CLOUD
ACCOUNTABILITY
PROJECT

D:C-3.1 Requirements for cloud interoperability

Deliverable Number: D33.1

Work Package: WP 33

Version: Final

Deliverable Lead Organisation: CSA

Dissemination Level: PU

Contractual Date of Delivery (release): 30th September, 2013

Date of Delivery: 5th November, 2013

Editor

Alain Pannetrat (CSA)

Contributors

Vasilis Tountopoulos (ATC), Daniele Catteddu (CSA)

SEVENTH FRAMEWORK
PROGRAMME

Executive Summary

This document proposes an analysis of logical interoperability requirements for accountability in the cloud.

Here, the terms “logical interoperability requirements” encompass the high-level requirements that are created by the interaction of accountability actors, independently of the actual underlying technologies involved. By opposition, “technical interoperability requirements” encompass the interoperability requirements that stem from the interactions of tools and components, supported by specific technologies.

To conduct our analysis of logical interoperability requirements, we first identify the 5 main actors relevant to the interoperability of an accountability framework: Cloud Customers, Cloud Providers, Cloud Brokers, Auditors (including Regulators) and Data Subjects.

Next, we identify 4 generic interactions paths between pairs of actors that are needed to support the accountability attributes of the A4CLOUD Conceptual Framework [3]. These interaction paths are identified as:

- **Agreement:** covers all interactions that lead to one actor taking responsibility for the handling of certain data provided by another party according to a certain policy (including a potential negotiation phase).
- **Reporting** covers all interactions related to the reporting by an actor about current data handling practices.
- **Demonstration** covers all interactions that lead to one actor demonstrating the correct implementation of some data handling policies.
- **Remediation** covers all interactions that lead one actor to seek and receive remediation for failures to follow data handling policies.

On this foundation, we then conducted a systematic analysis of all interactions between all pairs of actors in order to obtain a set of 31 logical interoperability requirements. These requirements serve two main purposes in the A4CLOUD project:

1) Provide an interoperability checklist to verify if the tools created by the project cover all the necessary interactions between actors in an accountability framework, allowing to detect, justify or correct potential gaps.
2) Contribute to the framework that will be used both for the description of the high-level reference architecture (D:D-2.2) and for the analysis of technical interoperability requirements (D:C-3.3).

Finally, as a validation exercise, we crosschecked these logical interoperability requirements against the general requirements that come from the A4CLOUD use cases (D:B-3.1) in order to show that none of these general requirements imply an interoperability requirement that is missing from our list of logical requirements.

We conclude our work by highlighting a few key observations derived from our analysis, notably that shared privacy and security attribute semantics in the accountability chain is a pre-condition for the construction of any interoperable accountability framework.

Table of Contents

1 Introduction

1.1 Scope of the document

Interoperability describes the ability of diverse systems and organizations to exchange and make use of information [1]. Interoperability is achieved through the definition of standards (either formal or *de facto*).

In the context of accountability, this document examines the logical interoperability requirements needed to support accountability attributes in the cloud ecosystem as defined in the A4CLOUD conceptual framework [3]. The scope of this work is restricted to logical requirements for interoperability as opposed to technical requirements, since it is mainly derived from an analysis of the conceptual framework of A4CLOUD, and represents the first results of Task T:C-3.2, which will continue in the next few months (until mid 2014). Technical requirements for interoperability will later be derived from work done in the Architecture work package (D-2), once basic architecture components are defined.

The logical interoperability requirements obtained through this work aim to serve two purposes:

1) Provide a checklist to verify the coverage of the tools produced by the A4CLOUD project, notably to:
    a. Verify if all actors and all accountability interactions are covered.
    b. Detail potential gaps and, when relevant, justify why we accept them.
    c. Review our toolset to check if all accountability requirements can be transmitted to all intermediaries in the cloud supply chain.
2) Contribute our actor-based approach to the framework that will be used both for the description of the high-level reference architecture (D:D-2.2) and for the analysis of technical interoperability requirements (D:C-3.3).

To conduct our analysis, we use and extend some of the concepts already developed in the A4CLOUD conceptual framework by adopting the following approach:

- We first recall the relevant actors in the cloud ecosystem, following the NIST model [6] with some minor extensions.
- We highlight existing interaction paths between actors.
- For each interaction path we define 4 families of accountability interactions: “agreement”, “reporting”, “demonstration” and “remediation”, each used to express a set of one or more accountability attributes between actors.
- Then for each one of these 4 interactions, we examine:
    - If they exist, since not all types of interactions are relevant between all actors;
    - What interoperability requirements they underpin.

When necessary, we will distinguish two domains of application for accountability: Information Security and Data Protection, thereby following the approach taken in the Conceptual Framework.

For the sake of clarity, we highlight that general cloud interoperability issues are out of scope in this work: we do not examine cloud interoperability issues related to portability or interactions between different layers of the cloud stack, such as provided by standards such as XML, JSON, OCCI, Amazon EC2, WDSL, etc. A general overview of cloud standards is provided by work conducted in A4Cloud Task T:A-5.

1.2 Position within the A4Cloud project

This document examines the logical interoperability requirements needed to support the 7 core accountability attributes defined in the A4CLOUD project [3] and will be followed by two others:

- A white paper at M24, which will extend this work from logical to technical requirements for accountability, to be notably derived from the maturing of the A4CLOUD architecture (T:D-2).
- A roadmap for a framework for cloud interoperability standardization at M33, which will be derived from the technical requirements as well as the lessons learned through the deployment of the A4CLOUD framework.

1.3 Outline of the document

This document is divided in 3 main parts.

Section 2 details the accountability analysis framework we have adopted in this work, based on attributes, domains, actors, interactions paths and families of logical interactions.

Section 3 applies the previously defined framework to identify a set of 31 logical requirements for interoperability supporting accountability.

Section 4 goes through all the general accountability requirements identified in the use-case scenarios of the A4Cloud project [5], and maps them to the logical interoperability requirements identified in the previous section. This mapping allows us to gain additional assurance on the coverage and relevance of the logical interoperability requirements we have identified.

2 Interoperability analysis framework

2.1 Attributes

In this document, we refer to the Accountability Attributes as initially defined in the A4Cloud Conceptual framework [3], with additional modifications and clarifications recently provided internally in the Project as of October 2013. These Attributes are provided here with their short definition:

- **Responsibility:** The state of being assigned to take action to ensure conformity to a particular set of policies or rules
- **Observability:** A property of an object, process or system, which describes how well the internal actions of the system can be described by observing the external outputs of the system
- **Verifiability:** A property of an object, process or system that its behaviour can be verified against a set of requirements
- **Attributability:** A property of an observation that discloses or can be assigned to actions of a particular actor (or system element)
- **Transparency:** The property of an accountable system that it is capable of "giving account" of, or providing visibility of, how it conforms to its governing rules and commitments
- **Liability:** The state of being liable (legally responsible)
- **Remediability:** The property of a system of being able to correct faults or deficiencies in the implementation of a particular set of policies and rules.

2.2 Domains

Recalling the scope of accountability that is established in the A4Cloud Conceptual Framework [3], our analysis will encompass interoperability issues in two application domains for accountability:

Information Security: covers the handling of business (non personal) data in the cloud, and is mainly concerned with:

- Confidentiality, including the control of disclosure to internal personnel and external third parties;
- Integrity and authenticity;
- Availability;
- Non-repudiation;

Data protection: covers the handling of personal data in the cloud. It has the same base concerns as information security, but notably adds the following additional items (see directive 95/46/EC [7]) :

- Legal basis (contract, consent, legitimate interest, etc.);
- Purpose specification and limitation;
- Personal right to access, modify and delete data (where applicable);
- Information to persons;
- Data retention and deletion quality;

- Data transfer restrictions (data location).

