUS use cases, the data format must follow well-defined standards: the Open Geospatial Consortium standards for the publication of geo-referenced data on the Internet, and the Health Level-7 standard for the transfer and format of healthcare information. Other standards can be considered for data formats. In order to support specific data types, a dedicated specific plug-in can be built to extend the CLARUS proxy.

3.2 Standardisation in CLARUS

Standardisation has been recognised as the key to supporting innovation by addressing interoperability issues and overcoming potential barriers due to the need to simultaneously leverage different solutions.. The technological aspects of cloud and privacy-preserving solutions are diverse, ranging from service management to security including authentication and data protection. The ecosystem is fast moving and "specific gaps still exist" for online security, as it has been recognised in the Digital Single Market strategy[2].

The objective of CLARUS is to implement standardised solutions supported by a wide range of Cloud Service Providers (CSPs) and end-users, thereby ensuring interoperability in collaborative, standardised and transparent cloud environments. By means of standardisation, the function calls implemented in the interfaces can be made homogeneous for cloud providers that provide similar services (e.g. data storage), so that data interoperability can be achieved among otherwise heterogeneous cloud providers. On the other hand, standards will allow the support of data splitting (for security enhancement and to meet privacy constraints), merging and replication (for improved data integrity in case of potential failures on the part of the CSPs), whereby the integration of the CLARUS solution into existing cloud infrastructure facilitates the adoption of already available distributed backup solutions.

The use of standardised solutions, well recognised and supported by a large community, brings several benefits to CLARUS, such as the possibility of implementing more robust security mechanisms and improving reliability and dependability, while increasing transparency and trust in cloud services.

Deliverable D2.5 [4] reviewed the major standards of interest for CLARUS. In the rest of the section, we revise the list and identify those that are part of the CLARUS roadmap to foster a standardisation culture in cloud privacy-preserving solutions.

The CLARUS proxy solution will implement specific security functionalities offered as a set of SaaS services primarily and PaaS modules that need to be implemented as add-ons to allow specific operations on the data (see Deliverable 4.2 [1] and Deliverable D5.1 [3]). The standardisation effort for model or applications at the SaaS level is still in its infancy due to the complexity of the large variety of software service solutions. In this deliverable, we first review the standards for storage, then we consider those for security and data formats that can be used to achieve a certain degree of interoperability for software applications.

3.2.1 Storage

CLARUS uses the cloud to store data either in encrypted or anonymised form. The proxy will implement and support recognised international de facto standards that are widely used for commercial and open source applications. This ensures higher penetration of the CLARUS proxy solution to the market.

[2] A Digital Single Market Strategy for Europe, COM(2015) 192.

- Amazon S3[3] provides storage capabilities thanks to a set of web services interfaces. It includes web hosting, image hosting and storage for backup systems. In CLARUS, S3 will be used to support the Geo-reference data application.
- PostgreSQL is a free and open source software that implements the ISO/IEC 9075 standard for the SQL database query language [8]. It allows storage and retrieval of data. In CLARUS, PostgreSQL is used for the eHealth and Geo-reference data applications.
- A standard under consideration is the Cloud Data Management Interface (CDMI) proposed by SNIA [9], which has the capability to discover storage elements of the cloud and manage metadata, including user accounts and credentials pertaining to the cloud storage.

Specific standards are considered for the storage of geospatial data (either in spatial databases or in GIS files). For this purpose, the following standards are considered:

- The OGC Simple Features Access (SFA) [10] is a standard that describes the common architecture for simple feature geometry (i.e. two-dimensional geographical data like points, lines, polygons, multi-lines) and defines a standard SQL schema that supports storage, access and update of these data types. The PostGIS extension to PostgreSQL is an example of open source software that follows the Simple Features for SQL specification.
- The ESRI Shapefile [11] format is a de facto standard for storing geospatial vector data in files. Developed originally by the Environmental Systems Research Institute (ESRI), the format gained prominence through widespread use in the field of Geospatial Information Systems. The shapefile format makes it possible to spatially describe vector features (points, lines, and polygons), representing for example boreholes, transportation networks and buildings. Each item can have descriptive attributes, such as a name or a scientific measurement.

