ASMONIA

Attack analysis and Security concepts for MOBILE Network infrastructures, supported by collaborative Information exchange

Analysis of Requirements for the Deployment of Cloud Systems

WP 3.1 Deliverable (public)

D31-1.0

Contributors: Cassidian Systems
Fraunhofer Institute for Secure Information Technology SIT
Nokia Siemens Networks GmbH & Co KG

Editor: Mark Gall (Fraunhofer SIT)
Analysis of Requirements for the Deployment of Cloud Systems
WP 3.1 Deliverable (public)
D31-1.0

Author(s)  Company  E-mail
Mark Gall  Fraunhofer SIT  mark.gall@sit.fraunhofer.de
Bernd Jäger  Nokia Siemens Networks GmbH & Co KG  bernd.jaeger@nsn.com
Heiko Kirsch  Cassidian Systems  heiko.kirsch@cassidian.com
Joachim Lüken  Nokia Siemens Networks GmbH & Co KG  joachim.lueken@nsn.com
Angelika Ruppel  Fraunhofer SIT  angelika.ruppel@sit.fraunhofer.de

About the ASMONIA project

Given their inherent complexity, protecting telecommunication networks from attacks requires the implementation of a multitude of technical and organizational controls. Furthermore, to be fully effective these measures call for the collaboration between different administrative domains such as network operators, manufacturers, service providers, government authorities, and users of the services.

ASMONIA is the acronym for the German name* of a research project that aims to improve the resilience, reliability and security of current and future mobile telecommunication networks. For this purpose the ASMONIA consortium made up of several partners from academia and industry performs a number of research tasks, based on the specific expertise of the individual partners. The project running from September 2011 till May 2013 receives funding from the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF). Various associated partners further contribute on a voluntary basis.

* The full name is "Angriffsanalyse und Schutzkonzepte für MObilfunkbasierte Netzinfrastrukturen unterstützt durch kooperativen InformationsAustausch" (Attack analysis and security concepts for mobile network infrastructures, supported by collaborative information exchange).

Partners:
Cassidian Systems
ERNW Enno Rey Netzwerke GmbH
Fraunhofer Institute for Secure Information Technology SIT
Hochschule Augsburg
Nokia Siemens Networks GmbH & Co KG
RWTH Aachen

Associated Partners:
Federal Agency for Digital Radio of Security Authorities and Organizations (BDBOS)
Federal Office for Information Security (BSI)
Deutsche Telecom AG (DTAG)

For more details about the project please visit www.asmonia.de.
# Table of Contents

## 1 Introduction

1.1 Cloud Computing .................................................. 7  
1.2 Early Warning Systems .......................................... 10  
1.3 ASMONIA Cloud Typology ...................................... 10  
1.4 ASMONIA Cloud Interfaces .................................... 12

## 2 Cloud Scenarios

2.1 Cloud as a means to provide Services for the Support of the Collaboration Concept ........................................ 14  
2.1.1 Compute as a Service ........................................... 15  
2.1.2 Data storage as a Service .................................... 17  
2.2 Cloud as a means to enhance Availability of Telco Components in Overload and Outage Situations .............................. 25  
2.2.1 Overload and Outage Scenarios for the Collaborative Cloud ......................................................... 28  
2.2.2 Connecting the Operator Cloud with the Collaborative Cloud ......................................................... 33  
2.2.3 Practical Operator Considerations for the Collaborative Cloud ......................................................... 33

## 3 Management of shared cloud resources

3.1 Moving a telecommunication component into a cloud .................... 36  
3.1.1 Handling and deployment of virtual images ....................... 37  
3.1.2 Choosing an adequate virtualization method ..................... 38  
3.1.3 Network issues .................................................. 38  
3.1.4 Privacy and data issues ....................................... 39  
3.1.5 Implementation and Interoperability issues .................... 39  
3.2 Moving a virtualized component to another cloud .................. 40  
3.2.1 Duration and timing of the copy process ....................... 41  
3.2.2 Handling of old copies ....................................... 41  
3.2.3 Considering Backups .......................................... 41  
3.2.4 Interoperability of virtual images .............................. 42  
3.2.5 Privacy and data issues ....................................... 42  
3.3 Scaling a component in a cloud .................................. 42  
3.3.1 Choosing a load balancing system ............................. 43  
3.3.2 Identifying overload situations ............................... 43  
3.3.3 Scalability of resources ....................................... 43  
3.4 Generating free resources through redistribution .................. 44  
3.4.1 How to prioritize components ................................. 45  
3.4.2 Means to free resources ...................................... 45