Note that in addition, both the information security domain and the data protection domain require a set of supporting processes, such as monitoring, third-party audits, data-breach notifications, law enforcement access procedures and remediation procedures, as described for example in Privacy Level Agreements [17].

2.3 Actors

2.3.1 The extended NIST actor model

This work examines interactions between the following 5 cloud actors:

- Cloud auditor, with the inclusion of regulators.
- Cloud customer (or consumer[1]).
- Cloud provider.
- Data subject.
- Cloud broker.

These actors are defined in the NIST reference architecture [6] and in the A4CLOUD Conceptual framework [3], with the addition of the "Data Subject" as a distinct actor for the data protection domain, but omitting "Cloud Carrier" which is defined in the NIST architecture but plays no role for interoperability at the accountability level. We also put less emphasis on the Cloud Broker since his role is often more limited than other actors in terms of accountability (see 3.3 for details).

We highlight that there are at least three reasons to add the "Data subject" as a distinct actor in the context of interoperability requirement for accountability in the data protection domain:

- In many cases the "Data subject" is not a *cloud customer*. The NIST defines a cloud customer (or consumer) as "a person or organization that maintains a business relationship with, and uses service from, Cloud Providers". In many cases this definition does not apply to "Data Subjects":
    - The data subject may not have a business relationship with a cloud provider but rather with a cloud customer.
    - The data subject may not have any business relationship with a cloud provider or customer, yet a cloud provider or customer will collect data from him on another basis than a business relationship.
- Data subjects enjoy particular rights that are distinct from other actors (right to access data, right to modify, right to be informed, etc.), which may be the source of specific interoperability requirements.
- The data subject does not necessarily have the same resources as other actors to evaluate risks, policies and compliance, and may require simplified tools.

2.3.2 Why not a controller/processor actor model

The concepts of Data Controllers and Data Processors are central to EU data protection [7]. A data controller is the entity, which (alone or jointly with others) "*determines the purposes and means of the processing of personal data*", while the processor is an entity that "*processes personal data on behalf of the data controller"*, and that must "*act only on instructions from the controller*". When the means and the purpose of a data processing are determined jointly by several entities they are sometimes referred as

[1] Following the glossary conventions adopted in the A4Cloud project [29] we use the expression "Cloud Customer" instead of the synonymous "Cloud Consumer".

"joint-controllers". We note that in practice, separating actors between controllers, joint-controllers and processors sometimes proves to be a complex task [27].

As an alternative to the previously proposed extended NIST actor model, we could have therefore considered "Data Controllers", "Joint-controllers" and "Data Processors" as actors instead of "Cloud Customers" and "Cloud Providers", by using data protection regulations as a framework.

While this actor model might be suited to describe general accountability requirements in the data protection domain, we believe it has some drawbacks for an analysis of logical interoperability requirements.

First, while a legal analysis might determine responsibilities by establishing which entity is a controller and which entity is a processor, this does not necessarily translate into interoperability requirements. For example: a data controller might have the legal responsibility to inform users about the processing of their data, yet it might effectively delegate the practical implementation of this responsibility to a processor, which would then carry the interoperability requirements. From the point of view of interoperability, both controllers and processors are just as likely to implements many interoperability requirements. We also note that the current proposed draft of the future data protection regulation [23] increases the obligations that apply to data processors, further reducing the distinction between processors and controllers in terms of interoperability requirements, since both types of actors may need to implement similar interoperability features on a case-by-case basis.

Secondly, an actor model based on a data protection centric approach cannot by nature be directly used in the information security domain we seek to cover as well, and would require in effect two models, one for each domain. One of the benefits of our extended NIST model is that it can cover both domains as we describe next.

2.3.3 Overview of interactions between actors

In the information security domain, we identify the following 3 types of interaction paths between actors from the perspective of accountability:

1) **Cloud Provider ⇔ Cloud Customer:** The cloud provider and the cloud customer will interact for the purpose of defining and implementing data stewardship requirements, as well as for the purpose of remediation when necessary.
2) **(Cloud Provider or Cloud Customer) ⇔ Auditor/Regulator:** The cloud customer or provider may have to demonstrate compliance to an auditor or regulator. A regulator may additionally request remediation actions.
3) **Cloud Customer ⇔ Cloud Broker ⇔ Cloud Provider:** A Cloud Broker may take over a subset of the accountability interactions between a Cloud Customer and Cloud Provider, such as for example the negotiation of data stewardship responsibilities.

In a cloud supply chain, an entity may act both as a cloud provider and cloud customer, which means that several interaction paths of type 1 (or 3) may be repeated for each link in the supply chain.

While Cloud Providers and Cloud Customers may have different accountability requirements and expectations, we have not identified any differences in terms of logical interoperability requirements: depending on the scenarios, both actors may need to interact with auditors and regulators. Therefore, we have chosen to group together Cloud Providers and Cloud Customer in interaction path (2).

These interactions will be analyzed more in detail in section 3, following the approach we define below.

The following figure summarizes these interaction paths in the information security domain, each numbered form 1 to 3:

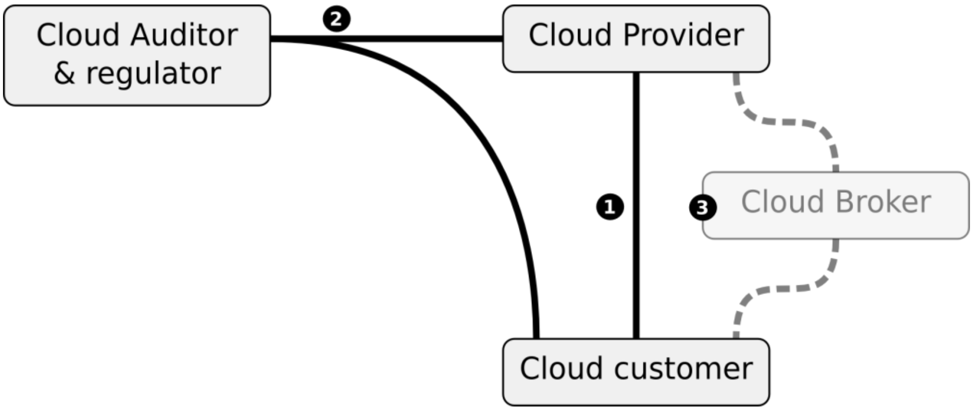

Figure 1. Interaction Paths in the Information Security Domain

Moving to the data protection domain, we augment the previous set of interaction paths and identify the following 2 additional types of interaction paths between actors from the perspective of accountability:

4) **Data Subject ⬄ (Cloud Provider or Cloud Customer):** Data Subjects may express choices regarding their data handling to the Cloud Provider or Customer, verify claims, exercise their rights and seek remediation.

5) **Data Subject ⬄ Auditor/Regulator:** Data Subjects may complain to the regulator, seeking remediation, or ask an auditor/regulator for verifications.

The simplification we made previously for interaction path (2) still holds in the data protection domain. We extend this simplification to the relationship between Data Subjects and cloud entities by grouping together Cloud Providers and Cloud Customers in their relationship with Data Subjects. Indeed, interoperability between Data Subjects and Cloud Entities is not driven by their role as providers or customers but by their legal status as data controllers or processors.

Again, these interactions will be analyzed in more detail in section 3.

