CLOUD
ACCOUNTABILITY
PROJECT

D:B-2.1 Workshop 1 Results (Requirements)

Deliverable Number: D22.1

Work Package: WP 22

Version: Final

Deliverable Lead Organisation: SINTEF

Dissemination Level: PU

Contractual Date of Delivery (release): January 31st 2013

Date of Delivery: March 15th 2013

Editor
Nils Brede Moe (SINTEF)

Contributors
Martin Gilje Jaatun (SINTEF), Børge Haugset (SINTEF), Maartje Niezen (TiU), Massimo Felici (HP)

SEVENTH FRAMEWORK PROGRAMME

Executive summary

This deliverable reports on the initial requirements that were identified in the first stakeholder workshop in the A4Cloud project. The main goal of the first workshop was to elicit initial accountability requirements from key stakeholders. In A4Cloud, a stakeholder means a person, group or organization that affects or can be affected by the A4Cloud project results. The second goal was to get a reality-check on the three business use cases that will demonstrate how the A4Cloud accountability approach can prevent breaches in trustworthiness, detect policy violations, and correct violations that may occur.

Face-to-face communication and interaction through active stakeholder participation is strongly encouraged when eliciting requirements. However, supporting a face-to-face process is difficult in complex situations involving multiple diverse stakeholders such as in the A4cloud project. Therefore we relied on the workshop techniques Open Space Technology and World Cafe, because these techniques handle complex situations involving diverse participants and the need for a quick decision-making.

To be able to capture the stakeholders' understanding of the concept of accountability, but without influencing them with how the challenges related to accountability are seen from the A4Cloud project, the stakeholders where only given a very brief introduction to the project. The following motivation for the workshop was presented in the invitation letter to the stakeholders: *We need to better understand Accountability in the cloud to create better tools and mechanisms that will allow cloud providers to be responsible stewards of customers' data*. We did not explain what kind of tools we where looking for.

Through a workshop based on open processes, led by the stakeholders themselves, 57 initial requirements in the form of accountability relationships have been identified. The accountability relationships will serve as a basis for the ensuing work of identifying accountability requirements for cloud and other future internet services. The identified relationships cover the accountability elements assurance, liability, observability, remediation, responsibility, sanctions, transparency and verifiability.

Table of Contents

1 Introduction

Cloud and IT service providers should act as responsible stewards for the data of their customers and users. However the current absence of accountability frameworks for distributed IT services makes it difficult for users to understand, influence and determine how their service providers honour their obligations. Motivated by the current absence of accountability frameworks in the cloud and other future internet services, the A4Cloud project will develop tools and technologies that enable accountability for how personal and business confidential information is used in the cloud, taking into account the chain of responsibilities that needs to be built throughout the cloud service supply network.

Involving stakeholders through the whole project is essential for the A4Cloud project to succeed. In A4Cloud, a stakeholder means a person (not part of the project), group or organization that affects or can be affected by the A4Cloud project results. Stakeholders will be involved in a series of workshops for identifying requirements for the A4Cloud project, and for getting feedback on the A4Cloud results. Involving stakeholders through workshops enables the possibility for identifying concerns and values, developing consensus among affected parties, and producing efficient and effective solutions through an open, inclusive process.

1.1 A4Cloud project

The A4Cloud project deals with accountability for the cloud and other future Internet services. In the context of the project, accountability concerns data stewardship regimes in which organizations that are entrusted with personal and business confidential data are responsible and liable for processing, sharing, storing and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data is destroyed (including onward transfer to and from third parties)(Siani Pearson et al. 2012).

A4Cloud aims at creating solutions to support users in deciding and tracking how their data is used by cloud service providers. By combining methods of risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress, A4Cloud aims to extend accountability across entire cloud service value chains, covering personal and business sensitive information in the cloud.

A4Cloud solutions aim at supporting service providers in preventing breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress.

A4Cloud aims to improve the acceptability of cloud-based infrastructures where critical data is perceived to be at risk. It will develop techniques for improved trustworthiness of cloud ecosystems as prerequisite for accountability. Therefore it will create policies and tools that enforce responsibilities while striking a balance between transparency and privacy, and determine issues and constraints for regulators, corporate and institutional service providers, users, and their end-users.

A4Cloud aims to have a lasting impact on the competitiveness of the European ICT sector by addressing major perceived barriers to trustworthy cloud-based services. These include concerns about complexity and enforceability of legal, regulatory and contractual provisions, socio-economic and corporate constraints, issues of trust for service-users such as risk-mitigation, privacy, confidentiality and transparency, and operational challenges such as interoperability and enforcing and monitoring compliance.

1.2 Reflecting needs of stakeholder groups

To ensure that project activities reflect the needs of important stakeholder groups, the A4cloud project is engaging with a broad base of relevant stakeholders for requirement elicitation purposes. Examples of relevant stakeholder groups can be found in **Figure 1**. Interaction with stakeholders will primarily be done in workshops.

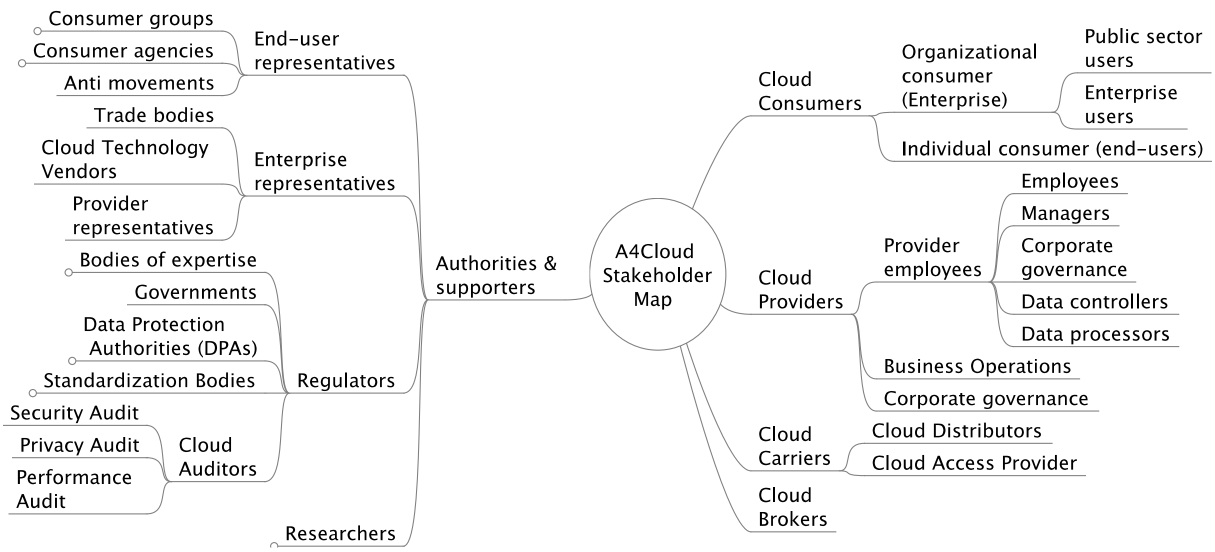


Figure 1: Example of stakeholders in the A4Cloud project

Interactions with stakeholders will be carried out in parallel with the conceptual developments and technical work in other work packages, to enable rapid feedback and validation of interim results. Stakeholder contact is important not only to elicit requirements, but also to get a reality-check on intermediate results produced in the project. The results of the first workshop, which is described in this document, will be fed back into the conceptual work and provide an initial baseline for work in the other WPs.

The aim of involving stakeholders in workshops is to gather a broad spectrum of requirements, good practices and risks related to the cloud eco-system covering the diverse range of geographical (including legal) constraints and challenges, sector/industry-specific requirements and cloud models.

A minimum of four stakeholder elicitation workshops (**Figure 2**) are planned in the A4Cloud project, the first of which is documented in this report.

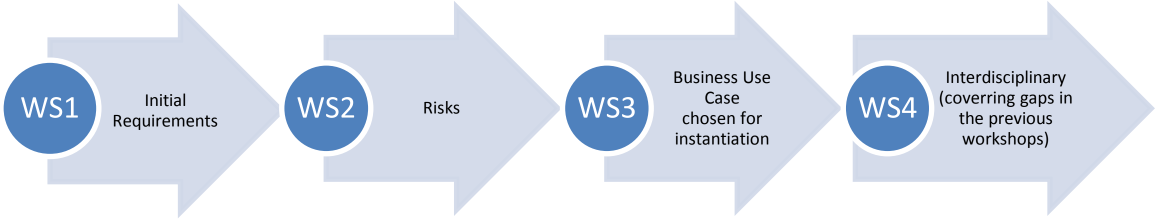

WS1
Initial Requirements
WS2
Risks
WS3
Business Use Case chosen for instantiation
WS4
Interdisciplinary (coverring gaps in the previous workshops)

Figure 2: Elicitation workshops and principal focus for each of them

To capture initial requirements the stakeholders in the first workshop were asked the following question during the introduction to the workshop: *What would make you or the people you represent more comfortable in the cloud?* The workshop relied on open processes (Open Space Technology and World Café) as techniques for documenting initial requirements. The workshop method for eliciting requirements will be described in detail in the next chapter.

1.3 Relationship to Other A4Cloud Work Packages

This deliverable is the first from WP:B-2 (Elicitation). Results from WP:B-2 will feed into a number of other work packages and deliverables in the A4Cloud project. There will be close interactions between all the WPs within stream B. In particular, WP:B-4 (Socio-economic context) and WP:B-5

(Contractual and regulatory considerations) will provide input into and analysis of stakeholder views and WP:B-3 (Use-case development) will use workshop results from WP:B-2 as input to the use case descriptions. In the following we list the most important relations between this deliverable and other work pages:

- The goal of **WP:B-3 (Use-case development)** is to provide understanding of 'real-world' scenarios from three distinct user domains in the form of use-cases that inform research and development work throughout the project. The stakeholders involved in the first A4Cloud stakeholder workshop have given important input to the real world scenarios. Use case 1 deals with the flow of healthcare information generated by medical sensors in the cloud. Use case 2 deals with cloud-based ERP software, which is enabled with third party extensions. Use case 3 deals with a multi-tenant cloud scenario to show how A4Cloud tools and technologies can help solve the intersection of policy enforcements at different IT domains. Also the third WP:B-2 stakeholder workshop will feed into the scenarios.
- The goal of **WP:C-2 (Conceptual Framework)** is to ensure a common understanding and consistent interpretation of issues relating to accountability and its contribution to trustworthy ICT. Draft content from the scoping report from WP:C-2 (MS:C-2.1) has been used when identifying the initial requirements from the first stakeholder workshop. The results from this report will be fed back into WP:C-2 and provide an initial baseline for work in other WPs in Streams C and D.
- The goal of **WP:A-3 (Dissemination)** is to ensure the proper dissemination of project results, the creation of communities of interest and the execution of training activities. WP:B-2 will rely on communication channels maintained by WP:A-3 to continue engaging with stakeholders.
- The goal of **WP:C-4 (Policy mapping and representation)** is to define a framework for enforceable accountability policies. Results from this report will be used as input to the first task in C-4: Policy model and language requirements.

1.4 Deliverable Organization

The remainder of this report is organized as follows. In Section 3, we describe our research method in detail. In Section 4 we present initial accountability requirements from the first stakeholder workshop. We discuss our findings in Section 5. Section 6 concludes.

2 Method for elicitation of requirements

Face-to-face communication and interaction through active stakeholder participation is strongly encouraged when electing requirements, typically with a single stakeholder representative present. However, supporting a face-to-face process is often difficult in complex situations involving multiple diverse stakeholders like in the A4cloud project (**Figure 1**). A potential solution is offered through the workshop technique Open Space Technology (Owen 2008; “OpenSpaceWorld.org” 2013), which is recommended for complex situations involving diverse participants and the need for quick decision making.

The rest of this section describes how stakeholders were selected for the workshop, how the workshop was organized and finally how initial requirements in the form of accountability relationships were identified based on the results from the workshop.

2.1 Selection of stakeholders

All partners in the A4Cloud projects were asked to nominate potential stakeholders for the first workshop. In this context a stakeholder was identified as an important influencer in defining future European Cloud solutions, such as cloud providers, data protection authorities, technology integrators, infrastructure providers, commercial cloud users, consumer representatives and researchers (see **Figure 1**). Partners were encouraged to nominate stakeholders both within and outside their contact network. 75 stakeholders were identified based on this process.