## 4 Collaborative Cloud Provider Models

4.1 Cloud Composition ................................................. 47  
4.1.1 Architectural Approaches ................................... 47  
4.1.2 Homogeneity regarding network resources .................... 50  
4.1.3 Dynamics of resource allocation .............................. 51  
4.1.4 Balancing usage and provision of resources .................. 53  
4.2 Cloud Provider Categories ...................................... 53
4.3 Cloud Provider Models
4.3.1 Provider Models for a Central Collaborative Cloud 54
4.3.2 Provider Models for a Hierarchical Distributed Collaborative Cloud 56
4.3.3 Provider Models for a Peer-to-Peer Collaborative Cloud 57

5 General Requirements for the Support of Cloud Scenarios 58
5.1 General requirements for the Support of Cloud based Data Storage and Data Evaluation Solutions 58
5.1.1 Potential WP2 use cases 58
5.1.2 Potential WP4 use cases 61
5.2 General Requirements for the support of Cloud based Telecommunication Resources in Overload and Outage Situations 61

6 Security Requirements for the Support of the Cloud Scenarios 64
6.1 Cloud Infrastructure and Management 66
6.2 Cloud Resources and Resource Management 68
6.3 Cloud APIs 70
6.4 Cloud Data 71
6.5 Cloud Applications 71
6.6 Cloud Customer Clients 72
6.7 End User 73

7 Regulatory Requirements for the Support of the Cloud Scenarios 75
7.1 Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) 77
7.2 Telecommunications Act (Telekommunikationsgesetz - TKG) 78
7.3 Telemedia Act (Telemediengesetz - TMG) 80

8 Conclusion 83
8.1 Outlook 83

References 84

Glossary and Abbreviations 86
Glossary 86
Abbreviations 86

Revision History 88
Executive Summary

This document deals with the usage of elastic systems, or cloud-computing systems as they are more commonly known, in the context of the ASMONIA project. Cloud computing represents a form of sharing resources and as such a basic form of collaboration.

Enabling the information exchange by using typical cloud service concepts, i.e. concepts for storage and computation services in the cloud, is one of the main usage scenarios discussed in this document. The usage scenario describes services that allow collaboration by sharing information in several ways. From this more specialized use cases are derived that reflect the usage of cloud computing systems as a supporting platform for other parts of ASMONIA.

Another core area of ASMONIA deals with security concepts. The usage of cloud computing systems in security concepts for mobile network operator networks is another main usage scenario discussed in this document. The focus lies on the mitigation of overload and outage situations caused by an attack on the provider network.

Furthermore this document presents and discusses requirements of various kinds describing different aspects of the usage of cloud computing systems. There are use cases describing the functional requirements that are needed in order to support the usage scenarios. The use cases are on a relatively abstract level and several issues leading to non-functional requirements are highlighted in their presentation. Other chapters present non-functional requirements, which were divided into general requirements, security requirements and regulatory requirements.

The presented requirements will be used as a basis for future work, in which a cloud architecture, that supports the use cases derived from the usage scenarios presented in this document, will be designed.
1 Introduction

This document deals with the usage of elastic systems, or cloud computing systems as they are more commonly known, in the context of the ASMONIA project. Although this document bears the title “Analysis of Requirements for the Deployment of Cloud Systems” a fully detailed requirements analysis is not contained in this document. This is because we too share the problems often encountered in the phases of requirements elicitation and requirements analysis: the stakeholders have different backgrounds and a different understanding of the project goals.

In order to help the creation of a common understanding and thus help the stakeholders to express their requirements correctly, we decided to use this document to present how we conceive that cloud computing systems can be used to support the various parts of the ASMONIA project. This document can therefore be seen as a first milestone in the process of requirements analysis. It presents in as much detail as possible various kinds of requirements that need to be adjusted for the currently still evolving use cases.