3.2.2 Web services

CLARUS implements a set of web services for the messaging and metadata specifications. In CLARUS, these standards will be relevant for specific use cases that require the publication of services. The Simple Object Access protocol (SOAP), specified by W3C, is a standard for the definition of the XML-based format of information exchanged in the implementation of web services. It is an extensible protocol (e.g. WS-Security for security specifications) and uses HTTP as a transport protocol. The Web Services Description Language (WSDL) [12] is a W3C specification that describes the functionalities of the web service and defines the message formats required to access it. Another relevant standard is JavaScript Object Notation (JSON) [13], which uses human-readable text to transmit data objects between a server and a web application. JSON is a widely used standard for the development of web services.

[3] Amazon S3. http://aws.amazon.com/s3/ [Online]

3.2.3 Security and privacy

CLARUS looks with interest to the security best practises related to procedures and processes related to information security management standardised by the ISO/IEC 270x family: ISO/IEC 27001 [14], which defines the requirements for the design, maintenance, and implementation of an information security system and identifies the interested parties and their needs, the security risks and actions; ISO/IEC 27017 - ITU-T X.1631 [15] defines security controls to maintain and implement the security system for cloud computing specifically by mapping the ISO/IEC 27002 to cloud services; ISO/IEC 27018 [16] deals with the protection of Personally Identifiable Information (PII) in public clouds, which act as processors of personal data. These documents have been considered for the requirements mapping process described in Deliverable D2.5.

Specific security standards have been analysed in Deliverable D2.5 and there is a plan to use them for the implementation of identity management in CLARUS, including authentication and authorisation. Specifically, CLARUS will support those mechanisms that allow the separation of roles between data owners and data consumers and provide a fine-grained access control when using cloud services. CLARUS will support Single Sign-On (SSO) to reduce the burden of multiple authentication steps and facilitate the management of users across trusted domains. Indeed, users should be able to access multiple services without being prompted for additional authentication and reuse the organisation authorisation framework without the need to deploy new ones. SSO requires trust relationships between service providers as the authentication token, issued by a provider, need to be trusted across multiple systems and domains.

CLARUS considers the following set of de-facto standards to provide SSO capabilities, as defined in Deliverable D4.2 [1] and D5.1 [3]. The *Lightweight Directory Access Protocol (LDAP)* [17] provides authentication and authorisation services. *Security Authorization Markup Language (SAML)* [18] is a XML-based standard for exchanging authentication and authorisation information between identity provider and service provider. OAuth2 [19] enables the delegation of rights and permissions by creating dynamic credentials to provide a trustworthy communicating infrastructure. For authorisation, the relevant standard is the eXtensible Access Control Markup Language (XACML) [20] used to express and evaluate authorisation policies to protect resources in a distributed computing environment.

3.2.4 Data format

The application of CLARUS to a number of different application scenarios requires the support of standard data formats. The two use cases of CLARUS are the Publication of geo-reference data and the eHealth scenario.

The Open Geospatial Consortium (OGC) is a worldwide consensus of organisations collaborating on the development and implementation of open standards for geospatial content and services, collectively referred to as OGC Web Services (OWS).

- OGC Web Map Service (WMS) is a standard communication protocol for serving maps on the web from several georeferenced data sources. WMS implementation involves the setup of a WMS server (to access, read and draw the data), and a WMS client (to query the server using specific request

operations, e.g. GetCapabilities for retrieving information about the map layers being exposed, GetMap for retrieving a map image of the data).