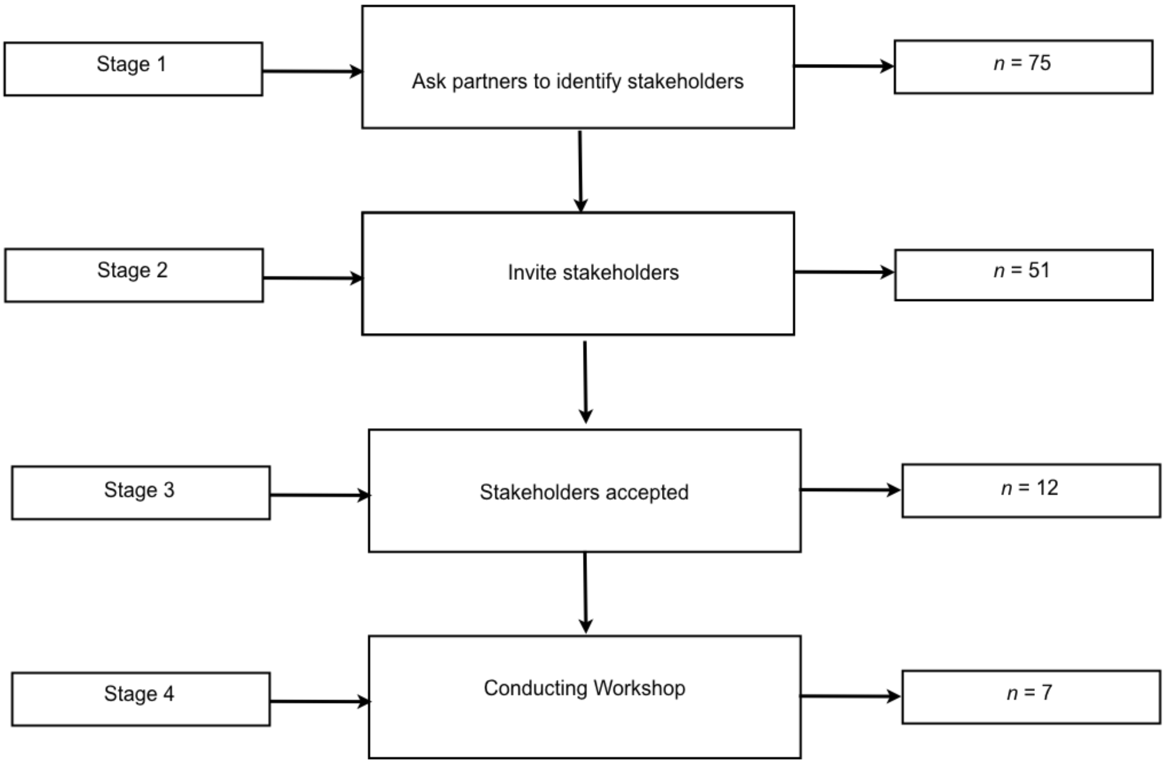


Figure 3: The stages of selecting stakeholders

In order to maximise the probability of a successful workshop, a multi-tiered approach was employed to recruit stakeholders to the workshop. First, a small group of six key stakeholder representatives from IBM, SURFnet's Taskforce Cloud, the Dutch consumer organisation (Consumentenbond), Independent Centre for Privacy Protection, VMware, and Google were identified, and queried for availability on six possible dates in January. Based on their feedback, January 16th was selected as the date for the first A4Cloud stakeholder workshop.

After setting the workshop date, project partners sent invitations letters (Appendix D) to 51 stakeholders previously identified by them. In order to avoid responder fatigue, it was decided not to invite the 6 stakeholders identified by Karlstad University, since these would be invited to local workshop in Sweden in February 2013. A further 18 stakeholders were not invited for various reasons, such as:

- being invited to the A4Cloud advisory board instead,
- no suitable representative identified in stakeholder association,
- presumption of unavailability (this includes those located outside Europe).

From the 51 stakeholder representatives invited to the workshop; 12 accepted, 17 declined, and the rest did not respond (the process is illustrated in Figure 3). In addition, we posted an open invitation on the LinkedIn groups Cloud Security Alliance and Cloud Computing Association, but this did not generate any further attendees.

Within the last 24 hours before the workshop, 5 of the 12 confirmed stakeholder representatives had to cancel for various travel-related and personal reasons, leaving only 7 external attendees on the day of the workshop.

Table 1: Participants at the workshop

Name	Position	Organisation	Stakeholder type
Massimo Attoresi	Technology and Security Officer	European Data Protection Supervisor	Data Protection Authority
Emmanuelle Bartoli	Chief Privacy Officer	ATOS	Cloud Provider
Marit Hansen	Deputy Head	Independent Centre for Privacy Protection Schleswig-Holstein	Data Protection Authority
Nick Hyner	Responsible for cloud compliance	Dell	Cloud Technology Vendor
Zoe Kardasiadou	Head of Auditors Department	Hellenic Data Protection Authority	Data Protection Authority
Benny Schaich-Lebek	Id Mgmt and Cloud solutions team	SAP	Cloud Provider
Simone Weenink	ORM-officer	ING (Bank and Insurance)	Cloud Consumer (bank & Insurance)
Julio Angulo, Massimo Felici Martin Gilje Jaatun Ronald Leenes Christopher Millard Nils Brede Moe Maartje Niezen Anderson Santana de Oliveira	A4Cloud A4Cloud A4Cloud A4Cloud A4Cloud A4Cloud A4Cloud A4Cloud	Karlstad University HP Labs SINTEF Tilburg University Queen Mary University of London SINTEF Tilburg University SAP	

2.2 Data collection in the workshop

We relied on Open Space Technology (Owen 2008; “OpenSpaceWorld.org” 2013) and World Café (“World Café” 2013) when organizing the workshop. Data was collected through minutes written by the stakeholders and minutes written by A4Cloud project participants who acted as observers during the discussion. We will now briefly describe the techniques and how data was collected.

2.2.1 Open Space Technology

The Open Space methodology is carefully designed to elicit maximum involvement and creativity in a constructive atmosphere. The technique is also highly flexible, because the topics discussed are entirely determined by the participants. The participants are encouraged to suggest topics that are regarded as the most important issues, which make Open Space an inventive, creative, and productive method well suited for eliciting initial stakeholder requirements.

First the workshop facilitator presented the Open Space question: *What would make you or the people you represent more comfortable in the cloud?*

Second, the rules for the Open Space session were presented:

Principle 1:	Whoever comes are the right people
Principle 2:	Whatever happens is the only thing that could have happened
Principle 3:	Whenever it starts is the right time
Principle 4:	When it's over, it's over
Law of two feet:	At any time during our time together if you find yourself in any situation where you are neither learning nor contributing, use your two feet, and go someplace else.

After presenting the question, rules and law, the stakeholders were invited to suggest topics to discuss during the open space. Only the invited stakeholders were allowed to suggest topics and to participate in the discussions. The original plan was to discuss 9 topics (3 sessions in 3 parallels). However, the limited number of stakeholders present (N=7) required adjustments in the agenda. In total 6 topics were discussed (3 sessions in 2 parallel). The parallel sessions were held in separate rooms.

The stakeholders suggested more than 6 topics. The topics ending up being discussed were chosen based on the sales pitches stakeholders held to argue why his/her topic should be discussed and following discussion on what topics were similar (could be in one session) and what should be in a separate session. After the sales pitches, the stakeholders signed up for the sessions they found most interesting, and the six most popular sessions were chosen.

The stakeholder who suggested a topic was responsible for taking notes from the discussion using a given template and flip-charts. The stakeholders' minutes provide insight into what stakeholders regard as the most important issues discussed in their session. Because only the stakeholders generated ideas for topics and were the only ones participating in the discussion, the achievement in the meeting was dependent upon the stakeholders and their collective responsibility to discuss the question being presented in the beginning of the workshop.

The stakeholder minutes varied from a detailed description on the discussion to merely short notes on a flip-chart. After the workshop the invited stakeholders who suggested a topic were asked to extend the minutes that were written on the flip-charts. Only two stakeholders wrote detailed minutes. In addition, observers from the A4Cloud project group took notes to complement the stakeholders' minutes. All minutes can be found in Appendix A. As the Open Space methodology leaves the content entirely up to the participants, the observational notes focused more on initial requirements in the form of accountability relationships, than the stakeholders minutes might do. An observation protocol was designed to minimize bias among observers (see Appendix B).

2.2.2 World Café

In the second part of the workshop the discussions were arranged according to the world café methodology, with the goal of getting feedback on the business use cases being developed in the project. The world café was organised by creating a café-like experience for the attendants, thereby creating a pleasant atmosphere for conversation. After the goal of the World Café was presented,

First the A4Cloud use cases were presented to the stakeholders by three café "table hosts". A table host was an A4Cloud project participant who had deep knowledge about one of the A4Cloud use case. The A4Cloud use cases and hosts can be found in Table 2.

The presentation of the business use cases ended with the question "what are the accountability issues in the business case?" In the main room, three tables were covered with grey paper and each of the hosts was responsible for a table and a topic. All hosts went to their tables and then stakeholders were encouraged to visit the table they found most interesting. The A4Cloud project participants also participated in the discussions during the world café.

The three hosts facilitated three discussions in parallel. Everyone participated in two discussions of 35 minutes. After the first session, the participants were encouraged to move to a new table. The second session opened with the host presenting the case and repeating the question ("what are the accountability issues in the business case?"), similarly to the first session, but also briefly sharing key insights from the first conversation. This enabled the second group to link and build on the previous ideas already discussed. Each participant was encouraged to write, doodle and draw key ideas on the flip-charts. Minutes from the World Café session were written by the hosts and can be found in Appendix A. These minutes were also sent to back to the participants for commenting after the workshop.

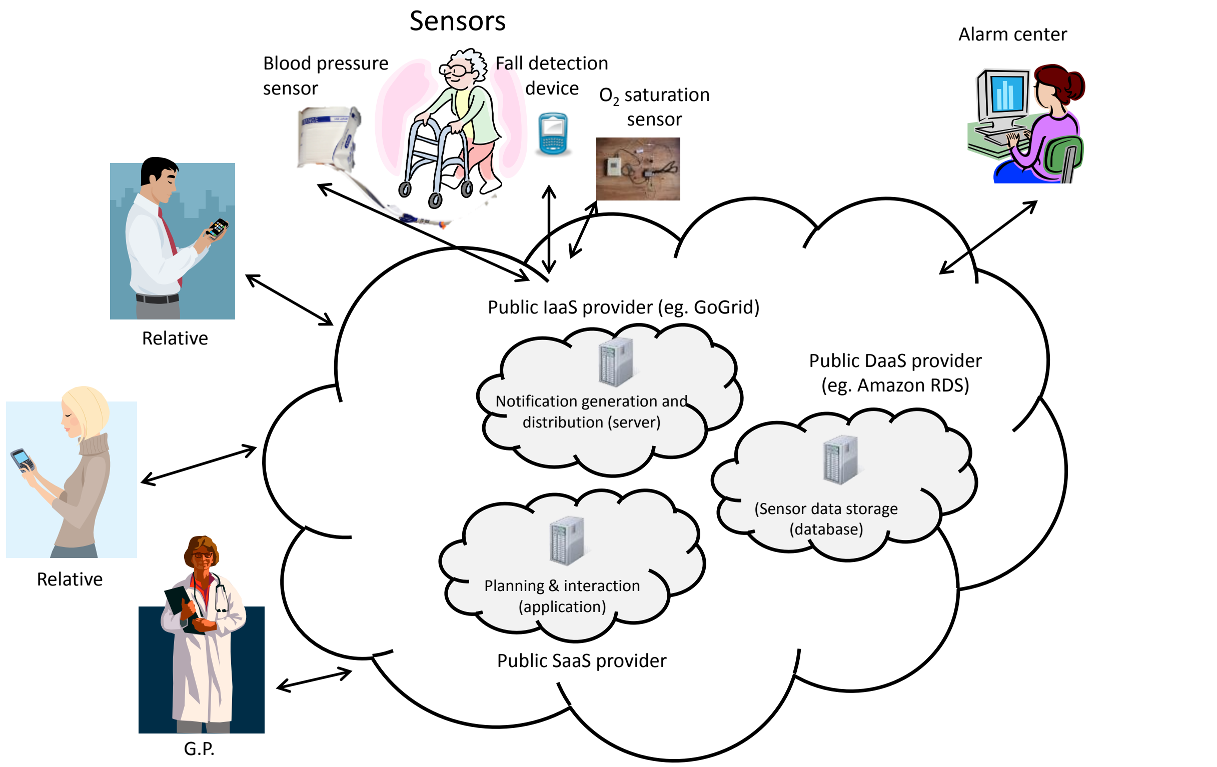
Table 2: A4Cloud use cases and world cafe hosts

A4Cloud Use Case	**Host**
Healthcare services in the cloud	Martin Gilje Jaatun (SINTEF)
Cloud-based ERP software	Anderson Santana de Oliveira (SAP)
Multi-tenant cloud	Massimo Felici (HP)

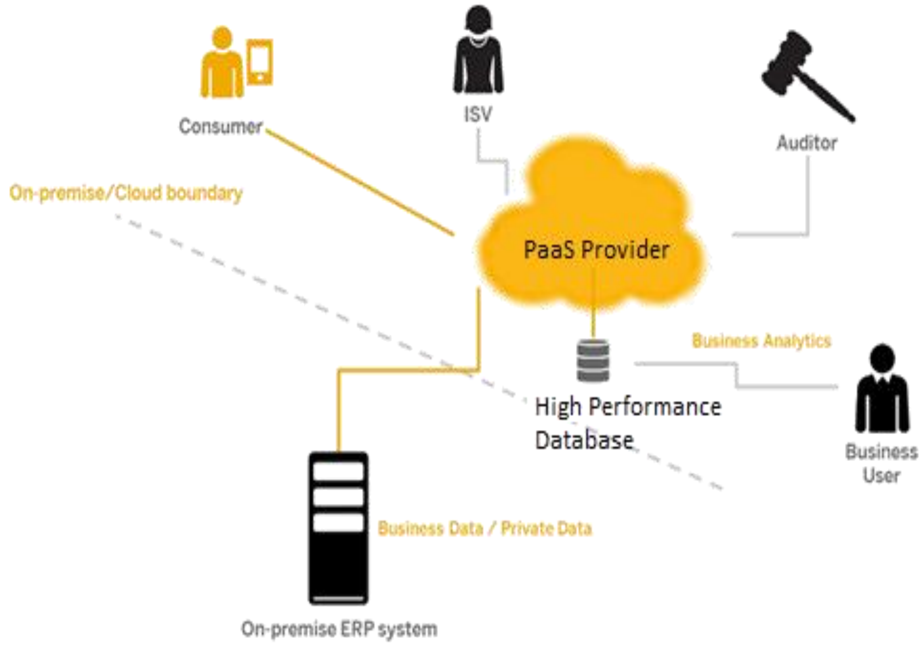
In the following, we present the three use cases as they were presented to the participants:

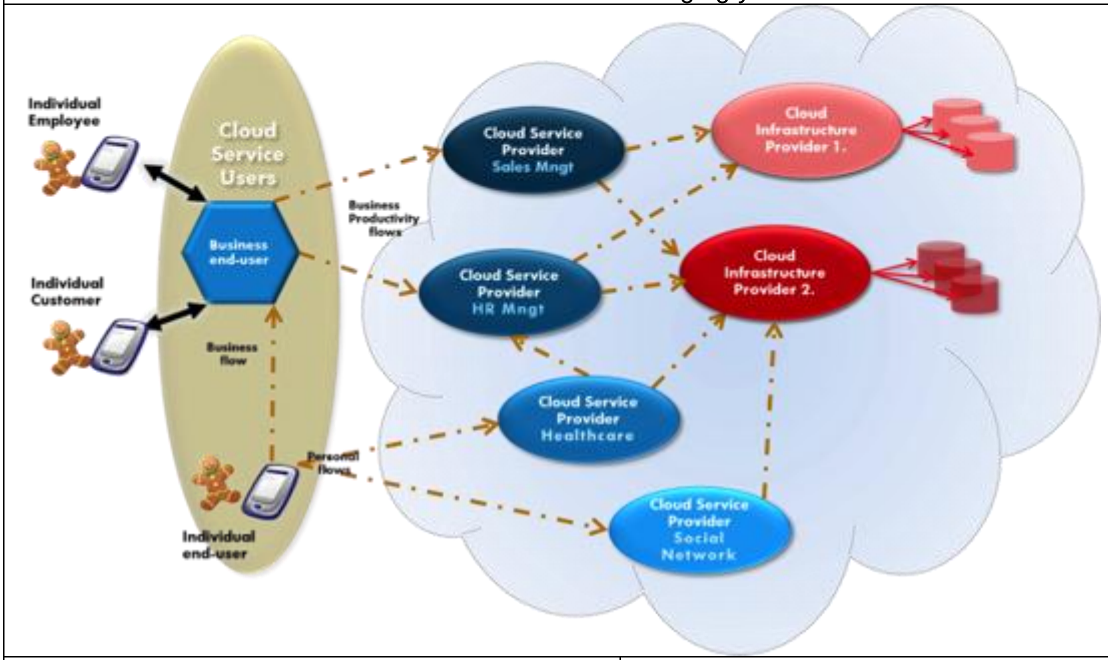
Healthcare services in the cloud

The focus of the case is "Data aggregation in the cloud", where a number of different medical sensors (e.g., blood pressure, oxygen saturation, fall detection) feed data into a cloud-based service.


Sensors
Blood pressure sensor
Fall detection device
O_2 saturation sensor
Alarm center
Relative
Public IaaS provider (eg. GoGrid)
Notification generation and distribution (server)
Public DaaS provider (eg. Amazon RDS)
Relative
(Sensor data storage (database)
Planning & interaction (application)
Public SaaS provider
G.P.

Main Actors (Roles):	**Activities/Responsibilities:**
Individual Users: elderly, relatives, friends, social workers, physicians (Data Subjects) Cloud Consumer: Trondheim municipality (Data Collector, Data Controller, Primary Service Provider) Cloud Auditor: The Norwegian Data Inspectorate (Data Protection Authority) Cloud Provider(s): SaaS, PaaS and/or IaaS providers (Data Processors)	Cloud Consumer must respect the individual users' preferences regarding PII and sensitive PII Cloud Consumer must ensure that obligations to protect the individual users' PII are respected by the Cloud providers (and all along the service provision chain) Cloud Providers must comply with SLAs
Sensitive Data Types:	**Accountability Relationships/Problems:**
Personal Identifiable Information (related to the all the individual users) Sensitive Personal Identifiable Information (related to the elderly)	Accountability relationships between individual users and Cloud consumers Accountability relationships between Cloud consumer and Cloud provider(s) Accountability related to storage and processing of sensitive data in the Cloud

<table>
<tr><td colspan="2"><b>Cloud-based ERP software</b>
The theme for the ERP use case was "Hierarchical service layering in the cloud".</td></tr>
<tr><td colspan="2">
</td></tr>
<tr><td><b>Main Actors (Roles):</b>
Individual User - Data Subject/Cloud Consumer: supermarket customer
Cloud Consumer - Data Controller, Primary Service Provider: supermarket chain
Independent Software Vendor (ISV) - Secondary Service Provider: payment service
Cloud Provider - Data Processor: PaaS provider (eg. SAP NetWeaver Cloud)
Cloud Auditor - Data Protection Authority</td><td><b>Activities/Responsibilities:</b>
Cloud Consumer, ISV - must respect that Individual Users' personal data is processed accordingly to the obligations stated privacy policy</td></tr>
<tr><td><b>Sensitive Data Types:</b>
Personal Identifiable Information from Individual Users
Credit card information</td><td><b>Accountability Relationships/Problems:</b>
How to keep the chain of accountability among software as a service providers, platform providers, and infrastructure providers</td></tr>
</table>

<table>
<tr><td colspan="2"><b>Multi-tenant cloud</b>
The theme for the multi-tenant cloud use case was "Bringing your own cloud".</td></tr>
<tr><td colspan="2">
Individual Employee
Cloud Service Users
Business end-user
Individual Customer
Business flow
Individual end-user
Business Productivity flows
Personal flows
Cloud Service Provider Sales Mngt
Cloud Service Provider HR Mngt
Cloud Service Provider Healthcare
Cloud Service Provider Social Network
Cloud Infrastructure Provider 1.
Cloud Infrastructure Provider 2.

</td></tr>
<tr><td><b>Main Actors (Roles):</b>
Individual end-user (Data Subject/Cloud Consumer)
Business end-user (Cloud Consumer/Data Controller)
Cloud Service Providers (SaaS Providers/Data Processor)
Cloud Infrastructure Provider (IaaS Provider/Data Processor)</td><td><b>Activities/Responsibilities:</b>
Business end-user is concerned with complying with relevant regulatory regimes
Business end-user is concerned with compliance throughout chains of accountability
Individual end-user accesses business as well as personal data by cloud services
Individual end-user is at the intersection between business and personal data flows</td></tr>
<tr><td><b>Sensitive Data Types:</b>
Personally Identifiable Information (PII) related to business and individual end-users
Cloud service usages</td><td><b>Accountability Relationships/Problems:</b>
Rights and obligations of business end-users with regards to cloud service usages and compliance with relevant regulatory regimes
Rights and obligations of individual end-users with regards to cloud services and Personally Identifiable Information (PII)
Accountability relationships between service providers (how accountability simplifies assurance and stewardship recognition by third parties), how some individuals could held to be accountable (in cases of security breaches or data-management non-compliances)</td></tr>
</table>

2.3 Analysing data collected in the workshop

The minutes and observation notes from the workshop (Appendix A) were analysed to identify passages of text that could be translated to accountability relationships. This was a two-step process. In the first step two researchers read all the minute text individually and coded statements relating to accountability, followed by a joint discussion between the researchers on all the coded material. The statements were documented in the following tabular format:

Statement #	Section	Stakeholder/Observant	Statement	Notes
Unique number	*Section of the workshop minutes*	*Who stated the accountability relationship*	*The passage from the minutes that resulted in the accountability relationship*	

In cases where it was difficult to judge whether a statement was relevant for the accountability focus in A4cloud, the statement from the minutes was added for further inspection. A total of 47 statements were identified.

In the second step, two other researchers read the statements and identified initial requirements in the form of accountability relationships. One example of an accountability relationship is: *"The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence that data policies have been applied satisfactorily."* The accountability relationships were documented with the following template:

Rel. Id	Accountability relationship	Accountability element (category)	Traceability to statements (Source)	Notes
Unique number	*Textual description of the requirement*	*See below*	*Trace to statement #*	

Each accountability relationship is traced to the statement it originates from. This way we provide two-way tracking of accountability relationships: which relationships stem from which statements/workshop and vice-versa.

A total of 57 accountability relationships were identified from the statements. Some statements led to several relationships, others to none. All accountability relationships were mapped according to categories developed in *Working Document: Definition and Scope* in C-2 (Siani Pearson et al. 2013), namely the **elements of accountability.** A brief description of these follows, the full description can be found in the mentioned document.):

- *Responsibility:* attribution of responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to center on accountability as the quality or state of being held to account for one's actions and an obligation or willingness to accept responsibility for one's actions
- *Liability* can be explained as an obligation (either financially or other penalty) in connection with failure to apply governing rules and/or honoring commitments; liability is an element of almost every definition of accountability
- *Transparency* describes 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
- *Assurance* is the provision of *ex ante* evidence for compliance to governing rules
- *Sanctions*: this relates to the presence of sanctions in the case of failure to apply governing rules and honor commitments
- *Observability* means that the parties can see what is happening; this is closely related to transparency, and to holding to account
- *Verification/Validation*: this is the provision of *ex post* evidence for compliance to governing rules
- *Remediation* is corrective action taken by the accountable organisation in case of failure to apply governing rules and honor commitments

Examination of the resulting statements identified relationships related to all elements of accountability.

3 Result

The main goal of the workshop was to elicit initial accountability requirements from key stakeholders. A secondary goal was to get a reality-check on the three business use cases that will demonstrate how the A4Cloud accountability approach can prevent breaches in trustworthiness, detect policy violations, and correct violations that may occur. To better understand our results we also conducted a retrospective on the workshop itself. We will now present our results.

3.1 Accountability relationships (Initial requirements)

Based on the minutes (Appendix A), statements were coded and put in a table and can be found in Appendix C. In total 47 statements were identified. 27 of these were from the minutes from the open space (22 of these again came from the observer notes and 5 from the stakeholder minutes), and 20 from the world café session.

Table 1 lists the accountability relationships that have been identified. The goal of expressing the requirements in terms of relationships among cloud stakeholders, is to highlight the need for chains of accountability in cloud ecosystems. The statements have been classified according to the elements of accountability (as described in Siani Pearson et al.): Assurance, Liability, Observability, Remediation, Responsibility, Sanctions, Transparency and Verification. Relying on such a classification will enable the possibility to discuss the dependencies between identified relationships, and to identify related groups of requirements. Identifying dependencies between the accountability relationships and defining requirements is out of scope of this report, but will be done in the next step.

Table 3: Accountability relationship

Rel. ID	Accountability Relationship (Initial Accountability Requirement)	Accountability Element (Category)	Statement #

R1	The Cloud Provider is responsible to the Cloud Consumer for data security.	Assurance;
		Responsibility;
			#1

R2	The Cloud Provider is responsible to the Cloud Consumer for implementing appropriate organizational and security measures in order to safeguard data integrity, availability, confidentiality and traceability.	Assurance;
		Responsibility;
		Verification
			#1

R3	The Cloud Provider is responsible to the Cloud Consumer for the provision of data segregation in order to safeguard control over data.	Assurance;
		Responsibility;
			#2

R4	The Cloud Provider is liable to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for compliance with data protection laws.	Liability	#2
R5	The Cloud Provider is responsible to the Cloud Consumer for the implementation of different policies tailored to the nature of data, privacy laws and needs of the Cloud Consumer.	Assurance; Responsibility	#3

R6	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence that data policies have been applied satisfactorily.	Transparency;
		Assurance;
		Responsibility;
		Verification
			#3

R7	The Cloud Provider is responsible to the Cloud Consumer for the provision of awareness-related mechanisms flagging up any policy violation (e.g. non-compliances with policies) while accessing cloud services for personal data.	Assurance;
		Observability;
		Remediation;
		Responsibility;
			#44

R8	The Cloud Provider is responsible to the Cloud Consumer for the provision of suitable audit mechanisms without compromising data security.	Assurance;
		Responsibility;
		Transparency
			#5

Rel. ID	Accountability Relationship (Initial Accountability Requirement)	Accountability Element (Category)	State-ment #

R9	The Cloud Provider is responsible to the Cloud Auditor for the provision of suitable audit mechanisms without compromising data security.	Assurance;
		Responsibility;
		Transparency
			#5

R10	The Cloud Provider is responsible to the Cloud Auditor for conducting risk analysis with the involvement of cloud experts identifying how security threats expose cloud vulnerabilities.	Assurance;
		Responsibility;
		Transparency;
		Verification
			#6

R11	The Cloud Provider is responsible to the Cloud Consumer for the provision of mechanisms for control and management over data.	Assurance;
		Observability;
		Responsibility
			#7

R12	The Cloud Provider is responsible to the Cloud Consumer for the recovery from security attacks.	Remediation; Responsibility	#7

R13	The Cloud Provider is responsible to the Cloud Consumer for the provision of mechanisms needed for the recovery from security attacks.	Assurance;
		Remediation;
		Responsibility
			#7

R14	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of the recovery from security attacks.	Transparency;
		Assurance;
		Observability;
		Responsibility;
		Verification
			#7

R15	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of the recovery from security attacks.	Transparency;
		Assurance;
		Observability;
		Responsibility;
		Verification
			#7