An outline of the topics discussed in this document is depicted in Figure 1. The remaining part of chapter 1 deals with general concepts of cloud computing to which we refer throughout this document. In chapter 2 we present the cloud scenarios, which illustrate the usage of cloud computing systems in ASMONIA and from which more specific use cases can be derived. We also present categories of requirements that need to be considered when use cases for the usage of cloud computing systems are developed. The following chapters 3 and 4 discuss technical considerations that will influence the design of a cloud computing system supporting the cloud scenarios from chapter 2. This discussion is then followed by a more detailed description of the requirements, divided along the requirement categories from chapter 2 into the chapters 5, 6 and 7. Chapter 8 concludes the document and gives a short outline of the following activities in ASMONIA regarding the usage of cloud computing.
1.1 Cloud Computing

The most widely recognized definition of Cloud Computing is provided by the US National Institute of Standards and Technology (NIST).

According to NIST cloud computing can be described as following:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction ([NIST_CDEF], Peter Mell and Tim Grance from the Information Technology Laboratory at NIST).”

The NIST cloud definition and details such as the cloud characteristics, the service models and the deployment models are depicted in the following figure.

![NIST Cloud Definition Framework](image)

**Figure 2: The NIST Cloud Definition Framework [NIST_CSEC]**

The cloud computing characteristics are:

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- **Resource pooling.** The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to
specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Cloud service delivery is divided among three architectural models and various derivative combinations.

![Figure 3: Cloud Computing Delivery Models](image)

The three fundamental classifications are often referred to as the “SPI Model”, where “SPI” refers to Software, Platform or Infrastructure (as a Service), respectively — defined thus:

- **Software as a Service (SaaS)** is software offered by a third party provider, available on demand, usually configurable remotely via the Internet. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Oracle CRM On Demand, Google Docs, etc).

- **Platform as a Service (PaaS)** is an application development and deployment platform delivered as a service to developers over the Web. This platform consists of infrastructure software, and typically includes a database, middleware and development tools. Some PaaS offerings have a specific programming language or API. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the
deployed applications and possibly application hosting environment configurations. Examples are Microsoft Azure, Force and Google App Engine.

- **Infrastructure as service (IaaS)** is the delivery of hardware (server, storage, network and other fundamental computing resources), and associated software (operating systems virtualization technology, file system), as a service. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). Examples include Amazon Elastic Compute Cloud (EC2) and Secure Storage Service (S3), Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.

There are also different ways to deploy cloud services which is roughly shown in the following figure.

![Figure 4: Cloud Computing Deployment Models](image)

Regardless of the service model utilized (SaaS, PaaS, or IaaS) there are four deployment models for cloud services, with derivative variations that address specific requirements:

- **Public cloud**: the cloud infrastructure is made available to the general public or a large industry group. Any organization may subscribe to the cloud and the cloud infrastructure is owned by an organization selling cloud services;

- **Private cloud (Enterprise cloud)**: the cloud infrastructure is operated solely for one specific organization. It may be managed by the organization or a third party and may exist on premise or off premise. Hereinafter we often use the term “private cloud” without further specification.
  - An internal private cloud is located in the enterprise data center (on premise) and all the assets are physically owned and operated by the organization itself. This gives IT managers complete control over the available resources. An internal private cloud could be a Eucalyptus or VMWare vCloud implementation in the data center of a medium or a large enterprise.
An external private cloud is a private cloud hosted off premise and connected to the intranet using a VPN infrastructure. An external private cloud could be operated by a service provider like T-Systems or IBM dedicating a number of racks in their facilities for a private cloud they operate on an enterprise’s behalf.

A managed private cloud is a private cloud infrastructure which is managed by an external IT service provider. The IT service provider is responsible for operating the cloud infrastructure on the basis of Service Level Agreements (SLAs). A managed private cloud could be hosted on premise (internal managed private cloud) or off premise (external managed private cloud).

• **Community or partner cloud**: The cloud infrastructure is shared by several organizations (limited and well-defined number of parties) and supports a specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. Community cloud works well for supply chains or collaborating government agencies.