- OGC Web Feature Service (WFS) is a standard communication protocol ensuring interoperability for exchanging geographical features across the web. Geographical features are vector data such as points, lines and polygons. WFS provides interfaces for manipulating features via different operations (e.g. GetCapabilities for serving the supported operations, GetFeature for serving geometries or attributes under various formats like GML or JSON, Transaction for creating, modify and deleting features published by the service).
- OGC Web Processing Service (WPS) is an interface standard for invoking geospatial services on the Internet, providing rules for the definition of inputs/outputs (i.e. requests/responses). WPS defines how a client can request the execution of a process and how the output from the process is handled. WPS makes it possible to execute a process thanks to different operations (e.g. GetCapabilities for information about the service, DescribeProcess for process description including inputs and outputs, Execute for the output of the process).
- OGC Catalogue Service for the Web (CSW) is a standard for interacting with one or many catalogue(s) of geospatial records on the web. CSW makes it possible to publish and search collections of descriptive information (metadata) for data, services, and related information objects. Metadata in catalogues can be queried thanks to different CSW operations (e.g. GetCapabilities for retrieving service metadata, DescribeRecord for discovering elements of the information, GetRecords for searching for records).

The ISO/TC 215 technical committee and the Health Level Seven International define a set of guidelines and international standards for the exchange, integration, sharing and retrieval of clinical and administrative health information. CLARUS has analysed the standards and considered specific best practices for defining the privacy-preserving mechanisms that will be applied to medical data. More information about the relevant standards and best practices for the eHealth sector are available in Deliverable D2.5 [4].

3.2.5 Analysis of the CLARUS design solution

This section provides an analysis of the CLARUS system architecture proposed in Deliverable D4.2 [1] with a specific focus on standards and interoperability aspects to enable an easy integration and use of the CLARUS solution. Section 3.1 already discusses the concept of interoperability and maps the actions taken in CLARUS to address interoperability issues to ensure that the CLARUS proxy will be able to interoperate with existing services. Section 3.2 revises the standards in the domain relevant for the development of CLARUS and proposes the final list that is considered for the implementation of the proxy.

Standardisation aspects are rather important in the multi-proxy architecture design in order to ensure that interoperability can be achieved among otherwise heterogeneous cloud providers and organisations. In the context of CLARUS, several aspects related to interoperability are considered to ensure that the CLARUS proxy could interoperate without requiring further development with existing and future systems. In this section, we briefly summarise the design choices and solutions to ensure interoperability for security, data format and

cloud storage solutions, including some insights about the Application Programming Interfaces (APIs), detailed in Deliverable D5.1 [3] that will be made available to programmers for a seamless development of end-user cloud based applications.

Section 3.2.3 reviews the standards that will be used to support external authentication and authorisation mechanisms. Specifically, the following ones are addressed in the design of the user management module to ensure clear separation of roles between data owners and data consumers with fine grained access control. Single sign-on (SSO) will enable the federation of identities and will reduce the authentication burden of the users of the CLARUS proxy and will use the authentication services already existing within the company. Several open and de-facto standards exist to implement SSO capabilities, such as:

- Lightweight Directory Access Protocol (LDAP) as authentication and authorisation service;
- SAML for exchanging authentication and authorisation information between the identity provider of the company and the CLARUS proxy;
- OpenID for the authentication of the users relying on the company verified identities;
- OAuth2 for authorisation by enabling the delegation of rights and permissions to the employee of the company using the CLARUS proxy.

CLARUS is specifically designed to operate over data by means of a set of identified privacy-preserving mechanisms. As such, the proxy integrates a set of specific “Data Type” plug-ins for each supported protocol and data format, so that parsed data can be forwarded in a homogeneous format to the data operation modules (see Deliverable D4.2 [1]). The operations are supported by the USER-CLARUS protocol module. The already supported open and de-facto protocols are PostgreSQL, Amazon S3, and PostGIS, shapefile (a standard format for storing vector data), as presented in Section 3.2.1.

The Data format relevant standards have been analysed in Section 3.2.4 and includes those from the Open Geospatial Consortium. The plugin approach adopted in CLARUS opens the possibility to support a wide range of data types, either structured (e.g., relational database) or unstructured (e.g., binary file, image, text file). Finally, CLARUS will implement Web services and, JSON and XML data type protocols, as discussed in Section 3.2.2.