R16	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of provided service levels and data governance practices.	Transparency;
		Assurance;
		Observability;
		Responsibility;
		Verification
			#8

R17	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of provided service levels and data governance practices.	Transparency;
		Assurance;
		Observability;
		Responsibility;
		Verification
			#8

R18	The Cloud Provider is responsible to the Cloud Consumer that data is used for the intended purposes.	Responsibility	#9
R19	The Cloud Provider is liable to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the compliance of security mechanisms with respect to legislative regimes.	Assurance; Liability	#10
R20	The Cloud Provider is responsible to the Cloud Consumer for the implementation of suitable security mechanisms throughout the data management lifecycle.	Assurance; Responsibility	#10

R21	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of compliance with respect to legislative regimes without exposing security vulnerabilities.	Transparency;
		Assurance;
		Responsibility;
		Verification
			#10

R22	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of data segregation.	Transparency;
		Assurance;
		Observability;
		Responsibility;
		Verification;
			#11

Rel. ID	Accountability Relationship (Initial Accountability Requirement)	Accountability Element (Category)	State-ment #
R23	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of compliance of data segregation with respect to legislative regimes.	Transparency; Assurance; Responsibility; Verification	#11
R24	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of compliance with respect to legislative regimes for specific industry or public sectors.	Transparency; Assurance; Observability; Responsibility; Verifiability	#12; #29
R25	The Cloud Provider is responsible to the Cloud Consumer for the maintenance and provision of security mechanisms.	Assurance; Responsibility	#13
R26	The Cloud Provider is responsible to the Cloud Consumer for the provision of rights management on data.	Assurance; Responsibility	#14; #23
R27	The Cloud Provider is responsible to the Cloud Consumer for the provision of mechanisms specifying what operations are allowed on data.	Assurance; Responsibility	#14; #23
R28	The Cloud Provider is responsible to the Cloud Consumer for the provision of real time information on physical data storage of different types of data.	Transparency; Assurance; Observability; Responsibility; Verification	#15; #23
R29	The Cloud Provider is responsible to the Cloud Consumer for the provision of real time information on data storage location of different types of data.	Transparency; Assurance; Observability; Responsibility; Verification	#15; #23
R30	The Cloud Provider is responsible to the Cloud Consumer for the timely notification and provision of evidence of data breaches.	Transparency; Assurance; Responsibility; Verification	#16; #36; #38
R31	The Cloud Provider is responsible to the Cloud Consumer for necessary actions to data breach.	Transparency; Assurance; Remediation; Responsibility; Verification	#16
R32	The Cloud Broker is responsible to the Cloud Consumer for the provision of evidence of service orchestration.	Transparency; Assurance; Observability; Responsibility; Verification	#18
R33	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of service orchestration.	Transparency; Assurance; Observability; Responsibility; Verification	#18
R34	The Cloud Broker is responsible to Cloud Providers for the provision of evidence of service orchestration.	Transparency; Assurance; Observability; Responsibility; Verification	#18
R35	The Cloud Provider is responsible to the Cloud Consumer for the provision of data classification mechanisms supporting different data security levels (e.g. confidential or non-confidential).	Assurance; Responsibility	#19

Rel. ID	Accountability Relationship (Initial Accountability Requirement)	Accountability Element (Category)	State-ment #
R36	The Cloud Provider is responsible to the Cloud Consumer for the provision of custom-made data security levels.	Assurance; Responsibility	#19

R37	The Cloud Broker is responsible to the Cloud Consumer for the provision of evidence of non-data aggregation (or effective data segregation).	Transparency;
		Assurance;
		Responsibility;
		Verifiability
			#20

R38	The Cloud Provider is liable to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the compliance with competition laws (non-cooperation) in the provision of services.	Liability	#21

R39	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence compliance with competition laws (non-cooperation) in the provision of services.	Transparency;
		Assurance;
		Responsibility;
		Verifiability
			#21

R40	The Cloud Provider is responsible to the Cloud Consumer for the provision of the highest data security level as default.	Assurance; Responsibility	#22
R41	The Cloud Provider is responsible to the Cloud Consumer for the compliance with local legislations for international data transfers.	Liability; Responsibility	#24

R42	The Cloud Provider is responsible to the Cloud Consumer for the provision of a data migration opt-out option.	Assurance;
		Liability;
		Responsibility
			#24

R43	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of compliance with respect to extraterritorial legislative regimes.	Liability; Responsibility	#25
R44	Cloud Auditors, Regulators and Data Protection Authorities (DPAs) are responsible to the Cloud Provider for clarifying any compliance with respect to extraterritorial legislative regimes.	Liability; Responsibility	#25

R45	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of organizational practices and structures.	Transparency;
		Assurance;
		Responsibility;
		Verification
			#26

R46	The Cloud Provider is responsible to the Cloud Consumer for allowing the use of data encryption.	Assurance; Responsibility	#30
R47	The Cloud Provider is responsible to the Cloud Consumer for the provision of alternative cloud deployments (i.e. private, community, public and hybrid) and custom-made Service Level Agreements (SLAs).	Assurance; Responsibility	#31

R48	The Cloud Provider is responsible to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the provision of evidence of data collection practices.	Transparency;
		Assurance;
		Responsibility;
		Verification
			#32

R49	The Cloud Provider is liable to the Cloud Auditors, Regulators and Data Protection Authorities (DPAs) for the compliance of data collection practices with regulatory regimes.	Liability	#32

Rel. ID	Accountability Relationship (Initial Accountability Requirement)	Accountability Element (Category)	Statement #
R50	The Cloud Provider is responsible to the Cloud Consumer for asking the explicit consent for any operation on data.	Assurance; Responsibility	#33
R51	The Cloud Provider is responsible to the Cloud Consumer for asking the explicit consent every time any operation is performed on data.	Assurance; Responsibility	#33
R52	The Cloud Provider is responsible to the Cloud Consumer for revoking data consent if requested.	Assurance; Remediation; Responsibility	#34
R53	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence that revoked consent has been acted on in a reasonable manner.	Transparency; Assurance; Responsibility; Verification	#34
R54	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of data collection practices.	Transparency; Assurance; Responsibility; Verification	#35; #39
R55	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of who has the authority to investigate any policy compliance.	Transparency; Assurance; Responsibility; Verification	#46
R56	The Cloud Provider is liable (also in terms of compensation) to the Cloud Consumer for data breaches.	Liability Sanctions	#37
R57	The Cloud Provider is responsible to the Cloud Consumer for the provision of evidence of data gathered, inferred or aggregated.	Transparency; Assurance; Responsibility; Verifiability	#39

These initial requirements are based on statements from the minutes written by stakeholders and observers, and they represent what the key stakeholders found to be important. It is thus clear that as the A4Cloud elicitation work progresses; many other types of requirements from e.g. regulatory documents will be identified.

3.2 Feedback on A4Cloud use cases

The input to the World Café was on the A4Cloud use cases. This session was important not only to elicit requirements, but also to get a reality-check on the use cases. We got feedback on the usefulness of the use cases and feedback on what needed to be improved to strengthen the use cases. Based on the feedback (minutes in Appendix A), it is clear that the A4Cloud use cases are suitable for illustrating accountability challenges in the cloud. However, it was also evident that the A4Cloud use cases need to be improved. The feedback from the stakeholders will be implemented in the first deliverable from WP:B-3 (Use-case development).

3.3 Workshop retrospective

At the end of the workshop day a retrospective on the workshop was conducted. The goal of the retrospective was to capture what the key stakeholder perceived as good (“+”) and what could be improved (“Δ”). The following issues were reported by the stakeholders:

Table 4: Stakeholder feedback

What was good (+)	Suggested Improvements (Δ)

Conversation	More customers of cloud services
Outcome of discussion	More from public sector
Ideas	Improved two-page summary about the project and workshop (Objective- Problem statement-Deliverables)
Use cases were OK	More information on what A4Cloud will implement
Stakeholders can bring/introduce new topics	More structure in Open Space Session
New perspectives	More focus on requirements
Brainstorming	More specific scenarios
Fun	More in-depth workshops
A diverse set of stakeholders were present	A main room with windows would have been better

The stakeholders felt that the discussions and conversations were very good, and that the workshop generated a lot of good ideas. The stakeholders introduced several new and good ideas and new perspectives on. The session was perceived as fun and engaging and one reason was the diverse set of stakeholders.

While the workshop was seen as a success from the stakeholders, it was also commented that more cloud customers should have been present, especially from the public sector. The stakeholders also claimed that they should have been given more background information about the project, to better focus the discussions and better contribute to the goal of the workshop. However, before the workshop it was decided not to give the stakeholders too much information about the accountability aspects because we were afraid of influencing their understanding of the concept of accountability. The lack of background information was one reason for why some felt the open space session was lacking structure. In the world café session, the stakeholders felt that the use cases were interesting; however they wanted a more specific description of them. Finally it was commented that the airport hotel did not provide the most exciting and creative environment for such a workshop.

4 Discussion

The previous chapter lists the initial requirements in the form of accountability relationships, derived from the first stakeholder workshop in the A4Cloud project. To summarize the results briefly: based on the minutes from the workshop we identified 47 requirement related statements, and from these statements we identified 57 accountability relationships (initial requirements) related to Assurance, Liability, Observability, Remediation, Responsibility, Sanctions, Transparency and Verification.

These are initial requirements from a few key stakeholders, and the results will create a basis for future work in the A4Cloud project, implying that they need to be further processed. In addition, the accountability relationships have to be prioritized, grouped, conflicting relationships need to be solved, and they need to be described for all types of stakeholder groups. We will now discuss the relationships we identified, and the method used for identifying them.

4.1 Accountability Relationships

As the Open Space methodology left the content entirely up to the participants, the results from the first part of the workshop (which comprised 27 statements) are drawn solely from the stakeholders. In the World Café sessions, which identified 20 statements, project partners could interact directly with the stakeholders. This created a synergy between the stakeholders' domain knowledge and the technical expertise of the project partners. From the 47 statements 38 led to accountability relationships (initial requirements).

The accountability relationships identified during the workshop have been categorized into one or several of eight accountability elements identified in the project; Assurance, Liability, Observability, Remediation, Responsibility, Sanctions, Transparency and Verification. When the accountability relationships are processed further to create more detailed requirements, we expect to have a wider coverage of all the accountability elements identified in the project.

The accountability categories were not mentioned to the stakeholders in order not to influence their perception of accountability. Assigning accountability relationships to the accountability categories was an iterative process that involved several researchers. This ensured that the selection was based on consensus. From analysing the output of the workshop we argue that the workshop succeeded in eliciting relationships from all accountability categories.

4.2 Methodological reflection

In retrospect, we believe that our stakeholder selection and invitation process was suitable for the A4Cloud project. We did, however, underestimate the complexity of finding a date that suited most stakeholders and the challenge of making stakeholders prioritize such a workshop. We started out with 75 potential stakeholders for the workshop, of which only 7 ended up participating after 5 stakeholders for various reasons cancelled during the last 24 hours. Since we had hoped for 15-20 stakeholders in the workshop, the invitation process should probably have started with a higher number of potential stakeholders. The attendees turned up because they knew the project partner who invited them. Since the project partner nominated everyone they saw as a potential stakeholder from their own network, we argue that it was difficult to increase the initial list of potential stakeholders. All invitations sent to open groups (e.g. LinkedIn) did not generate any attendees.

Looking at the list of stakeholder representatives, it seems fairly balanced, with 3 DPAs, 1 infrastructure provider, 1 Enterprise Cloud Consumer and 2 Cloud Providers. However, it was noted that it would have been helpful to have more cloud customers present, including stakeholders from the public sector. Furthermore, end-user representatives were not in attendance, so that aspect was not covered in any detail during the workshop. End-users will be included in future workshops.

One reason for the low number of stakeholders is the forthcoming local workshops in the project. Stakeholders that will participate in these local workshops were not invited. The local workshops will also include more stakeholders from the public domain. A lesson to be learned for future workshops would be to plan for a 10-20% acceptance rate, and ensure that sufficiently many invitations are sent to still reach the desired attendance goals.

When inviting the stakeholders, little information was given on the concept of accountability. The goal was to not influence the stakeholders with our own perceptions of accountability. In retrospect, the invited stakeholders could have received more information, both about the project, and about how the results from the workshop would be used. However, while the stakeholders became a bit confused as a result of our strategy of not influencing the attendees, our results show that we identified requirements covering all important aspects of accountability.

When reflecting on the method for generating discussions which led to initial requirements, we argue that the method seems to be effective. The stakeholders decided themselves what to discuss (Open space) and which discussions to take part in (world café), and through this strategy we ended up with 57 accountability relationships. The session was also reported as fun, interactive and interesting. The conversations and discussions were lively, and generated a lot of new knowledge both for project partners and invited stakeholders.

The achievement in the meeting depended on the attending individuals and their collective responsibility to discuss the question that was presented in the beginning of the workshop. Consequently, the results in this document are based on what each person shared, and the outcome is based on what the participants created. One limitation of our results is therefore related to which stakeholders were present.

5 Conclusions

5.1 From relationships to initial requirements

This report has documented how 57 accountability relationships have been elicited from the first stakeholder workshop in the A4Cloud project. The accountability relationships have been identified by analysing minutes from discussions initiated, led and decided by the stakeholders themselves. The accountability relationships will serve as a basis for the ensuing work of identifying accountability requirements for cloud and other future internet services. The identified relationships cover the important accountability elements identified by WP:C-2.