Adding the data subject and moving to the data protection domain, we can augment the previous figure with a total of 5 interaction paths as follows:

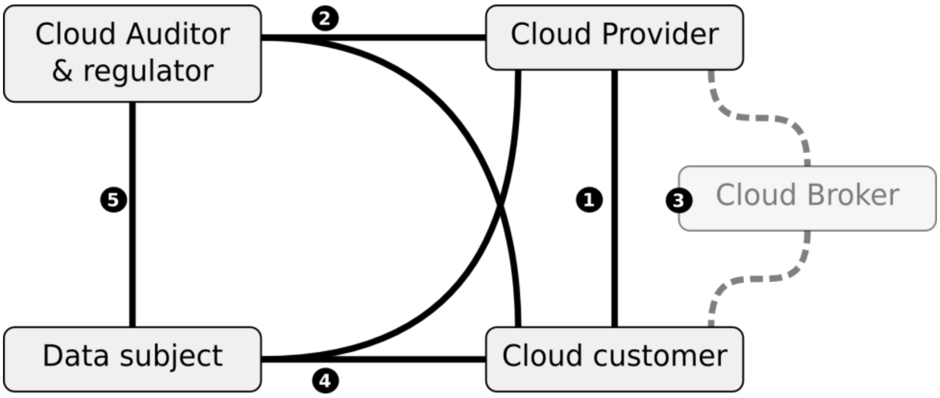

Figure 2. Interactions Paths in the Data Protection domain

In practice, we can identify interactions between all actors, with the exception of data subjects or auditors/regulators with cloud brokers.

Along each interaction path, we define 4 logical families of interactions between two actors:

- **Agreement**: [actor B] takes responsibility for processing of data provided by [actor A] according to a data handling policy.
- **Reporting**: [actor B] informs [actor A] about status of data handling policies.
- **Demonstration**: [actor B] demonstrates to [actor A] compliance with data handling policy.
- **Remediation**: [Actor A] seeks (and receives) remediation from [actor B] for failure to implement data policy.

The 4 families of interactions are used to cover the 7 core accountability attributes highlighted in the Conceptual framework, as follows:

Agreement covers all interactions that lead to one actor taking responsibility for the handling of certain data provided by another party according to a certain policy. These interactions may include a negotiation phase. A policy may express requirements that apply to all 7 core accountability attributes, and contributes to the implementation of the attribute of RESPONSIBILITY and LIABILITY. Agreement interactions requires both:

- Means to express data policies
- Means to describe implementation of policies, potentially through a negotiation.

Reporting covers all interactions related to the reporting by an actor about current data handling practices (e.g. reporting incidents on customer data) and policies. This type of interaction mainly supports the implementation of the accountability attribute of TRANSPARENCY and OBSERVABILITY.

Demonstration covers all interactions that lead to one actor demonstrating the correct implementation of some data handling policies. This includes external verifications by auditors or cryptographic proofs of protocol executions for example. This type of interaction mainly supports the implementation of the accountability attributes of VERIFIABILITY and ATTRIBUTABILITY.

We emphasize that *Demonstration* is different from *Reporting* in that it implies some form of proof or provision of evidence.

Remediation covers all interactions that lead one actor to seek and receive remediation for failures to follow data handling policies. This type of interaction mainly supports the implementation of the accountability attribute of REMEDIABILITY.

We note that *Reporting*, *Demonstration* and *Remediation* are interactions that contribute to the implementation of requirements related to the core accountability attributes. By contrast, *Agreement* is a type of interaction that is used both for the expression of requirements that apply to the core accountability attributes, and the implementation of taking responsibility to implement the core attributes in accordance with policies, regulations and ethics, and defining corresponding liabilities.

Not all interactions are relevant between all actors, as we detail in section 3.

In this document we do not address interactions that lead to the definition of responsibility and liability of auditors, in the case of third party audits of the cloud customer's compliance. We consider these interactions out of scope, since the accountability remains on the shoulders of the cloud customer or cloud provider. For similar reasons, we do not address interaction by cloud providers/customers with insurers, and other risk transfer entities.

2.3.4 Common core requirements

A logical interoperability requirement that emerges naturally by listing all interactions in an accountability framework is the ability of parties to share a common understanding of security and privacy policy **semantics** and their associated **metrics**, be it for the purpose of agreement, reporting, demonstration or remediation. Unfortunately, this common ground for semantics and metrics hardly exists today [9]. For example, all major cloud providers use different semantics and metrics for availability [8], which suggests that building interoperable policy negotiation protocols even for such a common attribute as "availability" would prove challenging. The same can be said if two interoperating actors have different interpretations of properties and concepts behind keywords such as "consent", "confidentiality level" or "user information" for example.

That said, from the point of view of interoperability, we are not suggesting that all actors must use a common unique definition to "availability, "confidentiality" or "consent" (though this may be desirable form a legal point of view). We merely underline that the policy language semantics must be sufficiently precise to define attributes in a way that they are interpreted unambiguously and uniformly by all entities in the supply chain. In practice, this means for example that we may have several flavors of "availability" or "consent" each different but defined precisely in a way that all actors are able to understand which flavor is "selected". For example, in [8] the authors show that there are two common models of availability in the cloud, one based on the percentage of successful requests served and the other based on failure rates in time slots. Each one of these models requires a set of parameters to be correctly defined such as sample sizes, failure thresholds, failure events, etc. Being able to specify these parameters in an SLA or policy language is therefore necessary to express the semantics of the property called "availability". Similar caution is required for many other policy attributes.

From these observations we provide two foundational requirements that are common to all interactions between actors:

R01. Shared and well-defined semantics for security and privacy attributes.

R02. Shared and well-defined metrics for security and privacy attributes.

The following figure summarizes our model:

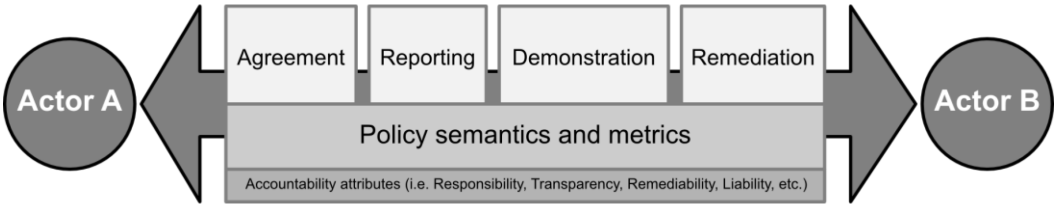
Actor A
Agreement
Reporting
Demonstration
Remediation
Policy semantics and metrics
Accountability attributes (i.e. Responsibility, Transparency, Remediability, Liability, etc.)
Actor B

Figure 3. Analytical model for logical interoperability requirements.

3 Elicitation of the logical requirements for interoperability

In the following section we derive requirements from each applicable family of interactions between actors. In most cases it is desirable to use a machine-to-machine interactions notably for efficiency and reduced risk of errors, but we do not claim that all interactions should be conducted this way.

As a consequence, unless specified otherwise, we use the term **protocol** broadly to cover a set of rules that govern the exchange of messages between entities, whether they are machines or humans. Similarly we use the term **language** to cover a system of signs used to express concepts or requirements in an unambiguous way, between machines or humans.

Additionally, when possible, we have attempted to illustrate the derived requirements with examples of existing protocols and languages that provide at least part of the required features listed in the requirements.

3.1 Path 1: Cloud providers and Cloud Customers

3.1.1 **Agreement (1a)**: Cloud customer expresses requirements to cloud provider OR cloud provider details offering to customer.

Description

Cloud customers must find a cloud provider that matches their data handling requirements, which may come from:

- Internal governance, risk and compliance frameworks (e.g. ISO 27001 [10], CSA Cloud Control Matrix [11], etc.)
- Regulations (e.g Directive 95/46/EC [7]) and ethics.
- Relaying requirements from their own customers in the supply chain, when the customer also acts as a cloud provider or relays the data subject’s requirements.

To achieve this, either:

- The cloud customer expresses requirements and the provider indicates its ability to implement them, potentially after a negotiation.
- The cloud customer chooses a provider that offers data handling practices that are compatible with its requirements.