• **Hybrid cloud**: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

It is important to note that there are derivative cloud deployment models emerging due to the maturation of market offerings and customer demand. An example of such is **virtual private cloud**, which is a way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers’ data center, usually via virtual private network (VPN).

### 1.2 Early Warning Systems

Early warning systems are an important part of the ASMONIA project. In order to be able to analyze how elastic systems can support early warning systems or interact with them, it is necessary to get a clear understanding of what early warning systems are and what their purpose is.

In the context of IT systems the purpose of early warning systems is to support the protection of the IT infrastructure. This is done by gathering information about the status of the infrastructure and communicating relevant information in order to prevent an aggravation of the status. Using evidence from the smallest number of entities to detect attacks or abnormal activities, this information should be shared and distributed in order to help many other not yet affected parts of the infrastructure or IT systems operators.

Early warning systems rely on sensors to collect information. What kind of information a sensor collects depends strongly on its type. Existing approaches for early warning systems use e.g. intrusion detection systems or honey pots as sensors, which collect information about the network traffic. But there are various other types of sensors that are used in current approaches as well as new types that are going to be developed in the course of the ASMONIA project.

### 1.3 ASMONIA Cloud Typology

In the context of the ASMONIA project we expect the usage of multiple cloud systems. We have identified two different types of cloud systems to which we will refer to in this document:
• Operator Cloud
An operator cloud is a cloud system that is part of the infrastructure of a mobile network operator. The operator cloud is – according to the NIST definition – a private cloud only available to the mobile network operator. None of the other collaborating mobile network operators participating in ASMONIA have any access to it.

• Collaborative Cloud
The collaborative cloud is – according to the NIST definition – a community cloud that is shared with all collaborating mobile network operators taking part in the ASMONIA project. All of them may access and use it. For our purpose the NIST definition of the deployment model “community cloud” is too vague. Therefore a further analysis of the various possibilities and their implications will be conducted in this chapter 4.

The two types of cloud systems are located in different parts of the infrastructure of mobile network operators participating in ASMONIA and serve different purposes. Usually our work will focus on the collaborative cloud.

Both cloud types are part of the high level architecture for the ASMONIA protection and collaboration concept. The ASMONIA architecture as defined in WP1 foresees three different so-called functional clusters:

1) **IP (Integrity Protection):** This functional cluster deals with new methods for software integrity protection for both mobile end devices and network elements. IP is handled in WP2.

2) **MA (Measurement and Analysis):** This functional cluster develops new methods for the detection, analysis and evaluation of anomalies and potential network attacks. Sensor data such as e.g. malware samples and conclusions drawn from the analysis of that data are foreseen for collaborative information exchange. MA is handled in WP4.

3) **CC (Cloud Computing):** The cloud computing functional cluster is handled in WP3.

The following figure provides a rough overview on how the ASMONIA functional cluster CC is integrated into the security and protection concept.
1.4 ASMONIA Cloud Interfaces

Cloud computing provides collaborative functions to support the ASMONIA security and protection concept of mobile networks. There are basically three different types of interfaces provided by the cloud platform.

a) Type A interfaces:

These interfaces are the basic cloud computing interfaces, meaning that cloud resources are exposed for usage in applications by these interfaces. Cloud resources can either be compute, network or storage resources. Please note that network and storage resources can be exported externally, i.e. to applications residing outside the cloud, or internally, i.e. to applications deployed on the same cloud platform. In order to be able to consume compute resources an application must be deployed on the same cloud platform.

b) Type B interfaces:

These interfaces are the cloud management APIs.

c) Type C interfaces:
These interfaces are not native cloud interfaces but are offered by applications running on the cloud platform. Those applications have been developed in the context of the ASMONIA project offering services via an interface to mobile networks.

The following figure illustrates the different types of interfaces and the purpose they serve.

![Cloud Computing Interfaces](image-url)

**Figure 6: Cloud Computing Interfaces**
2 Cloud Scenarios

WP3 will support two scenarios, which will be described in the following chapters in more detail. The scenarios are:

1) Cloud as a means to provide services for the support of the collaboration concept

Cloud systems are inherently elastic and scalable and thus are exceedingly qualified to offer storage and compute resources in a fast and on demand fashion. Especially when attacks on mobile networks occur, large amounts of sensor data and messages from early warning systems can be stored in the cloud. Compute resources can be offered to evaluate the data in order to generate information about the network security status. Furthermore a cloud system could support collaboration between network operators by sharing information on attacks, sensor data, malware patterns, etc., or by hosting applications such as a security dashboard on the platform.