5.2 Future work

The results from the workshops will be used in an iterative process to build and expand the A4Cloud requirements base, regularly fed back to the other A4Cloud work packages developing accountability mechanisms, tools and use case instantiation.

The results from the workshop will also give input to the local workshops that will be organized in the project. The advantages of having local workshops are that stakeholders save time and resources, it is easier for them to communicate in their own language and it is easier to understand the culture of organizations in their own country. Local workshops will make it easier for stakeholders to discuss with each other both language- and content-wise.

The results (accountability relationships) and lessons learned on how to involve and elect requirements from stakeholders in a workshop will also give important input to the remaining three workshops that will be held on a European level. These three workshops will be run at roughly six-monthly intervals, building up a picture of evolving attitudes and concerns. The next workshop (WS2) will focus on risks (events, consequences, and uncertainties), identifying predictive risk mitigation measures through participation of different stakeholders, considering different contexts. The third workshop will be organised in the context of the use-case domain chosen for instantiation, and the last workshop (WS4) will be an interdisciplinary workshop intended to cover any gaps not resolved by the preceding workshops. Input from the external environment and the implications of changes on the project horizon will influence the scope and focus of all the workshops, as will the challenges and insights identified in the other WPs. The workshops will rely on interactive methods such as focus groups and open space discussions.

Because it is important to continue involving the stakeholders already introduced to the project, a second level of elicitation will follow the workshop described in this document and each of the following workshops, using questionnaires and in-depth interviews designed for participants that have already been introduced to the project.

6 References

“OpenSpaceWorld.org.” 2013. Accessed March 11. http://openspaceworld.org/.

Owen, H. 2008. *Open Space Technology: A User’s Guide*. Berrett-Koehler Publishers.

Siani Pearson, Daniele Catteddu, Massimo Felici, Giles Hogben, Christopher Millard, Nick Papanikolaou, Daniel Pradelles, and Chris Reed. 2012. *A4Cloud Milestone Report MS:C-2.1 “Scoping Report and Initial Glossary.”*

Siani Pearson, Daniele Catteddu, Massimo Felici, Giles Hogben, Christopher Millard, Nick Papanikolaou, Daniel Pradelles, Chris Reed, and Vasilis Tountopoulos. 2013. *A4Cloud Milestone Report MS:C-2.2 Initial Description Framework Report*.

“World Café.” 2013. Accessed March 11. http://www.theworldcafe.com/.

7 Glossary

A complete glossary for the project can be found in **WP:C-2 (Glossary).** This section briefly describes the concepts and terms that are relevant to DB2-1.Some of these are also unique to this deliverable and are not described in the project glossary.

Term	Definition
Accountability	There are many definitions in the main glossary, the short one is “Responsibility of an entity for its actions and decisions.” The working definition of accountability in A4Cloud is based on the Elements of Accountability defined below.
Accountability Elements	See Elements of Accountability
Accountability relationships	Initial high-level requirements based on stakeholder statements from the workshop. Will later be refined to generate more detailed accountability requirements.
Assurance	Assurance is the provision of ex ante evidence for compliance to governing rules
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
Cloud Infrastructure Provider	The provider of the collection of hardware and software that enables cloud computing.
Cloud Service Provider	An organization that provides and maintains delivered cloud services.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties
Elements of Accountability	A set of concepts that collectively define our notion of accountability. A4Cloud has identified the following elements of accountability: Responsibility, Liability, Transparency, Assurance, Sanctions/Holding to account, Observability, Verification/Validation, and Remediation
Liability	Liability can be explained as an obligation (either financially or other penalty) in connection with failure to apply governing rules and/or honoring commitments; liability is an element of almost every definition of accountability
Observability	Observability means that the parties can see what is happening; this is closely related to transparency, and to holding to account
Open Space Technology (OST)	A workshop technique recommended for complex situations involving a diverse participants and the need for a quick decision making
Remediation	Corrective action taken by the accountable organisation in case of failure to apply governing rules and honor commitments
Responsibility	Attribution of responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to center on accountability as the quality or state of being held to account for one’s actions and an obligation or willingness to accept responsibility for one’s actions

Term	Definition
Retrospective	In software development, a retrospective means a meeting that is held at the end of a project (or completed part of an ongoing process) in order to discuss the successful parts of this effort, and the parts that need improvement.
Sanctions/Holding to account	This relates to the presence of sanctions in the case of failure to apply governing rules and honor commitments
Stakeholder	In A4Cloud, a stakeholder means a person, group or organization that affects or can be affected by the A4Cloud project results.
Transparency	Describes 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
Verification/Validation	This is the provision of ex post evidence for compliance to governing rules
World Café	Drawing on seven integrated design principles, the World Café methodology is a simple, effective, and flexible format for hosting a large group dialogue. See http://www.theworldcafe.com/method.html

8 Appendix A: Minutes from the workshop

The invited stakeholders created the following schedule:

	Room 1	Room 2
Session 1	Data security as a means to safeguard data protection	Not using general term Cloud
Session 2	Education	Transparency
Session 3	Guarantees	Make international data transfers within the cloud easier

In the following we will present the minutes from the topics discussed.

8.1 Data security as a means to safeguard data protection

Notes from the stakeholders:
After having identified data security as major factor to make us feeling comfortable with cloud computing, the group came to following conclusion:

- All aspects of data security for IT systems are valid and should be taken into account for cloud computing. In general, data security shall be implemented through appropriate organizational and security measures in order to safeguard data integrity, availability, confidentiality and traceability.
- In the following, the group firstly focused on some specific and important risks for cloud computing. i.e. a) malicious attacks, b) data leakage, c) violation of privacy laws and regulations by the cloud service providers as a result of non-adequate organizational and technical security measures.
- As a second step, the group identified the challenges to implement appropriate organizational and technical security measures. Such challenges are: a) In order to safeguard control over data and compliance with personal data protection laws data segregation is often mentioned as a requirement. However, this seems difficult to achieve in cloud computing services. b) Another challenge is the implementation of different policies – according to the nature of the data, the privacy laws and the needs of the clients. HP “sticky policies” are mentioned as an example of good handling. c) Data encryption during the processing phase is another challenge and further research is necessary. d) Suitable audit mechanisms which do not present an additional security risk, as for example if every client may audit the cloud service provider’s systems and applications.

Observer minutes:
The discussion topic, Data security as a means to safeguard data protection, was articulated by the stakeholders as a risk analysis exercise. The topic leader coordinated the discussion addressing the main points involved in a general risk analysis process. Firstly, they acknowledged that risk perception differs depending on viewpoints – personal vs. company perspectives. Then, the stakeholders followed a general risk analysis (see figure below) consisting of: (1) threats identification, (2) impact assessment, (3) perception assessment, and (4) identification of mitigation solutions (or limitations in current technologies).

The first step (1 threats identification) involved the identification and discussion of potential threats in the cloud (examples of attacks are: manipulating data/processes, viruses like malware and Trojan virus, etc.). The stakeholders identified threats that were common to Information and Communication Technology (ICT) but not specific to the cloud. However, the cloud or the complexity of sophisticated attacks seem to pose other challenges like response time to threats (it could take months before recognising an attack and being able to address it) and assessing their impacts (the scale and complexity of the cloud makes it difficult to assess the impact of threats). Risk analysis would benefit from involving cloud experts identifying how security threats expose cloud vulnerabilities.

The second step (2 impact assessment) concerned the discussion on impact assessment. Overall, it was acknowledged that due to the nature of the cloud it is difficult to perform impact assessment. From a company viewpoint, one the main concerns is how attacks would damage its reputation. The third step (3 perception assessment) discussed how risk is perceived by cloud stakeholders. The stakeholders pointed out that most security threats are already known. Such threats concern ICT in general. However, it seems that the cloud has changed the perception of those threats (and their risks). Cloud stakeholders are more and more aware of security threats. However, they feel a lack of control due to the fact that the cloud implies a different form of control and management over data. Moreover, it seems that recovering from security attacks is more difficult in the cloud than in other conventional ICT. For instance, once data leakage occurs it is difficult to recover from it (i.e. data are now open in the cloud). Another relevant aspect of risk perception in the cloud is concerned with trust. It seems that so far there are no mechanisms to distinguish among cloud servicers. Therefore, cloud stakeholders have no other option but to trust all actors in the cloud.

The final step (4 identification of mitigation solutions, or limitations in current technologies) concerned the discussion of security mitigations and mechanisms. Three main topics emerged from the final discussion on security mitigations. The first one is that data and purposes should be tightly linked together (in order to mitigate the risk of data being used for different purposes). Mechanisms (e.g. sticky policies) that link data and policies together seem to address such risks. The second point was concerned with emerging conflicts among the legislative regimes and security mechanisms (e.g. data encryption limits the ability to process data). Although some security mechanisms address specific threats, it is difficult to adopt them throughout the data management lifecycle. Moreover, complying with legislative regimes may require releasing critical information that might expose security vulnerabilities. The third point concerned with how data is managed, classified and stored. For instance, a strong accountable logical segregation of data separating personal sensitive data from ‘meta-data’ would enable compliance mechanisms with respect to relevant legislative regimes.

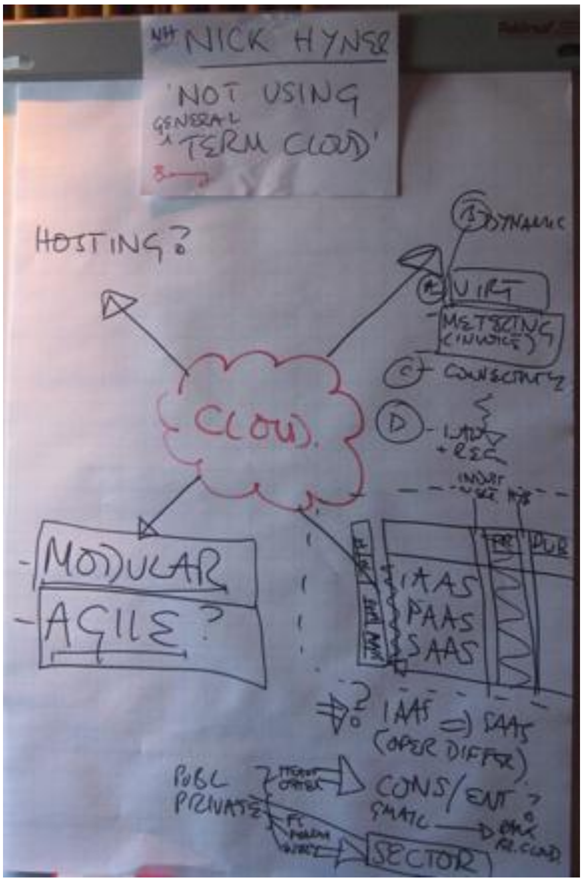
8.2 Not using general term Cloud

There were no minutes from the stakeholders on this topic, apart from the flip-chart drawing below.

Observer minutes:
‘The Cloud’ is more a marketing concept than a feasible notion from a legal and research perspective. This is the departing thesis for the discussion. A consequence of The Cloud as a marketing concept is that it has become a container concept, in which all cloud-computing and related activities are ‘stored’ without addressing its proper boundaries and limitations. This is a fundamental concern for the participants, who therefore propose to take a critical look at what the cloud is, and what correct terminology of concepts would be in discussing the cloud.

The Cloud presupposes that one regulation would fit all categories within cloud computing, yet the opposite is true. There should be distinct regulation for IAAS, PAAS and SAAS, as they have different needs due to their inherent differences. The characteristics of cloud-computing differ by: a) virtualization (metering), b) dynamics, c) connectivity and d) categorization. Regulation overlays are different per sector, the categorization of private or public sector covers a first distinction for a more modular approach. Within the public sector a distinction can be made between health and other public sectors. The private sector is split up in Pharma, Energy and Financial Services. Other aspects allowing for the definition of different modules are: commercialization (consumer / enterprise), and whether encryption is in place or not.

Requirements for the A4Cloud research project would be to approach accounta-bility in The Cloud in a modular and agile way. Cloud computing cases to explore should be identified by module; subsequently they should be worked on in an agile way. This will enable the different cloud categories to become more secure and with trust. In conclusion the participants advise to see where there is a chance to change and start there.



8.3 Education

Notes from the stakeholders:
The perception what cloud is and what not, what is possible and what not and specifically the spread of FUD is currently immense at consumer site. There are two important arguments that can convince consumers that it is even in their interest in entering the cloud.

1. Shift the line of defence

Like it or not, the future means that you have to deal with communication into the internet and providing data there. This introduces customers, partners and providers directly in front of your firewall. With those also criminals, hackers, and fraud will access it. How long does your firewall withstand this?

Cloud providers are in many cases some of the biggest software companies in the world and therefore are specialists in protecting themselves. Just numbers make easily clear that the security department of for example SAP outnumbers the complete IT staff of most of the midrange companies in the world. While this alone is not a guarantee for success, the setup for security processes and regular participation in the security community just enlarges the probability for success.

By using applications that are sitting in the cloud the line of defense moves to the firewall in the cloud and will be more secure in most cases just because more resources are protecting it. Whether the actual data is also sitting in the cloud or is accessed through a secure VPN tunnel from the customer backend is less important for this scenario.

However, for private computing it may be even an argument to put data into the cloud as it is in a controlled state there and access to it is more secured than on private computers, when security is depending on security knowledge of the user himself.

2. Insider Threat mitigation

Data protection very often is a matter of knowing about its value. And who knows best about this value in companies? Employees of course. While it is bad style to project a matter of distrust, it is also good style to not stress their sense of morality too much. Profitable crime with low risk is a matter that made many angels fall.