Interoperability requirements

R03. A language which is able to express:

a. Policies describing constraints and rules applicable to security and privacy attributes (attributes defined by R1) including where applicable:
    i. Purpose definition and limitation;
    ii. Security measures (confidentiality, integrity, availability, key management, purpose limitation measures, etc.);
    iii. Retention and deletion quality;
    iv. Access control to data by privileged and non-privileged staff;
    v. Mechanisms for the exercise of user rights (information, modification and deletion)
    vi. The location of data in relation to applicable law;
    vii. Transfer of data and/or policies to third parties;
    viii. Mechanisms for the implementation of consent and withdrawal of consent, where applicable.

b. Scope of RESPONSIBILITY for data handling policy elements, with the identification of the corresponding parties taking responsibilities for data stewardship.
c. Scope of LIABILITY.
d. Obligations regarding:
    i. The process of reporting (OBERVABILITY, TRANSPARENCY)
    ii. The process of demonstration (VERIFIABILITY, ATTRIBUTABILITY)
    iii. The process of remediation (REMEDIABILITY).

Example(s): The PrimeLife Policy Language [28]. Additionally, some machine-readable SLA languages [12][14] already specify a small subset of the above elements.

R04. A protocol between the two parties, formalizing the acceptance of the terms defined by R03, potentially after negotiation, thereby establishing RESPONSIBILITY and LIABILITY.

Example(s): Classical "human" contract negotiation and signature. Automated SLA negotiation protocols, such as WS-Agreement [13], with some enhancements needed to cover a wider set of policies.

3.1.2 **Reporting (1b)**: Cloud provider informs cloud customer about policy implementation

Description

In an accountable cloud, the provider should give the customer feedback on the state of data handling, such as for example:

- Current policy description.
- Indicators for performance, compliance management and incident management,
- Access control statistics (by users, admins, etc.)
- Location of data
- Effective deletion of data (the gap between deletion requests and their execution),
- Configuration and supply chain changes
- Incident reports, policy and data breach reports.

We will distinguish between:

1) Reporting the policy terms (e.g. availability is always greater than 99% per month).
2) Reporting the actual compliance level (e.g. availability was 99.5% this month).
3) Alerting on deviation / breaches of the policy (e.g. alert: availability was 95% in the past month!).

This distinction will be used to form the 3 types of requirements below:

Interoperability requirements

R05. A protocol to describe the general policy applied by the Cloud Provider to data provided by any Customer, and/or, where applicable, specifics terms that apply to the Customer as negotiated through R04.

Example(s): CSA's CTP [15][16], CSA PLA [17].

Notes: Requirements R05 and R04 are complementary. First, the updated policy obtained through R05 may be "better" than the one negotiated in R04, due to security improvements for example. Second, in some cases, the reporting phase (R05) may happen before the agreement phase (R04), as the cloud provider may choose to report *his policies to potential clients in order to demonstrate transparency and attract new customers.*

R06. A protocol to report performance and compliance indicators relative to the terms of the agreement reached through R04.

Example: CSA CTP [16].

R07. An alerting protocol to report policy deviations (including data breaches) from cloud provider to cloud customer.

Example: CSA CTP [16].

3.1.3 **Demonstration (1c)**: Cloud provider demonstrates data handling practices to Cloud Customer

Description

Demonstrating policy application can be performed by several means, such as:

- Technical tools, including cryptography and monitoring.
- Audits by the customer or by a trusted third party.

We distinguish two modes of verification:

- Evidence based: The cloud provider presents evidence artifacts for verification by the customer or allows the customer to directly gather evidence from the provider by performing some interactive tests, in order to verify claims made in the policy from R04.
- Trust based: The cloud provider presents a certification or a trust-mark that supports claims made about the policy from R04, without providing directly the underlying evidence.

Interoperability requirements

R08. Either:

a. A language to describe evidence that supports claims related to the terms of the agreement reached through R04, along with a supporting protocol to either:
   i. Query evidence gathered by the Cloud Provider for verification by the Cloud Customer (ATTRIBUTABILITY and VERIFIABILITY).
   ii. Query evidence gathered by a trusted third party (Auditor), and provided to the Cloud Customer by the Cloud Provider (ATTRIBUTABILITY and VERIFIABILITY)
b. A protocol that enables the cloud Customer to directly test claims made by the Cloud Provider (VERIFIABILITY).
c. A language that describes the certification by a trusted party of claims made in R04, along with a protocol for the Cloud Customer to verify the authenticity of the certificate.

Example(s):
(a) ISO 27001 reports, CSA CloudAudit details [18], if they map to policy requirements,
(b) Data retrievability and redundancy testing [19].
(c) Example(s): ISO 27001 certificates, CSA Star Certification [20].

3.1.4 **Remediation (1d)**: Cloud Customer seeks remediation from Cloud Provider.

Description

Cloud customers deal with remediation in two ways:

- Implicitly, when the cloud provider automatically provides compensation to the cloud customer based on pre-agreed terms (e.g. a refund for a missed availability performance target).
- Explicitly, when a cloud customer makes a request for remediation to the cloud provider after detecting a failure (or momentary disruption) in the implementation of the data handling policy defined through R04 and that the Cloud Provider did not implicitly address in a satisfactory way.

By definition, the implicit case does require interactions and therefore does not impose any interoperability requirements.

Interoperability requirements

R09. A protocol to submit requests for remediation and receive information on the processing and the outcome of the request.

Example(s): Online service support desks, along with a set of accompanying procedures, provide an embryo for such a requirement.

3.2 Path 2: Cloud Auditor/Regulator and (Cloud Customer or Cloud Providers)

3.2.1 **Agreement (2a)**: Cloud Customer/Provider and Regulator interact for the purpose of prior consultation or prior authorization.

Description

Cloud Customers or Providers --when acting as a data controller-- may be required to inform regulators about data handling practices, prior to implementing a service.

This may be the case for processing that requires prior authorization (i.e. a permit) or prior consultation, as already implemented today in diverse forms in EU member states, and as envisioned in the upcoming EU data protection regulation [23]. Such consultation or authorization scheme usually requires the data controller to submit a description of data handling principles, including potentially a PIA (Privacy Impact Assessment), which is also a form of *demonstration*.

Interoperability requirements

R10. A language equivalent to R03, for the purpose of describing data stewardship practices to the regulator.

R11. An acceptance (or rejection) protocol for prior authorization (or consultation respectively) from the data protection authority.

3.2.2 **Reporting (2b)**: Cloud Customer/Provider informs Regulator about a data breach.

Description

In some cases, Cloud Customers/Providers (when acting as a data controller) may be required to submit data breach notifications to the regulator, as is the case already today in the telecom sector [21].

The Cloud Customer may be subject to a data breach notification obligation to the regulator only when a certain severity threshold is met: in the EU, in the telecom sector, notification to the regulator is obligatory unless technological measures encrypting the data are in place [22]. Similarly, regulators are likely to prioritize their response to notifications based on the assessed severity of the breach.

Interoperability requirements

R12. A severity assessment methodology that allows describing policy deviations along with a common set of metrics to evaluate the apparent severity of a breach based on the deviation.

Note: The metrics can be viewed as a special case of R02.

R13. A protocol for Cloud Customers to submit data breach notifications to Regulators.

3.2.3 **Demonstration (2d)**: Cloud Customer/Provider demonstrates to Cloud Auditor or Regulator data handling principles.

Description

Cloud Customers/Providers are required to demonstrate compliance to cloud auditors. To this end, both the auditor and the audited entity will follow a common approach (e.g. ISO 27001), which serves as an interoperability feature, to gather evidence supporting claims made in R03, as well as more broadly evidence supporting the correct implementation of an Information Security Management System.

Cloud Customers/Providers may also be required to demonstrate data handling principles to Regulators in the case of an on-site inspection, or otherwise in the case of prior consultation or authorizations (see 3.2.1). Again, in this case, a common methodology is beneficial for interoperability purposes, and may include approaches similar to those used by Auditors, data protection oriented tools (Privacy Impact Assessment frameworks), or Trust-marks.