Interoperability with cloud service providers will be implemented by the CLARUS-CSP Protocol module that will transparently intercept and process any request of the CLARUS proxy and enable support for the same data types and protocols of the USER-CLARUS protocol module. The installation of few add-ons will be required on the CSP to ensure that the protocols will be correctly implemented and operations on the data can be performed. The details of the two protocol modules are provided in Deliverable D5.1 [3].

4 Relevance for the Digital Single Market

The Digital Single Market (DSM) in Europe is an unprecedented opportunity to create one of the biggest digital marketplaces in the world with cloud computing being one of the main enablers for other technologies, such as the Internet of Things and Big Data. Cloud computing has now gained its momentum leveraging the pay-as-you-go concept and the idea of using commodity public cloud providers based on customers needs without requiring an in-house dedicated infrastructure, thus reducing the entry to large processing and storage capabilities in any sector.

However, several barriers still remain to make the consumers really trust the cloud services; this is particularly true for organisations and public organisations as gatekeepers of large amounts of private data and companies that need to protect their business-critical data. Trust and confidence are central to the Digital Single Market to reap the benefits of the digital economy and standardisation has a key role to play in meeting security and privacy requirements.

A recent communication[4] has identified standardisation as one of the priorities for the Digital Single Market, and cloud computing and cyber security as two of the essential technology building blocks of the DSM. Moreover, the communication identifies the need of a convergence to common open standards to facilitate the access and usage of innovative services.

Standardisation and interoperability are therefore crucial to leverage existing technology and ensure to have common agreements on the most important technical and service requirements, while preventing vendor lock-in. CLARUS contributes to the goals of the Digital Single Market in several key ways:

- **Data protection.** Reinforcing trust and security in digital services, especially the handling of personal data.
- **Interoperability and Standardisation.** Defining priorities and interoperability in areas critical to European market and creating a level playing field across all sectors.

CLARUS has followed a pragmatic approach to ensuring the integration of relevant standards within the implementation of the proxy solution and demonstrates, by means of the two use cases, the importance of standards for data formats to ensure that other sectors will be able to leverage cloud computing. The decision to adopt a privacy-by-design approach at the early stage of the project has proven to be valuable to address security and privacy requirements and integrate them at the inception of the design of the architectural system. Trust among industrial and institutional actors, some of the CLARUS stakeholders, will play an important role, since it has been recognised as one of the barriers to ensure close synergies and cooperation at all levels. Regulations play a major role to address this barrier by ensuring that industrial and innovative solutions will abide to known best practices and standards. CLARUS has considered known best practices in

[4] ICT Standardisation Priorities for the Digital Single Market. COM(2016) 176 final.

security and privacy and derived relevant requirements mapped with the ones identified for the design of the CLARUS architecture, as defined in Deliverable D2.5 [4].

5 Conclusion

This deliverable analyses the CLARUS value proposition and provides the main results concerning standardisation and interoperability issues highlighting how they are addressed in the design of the CLARUS architecture.

A thorough review of the current standards landscape for cloud computing, security, and data format in light of the design decisions has been carried out. The objective of this document is to assess how CLARUS aligned with the standardisation roadmap built in Deliverable D2.5. The analysis has been extended to the preliminary decisions related to the implementation of the Application Programming Interfaces (APIs) of the components and tools, the protocols for supporting security (authentication and authorisation), and the format of data.

As part of the continuous monitoring of the standardisation landscape, CLARUS has created a catalogue of standards that can be consulted to obtain quick information about relevant standards, including those presented in Section 3.2. The goal is to foster the usage of standards and best practices.