Conclusions from discussion:

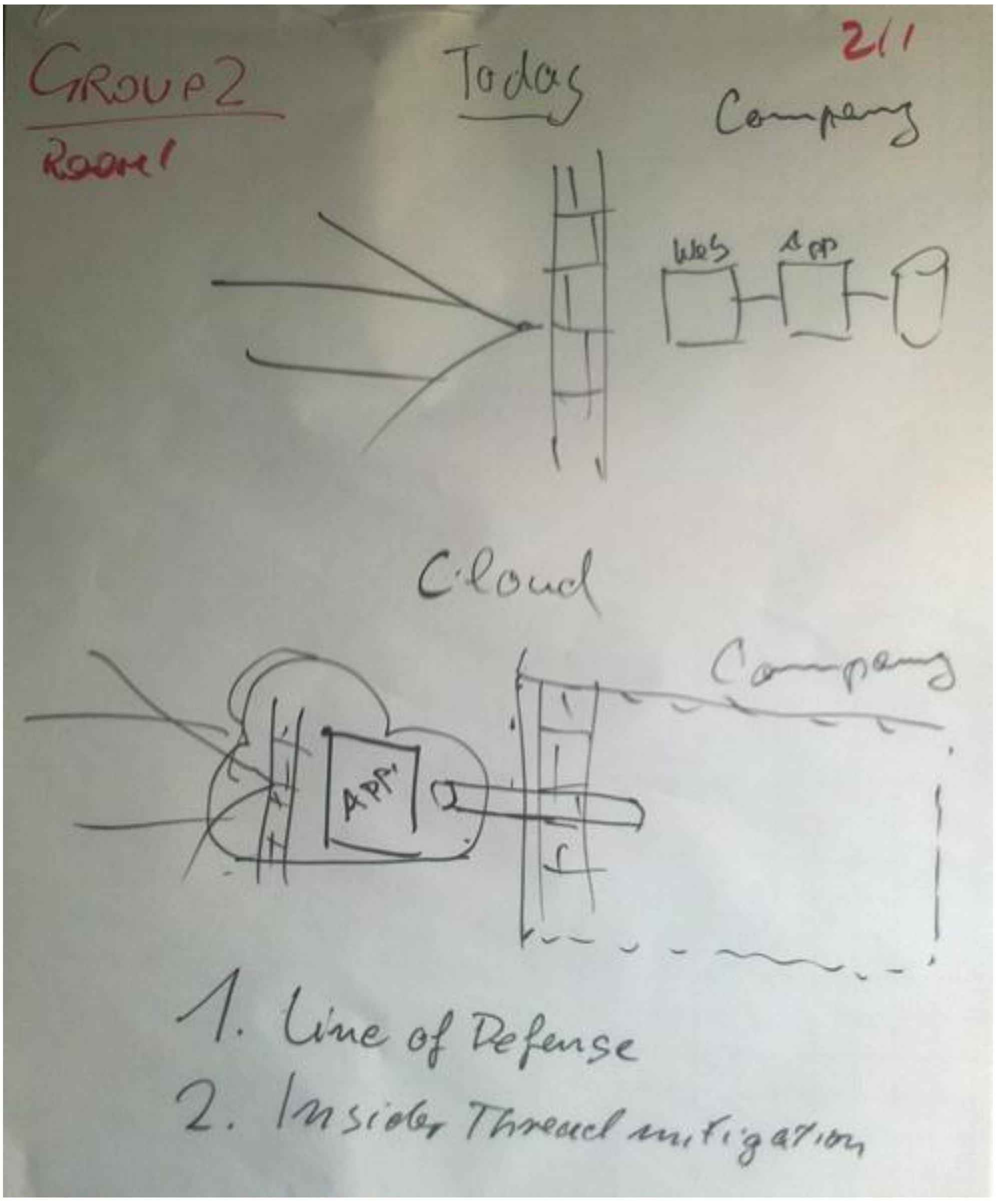
The facts were undisputed, but even in the expert group perception of cloud services were diverted. So it was expected that cloud would be a more distributed concept than it is today and that provider would buy their resources at other services that may be cheaper. Besides that this currently still is a technical challenge experience says that such a complex “chain of responsibility” will be avoided by providers due to inherent risk.

Observer minutes:
The main argument of the discussion topic – Education: uncomfortableness (or uncomfortability) with cloud security seems to be a biased position – was that cloud security concerns seem to be unfounded. The main argument consisted of the analysis of how cloud shifts security responsibilities by delegating them across company boundaries. The analysis discussed two main aspects of cloud security (see figure above): (1) Line of defence, (2) Insider threat mitigation.

The first aspect of cloud security was concerned with the position of the ‘line of defence’. Proprietary ICT requires company to maintain their security mechanisms (e.g. firewall), which might concerned mainly with defending sensitive data from external attacks. Cloud services enable companies to move the ‘line of defence’ externally to the company, far away from internal critical assets. This deployment of the line of defence in the cloud benefits from security expertise offered by cloud providers. Therefore, it would require maintaining limited resources dedicated to security making cloud services cost-convenient over the medium-long term. However, it is unclear whether or not moving the line of defence in the cloud involves a shift in security responsibilities across company boundaries. The second aspect of cloud security was concerned with how cloud services mitigate the risk of insider threat. Managing sensitive data requires a clear allocation of rights – Who can use data? What can be done on data? Who knows the value of data? Proprietary ICT and local data storage and manipulation expose companies to the insider threat (e.g. unauthorised data manipulation and exploitation). Cloud services mitigate such risk because data manipulation and exploitation becomes difficult without having insider data or business knowledge (data are ‘meaningless’ without their business contexts). The two aspects of security discussed during the session provide an argument supporting (to a certain extent) the thesis that security concerns in the cloud are unfounded. It is possible to register a problem shift from security (expertise and mechanisms) to trustworthiness. That is, the main problem is not to devise security mechanisms, but to enhance trustworthiness in the cloud. Accountability would be a convenient concept to address the trustworthiness problem in the cloud. For instance, it would enable awareness across chains of responsibilities (even from a legal perspective).

8.4 Transparency

There were no minutes from the stakeholders on this topic apart from the flip-chart drawing below.



Observer minutes:
Transparency in cloud computing is a major concern for both end-users and providers. In this session the case discussed is the banking industry, which leads to a fruitful exchange of knowledge and thoughts on the need for transparency of (end-) users and technical possibilities.

The banking industry is challenged with increasing accountability requirements demanded by regulation. In fact, multiple security policies apply to the banking sector. Depending on the risk level, banking industry becomes more demanding on control and the security requirements the cloud-computing services should meet. In practice this means that, from a banking industry perspective, the use of a private cloud is ok, but the use of public clouds is not. Nonetheless, if banks are going to use public clouds examples of banking sector specific requirements are: real time monitoring (control) and the division of data on different physical machines though with clear whereabouts of location depending on the type of data stored (data segregation). The feeling of ownership of the data is strong and risk oriented. As soon as there is a data breach, banks need to be notified to take necessary actions.

A concern of these high standards and demands of the banking industry is the developmental costs to meet these requirements. Users of cloud-computing services can define what they need and technology can develop such mechanisms. Yet, mixing technological possibilities and the level of needed security might lead to commercial problems. Developing in-house clouds might become cheaper, and the opportunity of the cloud is missed. A requirement for accountability in the cloud therefore should be that collaboration is needed within sectors. If such collaboration is lacking, all kinds of private in house clouds will be developed. However such collaboration is only possible on the same risk levels. Nevertheless, the banking industry is keen on collaborating since they rather are confronted with one audit, than ten different audits.

8.5 Guarantees

There were no minutes from the stakeholders on this topic, apart from the flipover drawing.

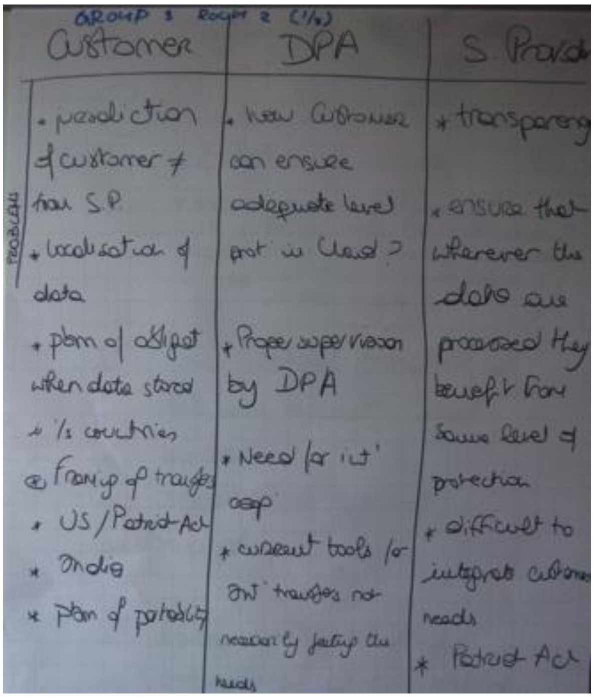
Observer minutes:
The discussion built around the concept of a “cloud-of-clouds”, meaning that the data is distributed in a number of different clouds that are orchestrated in some way. In other words, companies or users employ several cloud providers for their purposes. The orchestration of cloud providers is seamless to the users, but at the end there was a consensus on the need for an entity that would be responsible for this orchestration. Within this cloud-of-clouds concept, the participants also discussed the concept of horizontal and vertical clouds. An example of horizontal cloud-of-clouds could be a govern-mental institution adopting clouds for the education, health or financial services; whereas an example of a vertical cloud could be Dropbox storing data on Amazon cloud service. The stakeholders also saw the need of classifying data according to their level of security. Customers should be able to decide what piece of data can be classified as critical or non-critical. Costs and other factors might be dictated by these labeling of the data (e.g. critical data would require high level of security, thus cloud service providers could charge an expensive fee for handling and storing such critical data).

From a perspective of privacy, having a cloud-of-clouds environment would prevent any single cloud provider to access all customer data. Since data is distributed across different clouds, cloud providers would be unable to make sense of customer data, unless all of them ‘collaborate’. This concept was called during the discussion as “knowledge-splitting”. Splitting the data in this way blurs the concept of personal data, since the data processor would be unable to know what data is personal. The following sketches depict some of the concepts discussed.

An example was given about the possibility of blurring an image, so that the bits of the image would be distributed among the different clouds. These clouds would be unable to see the real contents of the un-blurred image, unless the cloud providers storing the different image’s parts ‘collaborate’ (that is, pass information to each other) with each other. Splitting the data, would also mean that you would need all of the cloud services (or at least some proportion of them) running in order to compile the data together during a data request from the user. Also, it brings some other legal issues concerning international regulations of data handling. The more cloud providers there are the more difficult is to determine what represents personal data. The accountability for each cloud provider has to be determined (for instance, by requesting log files), but this could be quite expensive – Is it possible to have some intelligent tool that makes complex situations reduce what the cloud providers have to prove? For instance, one of the things that they have to prove is that they are not communicating in some way. The stakeholders also deemed as important the ability of the customers or users to tag their data. By tagging the data customers would be able to distinguish what is critical or non-critical data. If there is no tagging of data, then all data should be treated with highest security, which is not optimal or efficient. To be able to guarantee security of the data is important. If a customer doesn’t feel or see a good security solution for the storage and processing of data, they will not go for that cloud service. At the end what is desired is: “maximum accountability, minimum risk at the least cost.”

8.6 Make international data transfers within the cloud easier

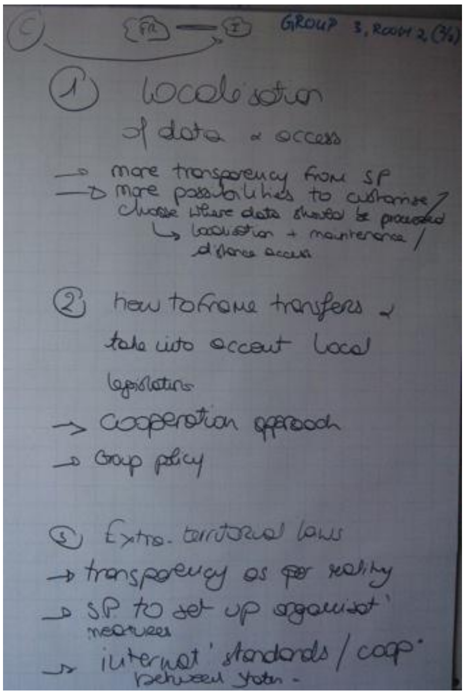
There were no minutes from the stakeholders apart from the flipcharts below.



GROUP 1 ROOM 2 (1/2)

PROBLEMS

Customer	DPA	S. Provider
• prediction of customer ≠ than S.P	• how Customer can ensure adequate level prot in Cloud?	* transparency
* localisation of data		* ensure that wherever the data are processed they benefit from same level of protection
* pbm of oblig. when data stored in ⅓ countries	* Proper supervision by DPA	
⊕ framing of transfers	* Need for int' coop	* difficult to interpret customer needs
* US / Patriot Act	* current tools for int' transfers not necessarily fitting the needs	* Patriot Act
* India		
* Pbm of portability		



© {FR} — {I} GROUP 3, ROOM 2 (2/2)

① localisation of data & access

→ more transparency from SP

→ more possibilities to customise / choose where data should be processed

↳ localisation + maintenance / different access

② how to frame transfers & take into account local legislations

→ cooperation approach

→ Group policy

③ Extra-territorial laws

→ transparency as per reality

→ SP to set up organisat' measures

→ internat' standards / coop' between states -

Observer minutes:
The central topic of this session was how to make inter-national data transfers within the cloud easier. In order to answer this question the participants first addressed the problems and concerns they have regarding international data transfers within the cloud from the perspectives of the customer, the data protection authority and service providers. Solutions to these problems should be discussed in a second round. As the notes on the flip-over provide a good overview of the discussion of problems, this summary focuses on the second part of the discussion, which due to time limitations was short (five minutes) but dense in information.