The interoperability requirements of these interactions are therefore quite similar to the case of a Provider demonstrating policy compliance to a Cloud Customer (R08), though the scope of the verification may be different.

Interoperability requirements

R14. Either one or the combination of:

a. A language to describe evidence that supports claims related to the terms of the agreement reached through R04, along with a supporting protocol to either:
    i. Query evidence gathered by the Cloud Provider/Customer for verification by the Auditor/Regulator (ATTRIBUTABILITY and VERIFIABILITY).
    ii. Query evidence gathered by a trusted third party (another Auditor), and provided to the Auditor/Regulator by the Cloud Provider/Customer (ATTRIBUTABILITY and VERIFIABILITY)
b. A protocol that enables the Auditor/Regulator to directly test claims made by the Cloud Provider/Customer (VERIFIABILITY).
c. A language that describes the certification by a trusted party of claims made in R04, along with a protocol for the Auditor/Regulator to verify the authenticity of the certificate.

3.2.4 **Remediation (2d)**: Regulator imposes remediation action to Cloud Customer/Provider.

Description

In case of a failure to comply with data protection regulations, regulators may impose sanctions on Cloud Customers/Providers and/or request Cloud Customers/Providers to take specific actions to remediate the effects of the compliance failure, including momentarily requesting the processing to be shut down until a solution is found.

Interoperability requirements

R15. A notification protocol from Regulators to Cloud Customers/Providers requesting actions to remediate the effect of a compliance failure, describing:

a. The compliance failure that was identified.
b. The requested corrective actions, including short terms corrections and long term corrections.
c. Timeframe requirements for the corrections to be implemented.

Note: This is very unlikely to be a machine-to-machine protocol, but rather a step in a legal process that the cloud customer/provider has different options to challenge. Therefore, it may not necessarily be regarded as a real "interoperability" requirement.

3.3 Path 3: Cloud Customer, Cloud Broker and Cloud Provider

According to a study by Gartner [2], Cloud Brokers may be classified into 3 different categories as intermediaries between Cloud Providers and Cloud Customers:

1) *Cloud Service Intermediation*: The broker provides added value to a cloud service, enhancing some capabilities or guaranties offered by the underlying cloud provider to cloud customers.
2) *Aggregation*: The broker acts as an integrator, combining several Cloud Provider services into one, ensuring security and governance of data circulating between the composing services.
3) *Cloud Service Arbitrage*: The broker continuously attempts to select the best cloud provider based on price/feature considerations, potentially changing and migrating data between providers frequently.

A broker may therefore provide additional data stewardship guaranties that the underlying services don't or alter the ones provided. For example, a cloud broker might advertise greater storage durability based on a combination of storage providers or may offer higher levels of financial compensation in case of failure. In many cases, this means that the Cloud (Customer ⇔ Broker ⇔ Provider) interactions could also alternatively be modeled as two interactions of the type Cloud (Customer ⇔ Provider), where the broker plays both the role of a Customer and Provider. As such, the broker needs to be "accountability" aware, and able to gather, modify, aggregate or relay accountability interactions between Providers and Customers.

3.3.1 **Agreement (3a)**: Cloud Broker assists Cloud Customer in selecting a Cloud Provider(s), potentially providing additional assurance.

Description

Accountability requirements identified between Customers and Providers are applicable here, with the Broker having the ability to modify, aggregate or simply relay data stewardship policy requirements.

Note that in the simple case where the Broker is merely a relaying agent, he is not strictly speaking a cloud accountability actor but still has the interoperability requirement of relaying accountability related flows without altering them, much like Internet service providers, which relay data packets on networks. In cases where the broker offers an added value service, he then becomes a full cloud accountability actor playing both the role of a cloud customer and cloud provider.

Interoperability requirements

R16. The cloud broker must be able to interpret policy requirements **R03** and, when applicable, express his own policy offering in relationship with the added value services he offers.

R17. The cloud broker must be able to execute a protocol to negotiate policy requirements as defined in **R04**, both with Providers and Customers, taking into account the added value services he offers.

3.3.2 **Reporting (3b)**: Cloud Customer requests information from Cloud Broker about data handling by Cloud Provider.

Description

Accountability requirements identified between Customers and Providers are applicable here, with the Broker having the ability to modify, aggregate or simply relay data stewardship information requests.

As we did for Cloud Providers and Customers, we distinguish 3 types of requirements (see 3.1.2).

Interoperability requirements

R18. The Cloud Broker must be able to report a relevant subset of the general or negotiated policy as in requirement **R05**.

R19. The Cloud Broker must be able to aggregate, relay and report the compliance and performance indicators, as understood in **R06.**

R20. The Cloud Broker must be able to relay data breach notification, as understood in requirement **R07**.

3.3.3 **Demonstration (3c)**: Cloud Customer requests demonstration from Cloud Broker about data handling principles.

Description

Accountability requirements identified between Customers and Providers are applicable here, with the Broker having the ability to modify, aggregate or simply relay data stewardship demonstration requests.

Interoperability requirements

R21. The Cloud Broker is able must be able to aggregate and relay demonstration requests between customers and providers, potentially adding its own demonstrations, following the approaches defined in R08.

Note: The cloud broker may notably be required to demonstrate that it does not “alter” policies with the effect of reducing the level of protection requested by a customer.

3.3.4 **Remediation (3d)**: Cloud Customer requests remediation action, due to failure of a Cloud Provider.

Description

Accountability requirements identified between Customers and Providers are applicable here, with the Broker having the ability to modify and dispatch remediation requests.

Interoperability requirements

R22. The Cloud Broker is able must be able to modify and dispatch remediation requests, while presenting a central remediation request entry point as defined in R09.

3.4 Path 4: Data Subject and Cloud Customer/Provider

3.4.1 **Agreement (4a)**: Data subject and Cloud Provider negotiate data stewardship.

Description

To discuss “agreement” accountability interactions, we focus exclusively on cases where the Data Subject provides data to a Cloud Provider/Customer for the execution of a contract to which he is a party, or when this data is collected by the Cloud Provider/Customer on the basis of the legitimate interest of the Provider/Customer. This is the case for the majority of online businesses. By contrast we exclude cases where the Data Subject does not have control or choice on stewardship of data handed to a Cloud Provider/Customer. This is often the case when data processing is based on a legal obligation, general public interest or the vital interest of the data subject, where there is generally no process of agreement.

There are many modalities that lead Data Subject and Cloud Provider to negotiate data stewardship practices:

- Explicitly, when the Data Subject globally accepts data handling policy of a service, potentially selecting optional sub-conditions (checkboxes).
- Implicitly, when acceptance of data handling is assumed by default, leaving the Data Subject the option to refuse the conditions at a later stage (opt-out).

It is debatable whether an accountable organization would use the second approach, as it poses an implicit contradiction to the TRANSPARENCY attribute of accountability: the data subject is only made aware after the fact that his data is being processed, and then given an opportunity to opt-out. There is therefore a time-window during which data is being processed non-transparently, that is without the knowledge of the data subject. This discussion is prominent in the field of online behavioral advertising [24]. On the other hand, in situations where a data processing presents a low privacy risk, some service providers argue that using an explicit agreement protocol for data handling policies may lead a cumbersome online experience for data subjects without a real benefit in terms of privacy. Looking a this question from an interoperability perspective, we can argue for a technical solution that could enable Cloud Providers to always use the “explicit” approach, without its drawbacks: the use of machine-to-machine data policy agreement mechanism. Previous failures such as P3P [25] and DNT [26] show however that a consensus on this approach is difficult to achieve.

Interoperability requirements

R23. A language equivalent to R03, for the purpose of describing data stewardship practices from the point of view of data subjects.

R24. A protocol to negotiate elements of R23 with the Cloud Provider/Customer tailored to the interests and needs of Data Subjects.