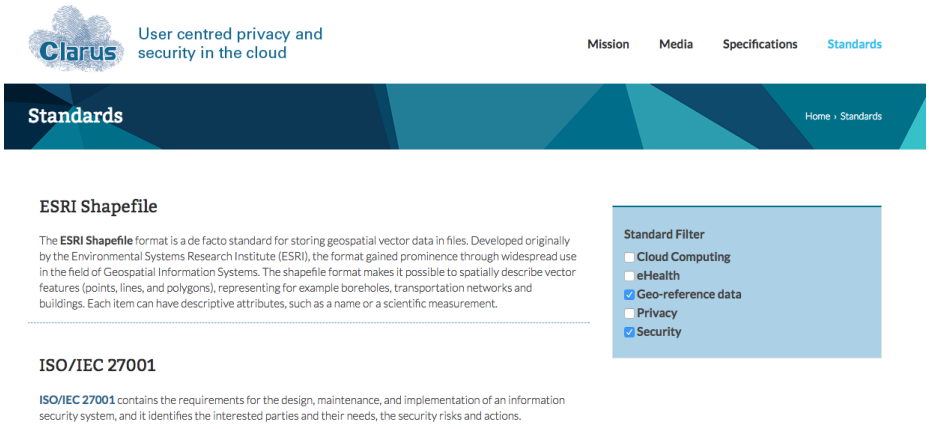

Figure 4 - CLARUS catalogue of standards

Figure 4 shows the online version of the catalogue that has been implemented and made available on the website. This action is aligned with the activities of the CLOUDWatch2 CSA project, which is creating a standards hub on cloud, security, privacy and risk management as a direct response to the EC Communication on ICT standardisation in April 2016 and which leverages contributions to standards by partners within the consortium. Alignment with the CW2 Catalogue of Standards allows easy comparison with the most relevant standards to address specific cloud challenges across different peer projects and can help other projects to identify the relevant standards to consider while designing and implementing their solution.

6 Bibliography

[1] Thierry Chevallier, Monir Azraoui, Kaoutar Elkhiyaoui, Melek Önen, Wissam Mallouli, Antonio M. Ortiz, Stefan Janacek, Sven Rosinger, James Alderman, Romain Ferrari, Roberto Cascella, Alberto Blanco, Oriol Farràs, Jordi Ribes, David Sánchez Frédéric Brouillé, "D4.2 Architecture V2," CLARUS project, Deliverable 2016.

[2] Antonio M. Ortiz, Sven Rosinger Stefan Janacek, "D4.4 Security as a service for CLARUS," CLARUS project, Deliverable 2016.

[3] Frédéric Brouillé et al., "D5.1 The CLARUS Interface," CLARUS project, Deliverable 2016.

[4] Roberto Cascella, "D2.5 Standardisation requirements," CLARUS project, Deliverable 2015.

[5] James Alderman, "D3.1 Characterization of enabling technologies ," CLARUS project, Deliverable 2015.

[6] AKKA and FCRB teams, "D2.1 Definition of Application Cases," Clarus project, Deliverable 2015.

[7] (2007) Directive 2007/2/EC of The European Parliament and of the Council. [Online]. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007L0002

[8] ISO/IEC, "ISO/IEC 9075 - Information technology -- Database languages -- SQL -- Part 11: Information and Definition Schemas (SQL/Schemata)," Standard 2011.

[9] SNIA, "Cloud Data Management Interface (CDMI) v1.1.1," Standard 2015.

[10] OGC Open Geospatial Consortium. OGC Simple Features Access (SFA) specifications. [Online]. http://www.opengeospatial.org/standards/sfa

[11] Environmental Systems Research Institute, "ESRI Shapefile Technical Description," White Paper 1998.

[12] W3C, "Web Services Description Language (WSDL) 2.0," Standard 2007.

[13] JavaScript Open Notation (JSON). [Online]. http://json.org

[14] ISO/IEC, "ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements," Standard 2013.

[15] ISO/IEC / ITU-T, "ISO/IEC 27017 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," Standard 2015.

[16] ISO/IEC, "ISO/IEC 27018 - Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors," Standard 2014.

[17] IETF, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," Standard RFC 4510, 2006.

[18] OASIS, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," Standard 2005.

[19] IETF, "The OAuth 2.0 Authorization Framework," Standard RFC 6749, 2012.

[20] OASIS, "eXtensible Access Control Markup Language (XACML) v3.0," Standard 2013.