Control is seen as a major aspect of sustaining accountability. This becomes evident in the three solutions discussed: localization of data, framing international transfers, and extraterritorial law. First, localization of data, access and maintenance are discussed. They are seen as important requirements for accountability in the cloud (and closely connected to the discussion of data portability). All participants stress the importance of a tool that visualizes the exact location of data centers and who has access to the data. Such tool can automatically lead to more customization of the cloud-computing services provided. The challenge than becomes the negotiation between customers and providers on the contracts.

Second, framing the international transfers should take into account local legislation. When responsibility is left to the service providers, control might be lost. Solutions can be found in a cooperation approach and / or a group policy. A requirement could be to allow for an ‘opt out’, the option to leave. The participants remark that in the media the patriot act seems the sole focus in privacy and data protection discussions, but other countries such as India should also play a role in the discussion of framing international transfers.

Third extraterritorial laws should be (further) developed. These laws should envision that transparency needs are different per reality. Service providers might be made accountable for setting up organizational measures that allows them to show their transparency. For example, a service provider might create a company without an US identity; if certain services have an US identity they can be excluded from certain activities.

The participants conclude there are no perfect solutions, yet certain requirements for improved control can be developed. Requirements elicited from this session are: A) The DPA’s supervision should be made easier and also become more valued (by regulation?) since there’s a need for centralized security with a strong management. B) There’s a need for international cooperation and development of tools supporting transfers to third countries. C) Protection should be made more practical without decreasing the level of protection.

8.7 Topics not discussed (not prioritized by the stakeholders)

- If it was based on: 1) Open source, 2) Open standards
- Accountable data portability

8.8 World café

The minutes from the world café session were written by the café hosts.

8.8.1 Healthcare

The first group concluded that for this scenario to be relevant for the A4Cloud project it would need to include a variety of sensors and not only medical sensors ("Runkeeper" was mentioned as an example). It was opined that everyone benefits from increased sharing of data, and that this also increases the value of each individual sensor. In Runkeeper you can store tracks of previous runs, others (presumably your "friends") can see your tracks, and maybe compete with your results etc. In the general case, there will be one actor who provides data, and another actor (maybe the same) who controls what happens to it.

The discussion digressed into whether social media is out of scope for the project, and it was opined that the European Commission doesn't want A4Cloud to build a Facebook competitor. It was further opined that Facebook doesn't care what is decided in Europe; they will do their own thing anyway. However, it was suggested that US providers will comply "enough" to do business in Europe (but maybe no more than minimum). More regulation was not seen as a solution to this. Furthermore, it was discussed whether "perceived barriers" represented something that could have a technological solution, and the consensus seemed to be that perceived barriers may indeed be real in some cases.

Round 2:

The second group was generally positive to the business case, and it was stated that this can save Europe a lot of money. One challenge is that the data controller must declare ahead of time for what purposes the data collected will be used, which means that other uses cannot be decided at some later time. Furthermore, the consensus among European Data Protection agencies seems to be that (Sensitive) Personal Data remains so, even when encrypted (unlike in some military organisations, where encrypted data is treated as unclassified).

Clouds will have specific risks, which must be met when deploying any system. Transparency and security must be provided. We may see the emergence of sectoral clouds to handle different requirements, notably for energy, financial service and health.

Some providers are offering services where the end-user keeps the encryption key, but it is not clear how this could be employed when sharing data with other actors.

8.8.2 Cloud-based ERP software

Round 1:

One of the first questions raised was what was specific to the cloud in this use case? The data protection issues would be shared with many real-world use cases where no specific cloud infrastructures are necessarily involved, basically the collection of personal data, and their processing by mutual parties that would perform data mining with diverse purposes on the data. A similar use case was brought up that would adjust SLA and contracts to whether a given SaaS user would like to be the exclusive data controller (more expensive), or it would agree to share their customer personal data with further companies and pay less.

The importance of the use case was highlighted when all mentioned that it was needed to have reasonable means to justify the data collection to data protection authorities and to demonstrate compliance.

Comparisons were made with respect to that in Germany and France. The outcome of the first round, if we can point one out, it that it is necessary to further explicit the cloud service provisioning chain, and to indicate how this impacts the already existing processes for demonstrating compliance to data protection.

Round 2:

The second group asked several questions regarding the Cloud-based ERP software use case. They were again mainly concerned about personal data processing. They have also asked questions about the Adjustable SLA use case explained during the first round. The conclusion was that the issues related to data protection compliance are not really new, but that the emergence of the cloud contributed to put those questions under the spotlight, and that accountability can be a game changer when it comes to increase trust in the cloud.

In addition, the group discussed the need for explicit consent of the users regarding data portability, withdrawal, etc. A suggestion was made that consent might not be collected just once, but every time data is released or, in the case of this SAP scenario, every time a supermarket's loyalty card is used. Consumers should be made aware that once consent is given, it is very difficult to revoke in practice. For example, I can give consent to display a picture at one point and then revoke that consent; however, that picture could have been already sent to third parties, or used by other users, etc. Thus, services have to reliably prove that they have at least attempted (or take some action) to revoke the customer's data is the customer has requested to do so.

Also, a discussion was made about the possibility of the different services involved in the scenario to feed a database of users' profiles. For the purposes of profiling, databases cannot be anonymized, but they can be pseudonomize. The group mentioned that there are situations in which keeping a profile can be very risky for the individual.

Regarding data breaches, the group discussed the need for notifying the data subjects about breaches to their data (e.g. who should be notified? how much information should the data subject be provided with?, etc.). The question was raised on what kind of compensation would consumers get in case of a data breach, and who is responsible for what? The group mentioned that responsibility would depend on the contracts between the different parties. Also, users should be notified with detail information about the breach to their data, since they might require taking some action in order to minimize further consequences of the attack. However, providing detail information in an understandable way is a challenge. Granularity of the data becomes a problem when providing too much granularity makes no sense.

The group also talked about the knowledge that data holders can generate "on the fly" about the data subjects. In other words, what inexplicit information about the user can be derived by a cloud service from the data they hold about such users.

8.8.3 Multi-tenant cloud

The multi-tenant cloud use case was discussed with an increasing number of details over the two rounds of discussion. The first round of discussion focused on explaining specific aspects of the case study. The initial discussion focused on the description "bring your own cloud". The main aspect of the scenario discussed was the interaction between business and personal data flows with respect to cloud services. It was difficult to explain clearly where the 'problem' was because it was understood initially as an access control problem. That is, it would be 'sufficient' to access cloud services by different accounts (i.e. business and private accounts). Therefore, the interaction described in the use case between a business end user (Employer) and an individual end user (Employee) was not perceived as being a problem as long as the access rights (e.g. employer access rights to employee's personal data) are well defined. The problem of using cloud services for personal use while in a business context is suggested could be addressed simply by guidelines (e.g. guidelines to regulate the use of clouds for personal data). Although many business end users (e.g. large enterprises) may have some internal guidelines (or formal policies), it was unclear how such guidelines should be detailed or regulated. Similarities were identified between "bring your own cloud" use case and "bring your own device". From a legal perspective, it seems that the problem could be described in terms of: Corporate Policy, Regulatory Regime, Data and Geographic Mobility (e.g. from where people access cloud services).

The discussion with the second group moved from understanding the features of the use case to analysing what properties (e.g. transparency and awareness) would be desirable. Awareness was one of the main features identified for the case study. For instance, it would useful to provide users with some awareness-related functionality flagging up any policy violation (e.g. in order to avoid non-compliance with guidelines and policies while accessing cloud services for personal data). However, it was somehow recognised that supporting awareness might conflict with security or other aspects of cloud services – how much awareness? Transparency was another property discussed. However, in the context of the case study the main focus was on the protection of individuals (personal data). For instance, it should be 'transparent' who has the authority to investigate any policy compliance. Overall, stakeholders acknowledged some of the issues concerning the case study. The discussion seemed to assume that some problems associated with the use case were problems associate in general with ICT. Therefore, some of technical solutions might still be relevant in the cloud. However, the cloud is affecting the risk perception of some problems. Accountability mechanisms would need to address such shift in risk perception in the cloud.

In addition: Specifically when cloud services are used to store both business and personal data from within a company, the question of access to data is deemed important by the participants. The participants wonder whether true segregation of business and personal data is possible, but emphasize the importance thereof. The balance between the protection of individuals versus the authority to investigate needs further exploration. There's a need of protection of individuals via tools such as a simple pop-up: "Hey! You're crossing a boundary of personal / business data" .

The way forward, uttered by one attendend, is not informed consent, but getting service providers to account even though end-users are not waiting for such information. The question therefore rised, to whom then should service provdiers than present this information.

One statement I cannot directly place in the summary, but is interesting with regard to accountability. "Our customers use this box (data storage at cloud provider) because they trust us. […] In general our company does not have access to the data in the box, accept when legal court orders are in place".

9 Appendix B: Observation template

Observation template workshop Brussels 20130116
(For legibility, whitespace has been removed from the template tables)

Start .. : .. hours
End .. : .. hours
Date January 16th 2013
Observer ________________

Workshop round I II III

Session topic / discussion ____

Location plan
(for an example see last page)

Description of participants

	Function	Company / Organization	Gender	Age	Position within group
A			M F		
B			M F		

9.1 Topics for observation

- **Participants & discussion process**
  - Relations between participants (organisational, personal, etc.)
  - Interaction between participants (possible enacted power-relationships)
  - Discussion process (order of topics discussed / questions asked)
- **The Cloud**
  - Perceptions on the cloud (what is the cloud? Opportunity, threat, (in)secure, etc…)
  - Concerns, Participants have concerns about … And why?
- **Requirements**
  - Social
  - Economic
  - Legal
  - Usability
  - Functionality
  - Other
- **Accountability, & defining notions of accountability**

    - Perceptions on accountability (what is accountability? Who should be accountable? For what? To whom?)
    - Perceptions on trust
    - Perceptions on transparency
    - Other defining notions of accountability
- **Scenarios**
    - Functionality of the scenarios
- **Other**

Please, take descriptive AND reflective notes.

Descriptive notes reflect the description of activities and discussed items and reflective notes are notes on your experiences, the process, reflections on activities.

Participants & Discussion process	***Descriptive notes*** (Description of activities and discussed items)	***Reflective notes*** (Notes about your experiences, the process, reflections on activities)
Relations between participants (organisational, personal, etc.)		
Interaction between participants (possible enacted power-relationships)		
Discussion process (order of topics discussed / questions asked)		

Cloud	***Descriptive notes***	***Reflective notes***
Perceptions on the cloud What is the cloud? Opportunity, threat, (in)secure, etc…		
Participants have		

concerns about … And why?		

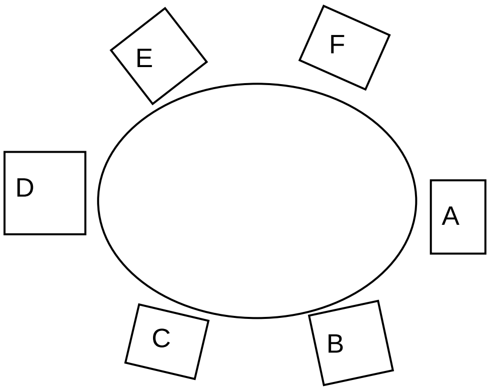
Requirements	***Descriptive notes***	***Reflective notes***
Social **Economic** **Legal** **Usability** **Functionality** **Other**		

Accountability, & defining notions of accountability	***Descriptive notes***	***Reflective notes***
Perceptions on Accountability What is accountability? Who should be accountable? For what? To whom?		
Perceptions on Transparency		
Perceptions on Trust		
Other defining notions of accountability		

Scenarios	***Descriptive notes***	***Reflective notes***
Functionality of the scenarios		

Other	***Descriptive notes***	***Reflective notes***

9.2 Example location plan and description (social) actants



Description participants

A: respondent 1; function, company/organisation, m/f, age (if known), position within the group (chair, dominant, quiet, questioning, etc)
B: respondent 2; function, company/organisation, m/f, age (if known), position within the group (chair, dominant, quiet, questioning, etc)
C: respondent 3; …
D: respondent 4; …
E: white board
F: observer; explicit status of observer (as announced (description) and as executed (reflection))
G: …

10 Appendix C: Statements from the minutes used for requirements

Section refers to section in Appendix A.