R25. A “data subject friendly” control interface for the policy language described in R23.

Example(s): A browser privacy control panel.

3.4.2 **Reporting (4b):** Cloud Provider/Customer informs Data Subject about data handling practices.

Description

In Europe, Data controllers have a legal obligation to provide information to Data Subject about personal data processing.

The recently introduced data breach notification framework in the telecom sector also offers regulators the possibility to oblige Cloud Customers/Providers to inform data subjects of a breach, if they haven’t done so already (see ePrivacy directive[21] and implementation measures [22]). Indeed, according to the ePrivacy Directive, the notification to the regulator is an obligation unless data was encrypted, but the notification to the data subject is subject to an evaluation of the existence of the adverse effects of the breach.

Just as we did for Cloud Customers and Cloud Providers in 3.1.2, we distinguish reporting the “agreed terms”, reporting the “compliance level to the agreed terms” and reporting “breach alerts”.

Interoperability requirement

R26. A protocol to query information in a “data subject friendly” format, presenting the general data policy and/or specific terms agreed in R24.

R27. A protocol to present compliance level information in a “data subject friendly” format, for the terms agreed in R24.

R28. An alert protocol that allows data subject to be informed about a breach should one occur. Such an interface should at least provide information about the nature of the breach and actions that the data subject can take to mitigate effects of the breach.

3.4.3 **Demonstration (4c)**: Cloud Customer demonstrates data handling principles to Data Subject.

Description

Data subject should be able to verify the claims of a Cloud Provider/Cloud Customer with the same tools that a Cloud Customer uses to verify the claims of a Cloud Provider (see 3.1.3). In practice, most users would not have the expertise to evaluate evidence provided by a Cloud Provider/Customer, and rely on trust, be that in a third party (certification and trust-mark), which is embodied in option (c) of requirement R29 below.

Interoperability requirements

R29. Either one or the combination of:

a. A language to describe evidence that supports claims related to the terms of the agreement reached through R24, along with a supporting protocol to either:

i. Query and verify evidence gathered by the Cloud Provider for verification by the Cloud Customer (ATTRIBUTABILITY and VERIFIABILITY).
ii. Query and verify evidence gathered by a trusted third party (Auditor), and provided to the Cloud Customer by the Cloud Provider (ATTRIBUTABILITY and VERIFIABILITY)

b. A protocol that enables the Data Subject to directly test claims made by the Cloud Provider (VERIFIABILITY).
c. A language that describes the certification (or trust-mark) by a trusted party of claims made in R04, along with a protocol for the Data Subject to verify the authenticity of the certificate.

3.4.4 **Remediation**: Data Subject seeks remediation from Cloud Customer/Provider.

Description

Much like loud customers, data subjects deal with remediation in two ways:

- Implicitly, when the cloud provider automatically provides compensation to the cloud customer based on pre-agreed terms (e.g. a refund for a missed availability performance target).
- Explicitly, when a cloud customer makes a request for remediation to the cloud provider after detecting a failure (or momentary disruption) in the implementation of the data handling policy defined through R04 and that the Cloud Provider did not implicitly address in a satisfactory way.

By definition, the implicit case does not require interactions and therefore does not impose any interoperability requirements.

Interoperability requirements

R30. A protocol for Data Subjects to submit requests for remediation to Cloud Providers/Customers and receive information on the outcome of the request.

Example(s): Online service support desks, along with a set of accompanying procedures, provide an embryo for such a requirement.

3.5 Path 5: Cloud Auditor/Regulator and Data Subject

3.5.1 **Agreement (5a)**: none.

We did not identify agreement interactions between these actors, for the purpose of data stewardship.

3.5.2 **Reporting (5b)**: none.

We did not identify information interactions between these actors, regarding data stewardship.

3.5.3 **Demonstration (5c)**: none.

We did not identify data demonstration interactions between these actors, regarding data stewardship.

3.5.4 **Remediation (5d)**: data subject seeks remediation to be imposed by regulator on a third party (cloud provider, cloud broker, cloud customer).

Description

Data Subjects regularly lodge complaint with regulators, due to perceived or real lack of compliance by a service provider. These complaints are examined by the Regulators and may be followed by an informal or formal inquiry, sanctions, etc.

Interoperability requirements

R31. An entry point for Data Subjects to submit complaints to Regulators about compliance failures of Cloud Providers/Customers.

3.6 Summary of logical interoperability requirements

The following table summarizes the logical interoperability requirements derived from the analysis provided in this document. The third column of this table describes each requirement in a short simplified sentence: we refer the reader to the full requirement descriptions in the previous sections for completeness.

Path	Actors involved	Summarized requirements
All	All	R01. Standardized security and privacy semantics R02. Metrics for security and privacy attributes.
1	Customer ⬄ Provider	R03. Data handling policy and obligation language R04. A negotiation protocol for the terms of R03. R05. A policy statement reporting protocol. R06. A compliance reporting protocol. R07. A data breach notification protocol, to customers. R08. An evidence reporting protocol. R09. A remediation request protocol.
2	Auditor/Reg. ⬄ Customer or Auditor/Reg. ⬄ Provider	R10. Data handling policy and obligation language, equivalent to R03. R11. A prior authorization/consultation protocol. R12. A breach severity assessment methodology. R13. A data breach notification protocol, to regulators. R14. An evidence reporting protocol for R10. R15. A corrective action request protocol.
3	Customer ⬄ Broker ⬄ Provider	R16. Data handling policy and obligation language, equivalent to R03 R17. A broker-mediated version of R04. R18. A broker-mediated version of R05. R19. A broker-mediated version of R06. R20. A broker-mediated version of R07. R21. A broker-mediated version of R08. R22. A broker-mediated version of R09.
4	Data Subject ⬄ Customer or Data Subject ⬄ Provider	R23. Data handling policy and obligation language, equivalent to R03 but scoped for data subjects. R24. A negotiation protocol for R22. R25. A user-friendly control panel for R22. R26. A user-friendly policy statement reporting protocol. R27. A user-friendly compliance reporting protocol. R28. A data breach notification protocol. R29. A trust-mark or evidence verification protocol. R30. A remediation request protocol.
5	Auditor/Reg. ⬄ Data Subject	R31. A complaint submission protocol.

4 Use-case based analysis of logical requirements

In the following, we present how the logical interoperability requirements identified in Section 3 are applied to the defined cloud roles of the three business use cases, based on their description in the A4Cloud Deliverable D:B-3-1: Use Case Descriptions.

4.1 Health Care Services in the Cloud

In this scenario, the different entities identified in D:B-3.1 are mapped to the cloud interactions, with the following distribution of actors:

- The Patient is a Data Subject, who shares personal data and sensitive information with the Hospital and the Cloud Provider x.
- The Relative/friend is also a Data Subject, who acts as an individual end user uploading further information about the Patient, but also receiving information on Patient's health status.
- The Hospital is a Cloud Customer, who makes the diagnosis of the Patient and decides on the appropriate treatment.
- The Cloud x is a Cloud Provider, acting as the organization that operates the sensor data collection and processing the collected data.
- Cloud y is a Cloud Provider, acting as the organization that operates the data storage cloud.
- The MedNet platform provider is both a Cloud Customer and a Cloud Provider, which delivers the software for sensor data collection and processing to the hospital and operates Cloud z.
- The Norwegian Data Protection Authority is a Cloud Auditor/Regulator that verifies that statutes and regulations that apply to the processing of personal data are complied with, and that errors or deficiencies are rectified. We assume that due to the use of sensitive data, the regulator will conduct some form of prior checking.

The following table maps the general accountability requirements identified D:B-3.1 for this scenario to a set of logical interoperability requirements using the requirement list provided in section 3:

Accountability relationship	Implied interoperability requirements
The **relative/friend is responsible to the patient** for adhering to the patient's privacy preferences when uploading personal data about the patient	None directly, though this is probably enforced by the hospital, and would then become part of policy terms for the relatives/friends **[R23]**.
The **hospital is responsible to the patient** for asking the explicit consent for collecting and processing personal data	These are policy terms **[R23]** materialized by an agreement on the processing of the data **[R24]**
The **hospital is responsible to the patient** for asking the explicit consent for allowing relatives to access personal data	These are policy terms **[R23]** appearing in a contract **[R24]**.
The **hospital is responsible to the patient** for using personal data for the specified purpose only	These are policy terms **[R23]** appearing in a contract **[R24]** (which derive form regulations)
The **hospital is responsible to the patient** for informing them about data handling practices.	These are policy terms **[R23]** appearing in a contract **[R24]**, which will lead to the implementation of user information **[R26]**.
The **hospital is liable to the patient** in case of personal data loss or misuse	These are policy terms **[R23]** appearing in a contract **[R24]**, which will lead to a remediation request mechanism **[R30]**.

The **hospital is responsible to the Norwegian Data Protection Authority** for using personal data in accordance to applicable rules and legislations	This could imply prior checks form the DPA **[R11]**, with a description of the policy **[R10]**.
The **hospital is responsible to the Norwegian Data Protection Authority** for proving evidence jon the data collection practices	This could imply prior checks from the DPA **[R11]** or demonstrations during an inspection **[R14]**.
The **hospital is responsible to the Norwegian Data Protection Authority** for informing about the collection and processing of personal data	This could imply prior checks from the DPA **[R11]**.
The **MedNet platform provider is responsible to the hospital** for logging all access to personal data	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
The **MedNet platform provider is responsible to the hospital** for informing about 3rd party service providers in the service deliverable chain	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will likely result in compliance information reporting **[R06]**.
The **MedNet platform provider is liable to the hospital** when including 3rd party service providers in the service deliverable chain	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to remediation requests **[R09]**.
The **MedNet platform provider is responsible to the hospital** for fulfilling their contract terms	This is true if terms have been agreed **[R04]**.
The **MedNet platform provider is responsible to the hospital** for proving evidence on the data processing practices	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the implementation of a demonstration mechanism **[R08]**.
The **MedNet platform provider is responsible to the hospital** for notification of security or privacy breaches	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the implementation of a data breach notification mechanism **[R07]**.
The **MedNet platform provider is liable to the hospital** in case of personal data loss or misuse	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to a remediation request mechanism **[R09]**.
Cloud provider x is responsible to the MedNet platform provider for the security of the provided service	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
Cloud provider x is responsible to the MedNet platform provider for proving evidence on the data processing practices	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the implementation of a demonstration mechanism **[R08]**.
Cloud provider x is responsible to the MedNet platform provider for fulfilling their contract terms	This is true if terms have been agreed **[R04]**.
Cloud provider x is liable to the MedNet platform provider in case of personal data loss or misuse	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
Cloud provider y is responsible to the MedNet platform provider for secure storage and back-up of sensor data	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
Cloud provider y is responsible to the MedNet platform provider for correct and timely deletion of stored sensor data	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
Cloud provider y is responsible to the MedNet platform provider for the security of the provided service	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.

Cloud provider y is responsible to the MedNet platform provider for proving evidence on the data storage practices	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the implementation of a demonstration mechanism **[R08]**.
Cloud provider y is responsible to the MedNet platform provider for fulfilling their contract terms	This is true if terms have been agreed **[R04]**.
Cloud provider y is responsible to the MedNet platform provider for notification of security or privacy breaches	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will result in data breach notification mechanism **[R07]**.
Cloud provider y is liable to the MedNet platform provider in case of personal data loss or misuse	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to a remediation request mechanism **[R09]**.
The Norwegian Data Protection Authority is responsible to the patient for monitoring that the rules and legislation for protecting personal data are being obeyed	This is done through prior checks **[R11]** or inspections **[R14]**, which could be triggered by complaints by patients **[R31]**.
The Norwegian Data Protection Authority is responsible to the patient for controlling that incorrect usage of personal data is corrected	Control and remediation are the result of an inspection / post-check process **[R14]**.

4.2 Cloud-based ERP Software Enabled with Third Party Extensions

In this scenario, the different entities identified in D:B-3.1 are mapped to the cloud interactions, with the following distribution of actors:

- The supermarket customer is a Data Subject, who shares personal data and financial information.
- The supermarket chain is both a Cloud Customer and a Cloud Provider that processes the customers' data and shares them for supermarket offers and third party exploitation.
- Third-party service provider is both a Cloud Customer and a Cloud Provider, acting as a provider to send additional advertisements.
- PaaS owner is a Cloud Provider, deploying the platform through which data is collected and distributed among the end users.
- IaaS provider is again a Cloud Provider that provides storage and communication capabilities
- Regulator is a Cloud Auditor responsible for providing the legal framework that governs the information exchange among the users and providers.

The following table maps the general accountability requirements identified D:B-3.1 for this scenario to a set of logical interoperability requirements using the requirement list provided in section 3:

Accountability relationship	Implied interoperability requirements
The **supermarket customer is responsible to the supermarket chain** for providing correct identification information	These are policy terms **[R16]** materialized by a contractual agreement on the processing of the data **[R17]**.
The **supermarket chain is responsible to the supermarket customer** for processing data according to the customer preferences	These are policy terms **[R23]** materialized by an agreement on the processing of the data **[R24]**.
The **supermarket chain is responsible to**	This can be demonstrated through certification

Accountability relationship	Implied interoperability requirements
the supermarket customer for providing the evidence that the data was processed accordingly	and trust-marks **[R29]**.
The **supermarket chain is responsible to the supermarket customer** to send only the offers that are related to the customer's preferences	These are policy terms **[R23]** materialized by an agreement on the processing of the data **[R24]**.
The **supermarket chain is responsible to the supermarket customer** to share with the third-party service provider only the information required for the business needs of the latter	These are policy terms **[R23]** materialized by an agreement on the processing of the data **[R24]**.
The **third-party service provider is liable to the supermarket chain** in case of the loss of control over the supermarket customer data	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to a remediation request mechanism **[R09]**.
The **third-party service provider is responsible to the supermarket chain** to inform it about any changes related to the handling of the data received for providing the business purpose	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will likely result in compliance information reporting **[R06]**.
PaaS Owner assures the supermarket chain and the third-party service provider that the correct measures protecting from unauthorized data access are in place	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the implementation of a demonstration mechanism **[R08]**.
The **supermarket chain** should be held responsible in case of the loss of control over the **supermarket customer** data	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to a remediation request mechanism **[R09]**.
The **third-party service provider** should give a clear explanation why the data he collects from the **supermarket chain** is necessary for providing the service	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to the information of data subjects **[R26]**.
IaaS Owner is liable to the **PaaS Owner** over any security breach in the infrastructure	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will lead to a remediation request mechanism **[R09]**.
The **regulator** is responsible to assure the **supermarket customer** that the supermarket chain processes the data accordingly	This is done through prior checks **[R11]** (unlikely) or inspections **[R14]**, which could be triggered by complaints by customers **[R31]**.
The **supermarket chain** is responsible to provide the necessary data to the **regulator** during the audit	This is done as part of inspections **[R14]**.
PaaS Owner should notify the **supermarket chain** and the **third-party service provider** in case of any security incident related to the platform	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which will result in data breach notification mechanism **[R07]**.

4.3 Rights and Relevant Obligations in a Multi-tenant Cloud

In this scenario, the different entities identified in D:B-3.1 are mapped to the cloud interactions, with the following distribution of actors:

- In some cases, the individual end user can both be a Data Subject and a Cloud Customer. In those cases, without loss of generality, we will consider him as a Cloud Customer in the table below, though an equivalent mapping can be constructed from the point of view of a Data Subject.