Statement #	Section	Stakeholder/ observer	Statement
1	8.1	Stakeholder	In general, data security shall be implemented through appropriate organizational and security measures in order to safeguard data integrity, availability, confidentiality and traceability.
2	8.1	Stakeholder	In order to safeguard control over data and compliance with personal data protection laws data segregation is often mentioned as a requirement. However, this seems difficult to achieve in cloud computing services.
3	8.1	Stakeholder	Another challenge is the implementation of different policies –according to the nature of the data, the privacy laws and the needs of the clients. HP “sticky policies” are mentioned as an example of good handling

Statement #	Section	Stakeholder/ observer	Statement
4	8.1	Stakeholder	Data encryption during the processing phase is another challenge and further research is necessary.
5	8.1	Stakeholder	Suitable audit mechanisms which do not present an additional security risk, as for example if every client may audit the cloud service provider's systems and applications.
6	8.1	Observer	Risk analysis would benefit from involving cloud experts identifying how security threats expose cloud vulnerabilities.
7	8.1	Observer	Cloud stakeholders are more and more aware of security threats. However, they feel a lack of control due to the fact that the cloud implies a different form of control and management over data. Moreover, it seems that recovering from security attacks is more difficult in the cloud than in other conventional ICT.
8	8.1	Observer	It seems that so far there are no mechanisms to distinguish among cloud servicers. Therefore, cloud stakeholders have no other option but to trust all actors in the cloud.
9	8.1	Observer	data and purposes should be tightly linked together (in order to mitigate the risk of data being used for different purposes). Mechanisms (e.g. sticky policies) that link data and policies together seem to address such risks.
10	8.1	Observer	emerging conflicts among the legislative regimes and security mechanisms (e.g. data encryption limits the ability to process data). Although some security mechanisms address specific threats, it is difficult to adopt them throughout the data management lifecycle. Moreover, complying with legislative regimes may require releasing critical information that might expose security vulnerabilities.
11	8.1	Observer	A strong accountable logical segregation of data separating personal sensitive data from 'meta-data' would enable compliance mechanisms with respect to relevant legislative regimes.
12	8.2	Observer	Regulation overlays are different per sector, the categorization of private or public sector covers a first distinction for a more modular approach. Within the public sector a distinction can be made between health and other public sectors. The private sector is split up in Pharma, Energy and Financial Services. Other aspects allowing for the definition of different modules are: commercialization (consumer / enterprise), and whether encryption is in place or not.
13	8.3	Observer	The first aspect of cloud security was concerned with the position of the 'line of defence'. Proprietary ICT requires company to maintain their security mechanisms (e.g. firewall), which might concerned mainly with defending sensitive data from external attacks. Cloud services enable companies to move the 'line of defence' externally to the company, far away from internal critical assets. This deployment of the line of defence in the cloud benefits from security expertise offered by cloud providers. Therefore, it would require maintaining limited resources dedicated to security making cloud services cost-convenient over the medium-long term. However, it is unclear whether or not moving the line of defence in the cloud involves a shift in security responsibilities across company boundaries.
14	8.3	Observer	Managing sensitive data requires a clear allocation of rights – Who can use data? What can be done on data? Who knows the value of data?
15	8.4	Observer	Real time monitoring (control) and the division of data on different physical machines though with clear whereabouts of location depending on the type

Statement #	Section	Stakeholder/ observer	Statement
			of data stored (data segregation).
16	8.4	Observer	As soon as there is a data breach, banks need to be notified to take necessary actions.
17	8.4	Observer	A concern of these high standards and demands of the banking industry is the developmental costs to meet these requirements. Users of cloud-computing services can define what they need and technology can develop such mechanisms. Yet, mixing technological possibilities and the level of needed security might lead to commercial problems. Developing in-house clouds might become cheaper, and the opportunity of the cloud is missed. A requirement for accountability in the cloud therefore should be that collaboration is needed within sectors. If such collaboration is lacking, all kinds of private in house clouds will be developed. However such collaboration is only possible on the same risk levels. Nevertheless, the banking industry is keen on collaborating since they rather are confronted with one audit, than ten different audits.
18	8.5	Observer	The orchestration of cloud providers is seamless to the users, but at the end there was a consensus on the need for an entity that would be responsible for this orchestration
19	8.5	Observer	The stakeholders also saw the need of classifying data according to their level of security. Customers should be able to decide what piece of data can be classified as critical or non-critical. Costs and other factors might be dictated by these labeling of the data (e.g. critical data would require high level of security, thus cloud service providers could charge an expensive fee for handling and storing such critical data).
20	8.5	Observer	From a perspective of privacy, having a cloud-of-clouds environment would prevent any single cloud provider to access all customer data. Since data is distributed across different clouds, cloud providers would be unable to make sense of customer data, unless all of them 'collaborate'. This concept was called during the discussion as “knowledge-splitting”. Splitting the data in this way blurs the concept of personal data, since the data processor would be unable to know what data is personal. The following sketches depict some of the concepts discussed
21	8.5	Observer	The accountability for each cloud provider has to be determined (for instance, by requesting log files), but this could be quite expensive - Is it possible to have some intelligent tool that makes complex situations reduce what the cloud providers have to prove? For instance, one of the things that they have to prove is that they are not communicating in some way.
22	8.5	Observer	By tagging the data customers would be able to distinguish what is critical or non-critical data. If there is no tagging of data, then all data should be treated with highest security, which is not optimal or efficient. To be able to guarantee security of the data is important.
23	8.6	Observer	All participants stress the importance of a tool that visualizes the exact location of data centers and who has access to the data .
24	8.6	Observer	Second, framing the international transfers should take into account local legislation. When responsibility is left to the service providers, control might be lost. Solutions can be found in a cooperation approach and / or a group policy. A requirement could be to allow for an ‘opt out’, the option to leave.

Statement #	Section	Stakeholder/ observer	Statement
25	8.6	Observer	Third extraterritorial laws should be (further) developed. These laws should envision that transparency needs are different per reality.
26	8.6	Observer	Service providers might be made accountable for setting up organizational measures that allows them to show their transparency. For example, a service provider might create a company without an US identity; if certain services have an US identity they can be excluded from certain activities.
27	8.7	Observer	A) The DPA's supervision should be made easier and also become more valued (by regulation?) since there's a need for centralized security with a strong management. B) There's a need for international cooperation and development of tools supporting transfers to third countries. C) Protection should be made more practical without decreasing the level of protection.
28	8.8.1	Cafe Host	it was suggested that US providers will comply "enough" to do business in Europe (but maybe no more than minimum). More regulation was not seen as a solution to this
29	8.8.1	Cafe Host	We may see the emergence of sectoral clouds to handle different requirements, notably for energy, financial service and health .
30	8.8.1	Cafe Host	Some providers are offering services where the end-user keeps the encryption key, but it is not clear how this could be employed when sharing data with other actors.
31	8.8.2	Cafe Host	A similar use case was brought up that would adjust SLA and contracts to whether a given SaaS user would like to be the exclusive data controller (more expensive), or it would agree to share their customer personal data with further companies and pay less.
32	8.8.2	Cafe Host	The importance of the use case (ERP) was highlighted when all mentioned that it was needed to have reasonable means to justify the data collection to data protection authorities and to demonstrate compliance.
33	8.8.2	Cafe Host	In addition, the group discussed the need for explicit consent of the users regarding data portability, withdrawal, etc. A suggestion was made that consent might not be collected just once, but every time data is released or, in the case of this SAP scenario, every time a supermarket's loyalty card is used.
34	8.8.2	Cafe Host	I can give consent to display a picture at one point and then revoke that consent; however, that picture could have been already sent to third parties, or used by other users, etc. Thus, services have to reliably prove that they have at least attempted (or take some action) to revoke the customer's data is the customer has requested to do so
35	8.8.2	Cafe Host	Also, a discussion was made about the possibility of the different services involved in the scenario to feed a database of users' profiles. For the purposes of profiling, databases cannot be anonymized, but they can be pseudonomize. The group mentioned that there are situations in which keeping a profile can be very risky for the individual.
36	8.8.2	Cafe Host	Regarding data breaches, the group discussed the need for notifying the data subjects about breaches to their data (e.g. who should be notified? how much information should the data subject be provided with?, etc.).

Statement #	Section	Stakeholder/ observer	Statement
37	8.8.2	Cafe Host	The question was raised on what kind of compensation would consumers get in case of a data breach, and who is responsible for what? The group mentioned that responsibility would depend on the contracts between the different parties
38	8.8.2	Cafe Host	Also, users should be notified with detail information about the breach to their data, since they might require taking some action in order to minimize further consequences of the attack. However, providing detail information in an understandable way is a challenge. Granularity of the data becomes a problem when providing too much granularity makes no sense.
39	8.8.2	Cafe Host	The group also talked about the knowledge that data holders can generate "on the fly" about the data subjects. In other words, what inexplicit information about the user can be derived by a cloud service from the data they hold about such users.
40	8.8.3	Cafe Host	The problem of using cloud services for personal use while in a business context is suggested could be addressed simply by guidelines (e.g. guidelines to regulate the use of clouds for personal data).
41	8.8.3	Cafe Host	Although many business end users (e.g. large enterprises) may have some internal guidelines (or formal policies), it was unclear how such guidelines should be detailed or regulated
42	8.8.3	Cafe Host	Similarities were identified between "bring your own cloud" use case and "bring your own device".
43	8.8.3	Cafe Host	From a legal perspective, it seems that the problem could be described in terms of: Corporate Policy, Regulatory Regime, Data and Geographic Mobility (e.g. from where people access cloud services)
44	8.8.3	Cafe Host	Awareness was one of the main features identified for the case study. For instance, it would useful to provide users with some awareness-related functionality flagging up any policy violation (e.g. in order to avoid non-compliance with guidelines and policies while accessing cloud services for personal data).
45	8.8.3	Cafe Host	However, it was somehow recognised that supporting awareness might conflict with security or other aspects of cloud services – how much awareness?
46	8.8.3	Cafe Host	it should be 'transparent' who has the authority to investigate any policy compliance
47	8.8.3	Cafe Host	The discussion seemed to assume that some problems associated with the use case were problems associate in general with ICT. Therefore, some of technical solutions might still be relevant in the cloud. However, the cloud is affecting the risk perception of some problems. Accountability mechanisms would need to address such shift in risk perception in the cloud.

11 Appendix D: Invitation letter to stakeholders

Your ref.	**Our ref.**	**Project No. / File code**	**Date**
Your ref	90C375/MGJ/mgj	90C375	2013-01-10

Dear participant,

Invitation to A4Cloud Stakeholder Workshop

It is our pleasure to invite you to participate in the first A4Cloud stakeholder workshop to be held at the Holiday Inn Brussels Airport Hotel, Holidaystraat 7, 1831 Diegem, Belgium on **Wednesday, January 16th 2013**.

The Accountability for Cloud and other future Internet Services project (A4Cloud) is an Integrating Project in the EU 7th Framework Programme, with a goal to develop mechanisms and tools to enable cloud service providers to give their users appropriate control and transparency over how their data is used. A4Cloud is led by HP labs, with participation from SAP and a number of European research organizations and university partners.

You have been identified as an important influencer for defining future European Cloud solutions, and we would therefore like to invite you to participate in our workshop to elicit and prioritize requirements for new accountable cloud-based services. Based on your expertise and focus area, you will help shape the content of the workshop, ensuring that the topics that are important to you are reflected in the resulting requirements.

We have outlined the following agenda:

09:30: Coffee
10:00: Welcome & introduction
10.15: Workshop Part I
13.05: Lunch
13.45: Workshop Part II
15.50: Closing remarks
16:00: Workshop ends

The workshop results will be documented in a report which will be available to all participants. Participants can choose to remain anonymous, but if not they will be acknowledged in the project documentation.

Please confirm your attendance at your earliest convenience.

Yours sincerely,
for SINTEF IKT and the A4Cloud Project

Martin Gilje Jaatun
Senior Scientist

12 List of tables

13 List of figures

More about the Accountability for Cloud and other future Internet Services project (A4Cloud)

Cloud and IT service providers should act as responsible stewards for the data of their customers and users. However the current absence of accountability frameworks for distributed IT services makes it difficult for users to understand, influence and determine how their service providers honour their obligations.

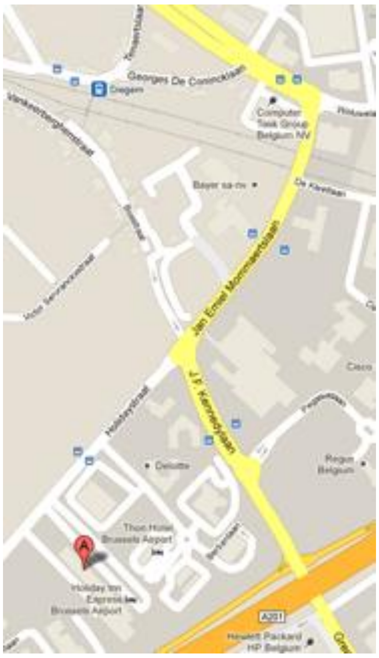
A4Cloud will create solutions to support users in deciding and tracking how their data is used by cloud service providers. By combining methods of risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress, A4Cloud aims to extend accountability across entire cloud service value chains, covering personal and business sensitive information in the cloud.

A4Cloud solutions will support service providers in preventing breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress.

A4Cloud aims to improve the acceptability of cloud-based infrastructures where critical data is perceived to be at risk. It will develop techniques for improved trustworthiness of cloud ecosystems as prerequisite for accountability. Therefore it will create policies and tools that enforce responsibilities while striking a balance between transparency and privacy, and determine issues and constraints for regulators, corporate and institutional service providers, users, and their end-users.

A4Cloud will have a lasting impact on the competitiveness of the European ICT sector by addressing major perceived barriers to trustworthy cloud-based services. These include concerns about complexity and enforceability of legal, regulatory and contractual provisions, socio-economic and corporate constraints, issues of trust for service-users such as risk-mitigation, privacy, confidentiality and transparency, and operational challenges such as interoperability and enforcing and monitoring compliance.

Additional venue information



Distance from airport: 5km (5 minutes by taxi)
Distance from Diegem railway station: 850 meters (10 minutes' walk)