- The business end user is a Cloud Customer that provides corporate data in the cloud.
- The cloud service user is a Cloud Customer that consumes the results of a service chain.
- The cloud service provider is a Cloud Provider that offers services over the cloud.
- The cloud infrastructure provider is a Cloud Provider that is responsible to secure the appropriate infrastructure resources, so that the cloud services can be executed.

The following table maps the general accountability requirements identified D:B-3.1 for this scenario to a set of logical interoperability requirements using the requirement list provided in section 3.

We note that the format of the accountability relationships defined in this third scenario extracted from D:B-3.1, and represented in the first column of the table below, differ slightly in format from the previous two. When needed, we therefore enriched these accountability relationships with our annotations provided between brackets for coherence.

Accountability relationship	Implied interoperability requirements
The **individual end user** is responsible **[*to the cloud provider*]** for selecting the personal data to be placed in the cloud	These are policy terms **[R23]** materialized by a contractual agreement on the processing of the data **[R24]**.
The **business end user** is responsible **[*to the cloud provider*]** for providing the corporate data to be placed in the cloud	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**.
The **cloud service user** is responsible for accepting the results provided by the **cloud service providers**	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]** (alternatively **[R23]** and **[R24]**).
The **cloud service provider** is responsible for maintaining the integrity of the cloud-based personal data delivered to the **cloud service users**	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]** (alternatively **[R23]** and **[R24]**).
The **cloud infrastructure provider** is responsible **[*to the cloud users*]** for preventing any unauthorised access to the resources of the cloud ecosystem	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]** (alternatively **[R23]** and **[R24]**).
The **cloud service provider** should pay penalty **[*to the cloud user*]** when data used for the service to be offered are leaked to other service providers without the cloud (individual or business) end user consent	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which may result in remediation requests **[R06]** (alternatively **[R23]**, **[R24]** and **[R30]**)
The **cloud infrastructure provider** should pay penalty to **cloud service provider and/or cloud service user** on data misuse	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the data **[R04]**, which may result in remediation requests **[R06]** (alternatively **[R23]**, **[R24]** and **[R30]**)
The **cloud service provider** should make an analysis of risks from the misuse of cloud end users' data in the cloud [*for the purpose of user information and demonstration*]	This can be part of a demonstration mechanism **[R08]**.
The **cloud service provider** should make explicit **[*to the cloud user*]** which cloud end users' personal and sensitive data are necessary to offer the service on the cloud	These are policy terms **[R23]**, which may be reported as information to users **[R05]**.
The actions performed by the **cloud service provider** and the **cloud service user** when	These are policy terms **[R03]** materialized by a contractual agreement on the processing of the

Accountability relationship	Implied interoperability requirements
accessing personal and sensitive data should be logged [*for the purpose of user information and demonstration*]	data **[R04]**. (alternatively **[R23]** and **[R24]**).
The **cloud service provider** assures **[*to the DPA*]** that the process of data stored in the cloud is compliant with regulatory frameworks and the business policies of the service provider	This is not directly an interoperability issue, but could trigger consultation/authorization interactions with the DPA **[R11]**, and/or a demonstration process **[R06]**/**[R27]**.
The **cloud infrastructure provider** assures **[*to the cloud user*]** that no data is leaked outside the scope of the underlying applications	This is not directly an interoperability issue, but could support demonstration efforts to customers **[R06]** or the DPA **[R14]**.

5 Conclusion

This work identified a set of 31 logical interoperability requirements for the purpose of supporting accountability attributes in the cloud.

We believe that one requirement stands above all the others: the need for shared privacy and security attribute semantics in the accountability chain. Such a requirement, as embodied in **R1**, is a precondition to the realization of all others.

Some of the requirements we identified in this documents are likely to benefit from a set of automated machine-to-machine protocols and languages with high standardization requirements while others are likely to remain largely “manual” with low standardization requirements. Building such a classification might prove useful in order to prioritize future standardization actions. We intend to provide this classification at a later stage in the A4CLOUD project.

As a next step we aim to move to a logical and technical interoperability analysis that not only includes actors described in this deliverable but adds functional blocks implemented by each actor as identified in the A4CLOUD project, in order to identify potentially missing functional blocks or inconsistencies between functional block used by different actors.

6 References

[1] Oxford dictionary. http://oxforddictionaries.com/definition/english/interoperable

[2] Gartner: Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services, https://www.gartner.com/newsroom/id/1064712

[3] A4Cloud, “MS:C-2.2, Conceptual framework”, internal milestone document, March 31, 2013.

[4] A4Cloud, “MS:C-3.1 Standards for interoperability”, internal milestone document, March 30, 2013.

[5] A4Cloud, “D:B-3.1 Use case description”, June 30, 2013.

[6] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST special publication*, *500*, 292.

[7] European Commission, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." *Official Journal L* 281.23/11 (1995): 0031-0050.

[8] Giles Hogben, Alain Pannetrat, “Mutant Apples: A critical examination of cloud SLA availability definitions", accepted for publication at IEEE 5th international conference Cloud Computing Technology and Science (CloudCom). December 2013.

[9] G. Hogben, M.Dekker (Eds.) Procure Secure, A guide to monitoring of security service levels in cloud contracts, ENISA, 2012

[10] ISO/IEC 27001:2005, “Information technology -- Security techniques -- Information security management systems – Requirements”, International Organization for Standardization.

[11] Cloud Security Alliance: “Cloud Control Matrix”, https://cloudsecurityalliance.org/research/ccm/.

[12] Kearney, K.T.; Torelli, F.; Kotsokalis, C., "SLA★: An abstract syntax for Service Level Agreements," *11th IEEE/ACM International Conference on Grid Computing (GRID), 2010,* vol., no., pp.217,224, 25--28 Oct. 2010.

[13] Alain Andrieux, Karl Czajkowski, Asit Dan, Kate Keahey, Heiko Ludwig, Toshiyuki Nakata, Jim Pruyne, John Rofrano, Steve Tuecke, Ming Xu: “Web Services Agreement Specification” (WS--Agreement), September 7, 2006.

[14] Ludwig, H., Keller, A., Dan, A., King, R., Franck, R.: Web service level agreement (WSLA) language specication. IBM Corporation (2003)

[15] Cloud Security Alliance. CTP Data Model and API – Version 2.5, August 2013.

[16] Cloud Security Alliance. CTP Reference Specification of Service Security Attributes – version 0.2, July 2013.

[17] Cloud Security Alliance. Privacy Level Agreements for CSPs serving the EU. https://cloudsecurityalliance.org/research/pla/

[18] Cloud Security Alliance. CloudAudit. https://cloudsecurityalliance.org/research/cloudaudit/

[19] Juels, Ari, and Alina Oprea. "New approaches to security and availability for cloud data." *Communications of the ACM* 56.2 (2013): 64-73.

[20] Cloud Security Alliance. “STAR Certification / Attestation”, https://cloudsecurityalliance.org/star/

[21] European Commission. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector." *Official Journal L* 201.31 (2002): 07.

[22] Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

[23] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012/0011 (COD), Brussels, 25.1.2012.

[24] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011.

[25] Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., & Reagle, J. (2002). The platform for privacy preferences 1.0 (P3P1. 0) specification. *W3C recommendation*, *16*.

[26] W3C Tracking Protection Group, “Tracking Preference Expression (DNT)”, W3C Editor's Draft 02 October 2013, http://www.w3.org/2011/tracking-protection/drafts/tracking-dnt.html

[27] Article Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", Adopted on 16 February 2010.

[28] Ardagna, C., Bussard, L., De Capitani di Vimercati, S., Neven, G., & Paraboschi, S. (2009). Pedrini: The PrimeLife Policy Language.

[29] A4Cloud, “MS:C-2.3, Glossary”, internal milestone document, Work in progress.