The uses cases supported in this cloud scenario will be developed mainly in the other WPs of the ASMONIA project. As such the CC cluster only provides the capabilities to support those uses cases.

2) Cloud as a means to enhance availability of telco components in overload and outage situations

The goal of this cloud scenario is the development of concepts and methods to improve the availability and the security in overload and outage situations by the means of using cloud systems. The collaborative cloud can be used for the distributed backup storage of configuration and recovery information. Furthermore it will be explored whether parts of telecommunication networks are suited to be instantiated in a collaborative cloud. The main focus here lies on security considerations and the evaluation of the technical realization.

The use cases supported in this scenario are somewhat stand-alone since there is no linkage to other WPs of the ASMONIA project besides the fact that the scenario uses a cloud infrastructure that could be similar, or possibly identical, to the infrastructure required for the above scenario.

2.1 Cloud as a means to provide Services for the Support of the Collaboration Concept

Services provided by cloud platforms can be categorized basically into three classes:

1. compute,
2. storage and
3. network services.

These service classes can be further subdivided into single services as shown in the following figure.
The following chapters contain a more elaborate description of the rationale behind these services.

### 2.1.1 Compute as a Service

Compute resources can be offered either via IaaS or PaaS.

The IaaS compute service offers running a virtual machine (VM) on top of a virtualization layer.

In a public cloud offering the virtualization layer is very often implemented either using Linux/Xen software stacks or VMware virtualization solutions.
Besides the pure runtime environment for VMs, IaaS cloud platforms very often provide additional services.

**Firewall:** The firewall prevents network attacks and allows defining packet filter rules for IP traffic. Very often VMs can be associated with a security group and the filter rules are applied to those groups. A firewall should also ensure that VM instances cannot send spoofed network traffic, i.e. the source IP address should be checked at the firewall.

**VM monitoring:** This is a service that provides monitoring for cloud resources providing resource utilization, operational performance, etc.

**Auto scaling:** This service allows automatic scaling of compute resources, i.e. dependent on VM monitoring data the service launches new instances if more capacity is needed, or terminates instances if the resource is no longer needed.

**MapReduce service:** This service allows processing vast amounts of data.

As an alternative to the IaaS approach, applications can be developed on PaaS platforms.

---

**Figure 9: PaaS Model**

PaaS offerings provide a runtime environment for applications as a service. Runtime environments include Java, Python, .NET and others. Very often PaaS clouds also offer facilities for application design, application development, testing, deployment and hosting.

The strength of PaaS is to allow fast development and offer of new applications with the help of the included PaaS platform tools. Since this is not really required by ASMONIA, it is more likely that ASMONIA will use an IaaS platform. However, at present this is kept open and will be decided in a later phase of the project.
2.1.1.1 Potential WP2 Use Cases

At present WP2 use cases requiring compute resources from the context of WP2 are not known. But it is possible that during the future work on the project WP2 will create such use cases.

2.1.1.2 Potential WP4 Use Cases

Potential use cases are the following:

1. Local security dashboard
   The local security dashboard is represented as an application offering a visualization of the health and security status for the domain of one mobile network operator. Despite the fact that this dashboard provides value added information to different target groups, i.e. decision maker, administrators, security specialists or third party maintenance teams, it is fully under the control of the respective operator. To address these target groups and their special needs, the dashboard has to provide different layers of abstraction, i.e. operational, tactical and strategic views.

   The local security dashboard takes into account data collected by different sensors running within the domain of one mobile network. The collected data consists of messages about integrity violations, supplemented with information from outside this domain, e.g. the global security dashboard or vulnerability information from vendors. This data may be stored within the operator cloud by means of DaaS (see chapter 2.1.2), externally within for example a database cluster connected to the cloud via a defined interface or in a hybrid approach. The stored, computed and visualized data represents highly sensitive information belonging to one operator. Thus the fulfilment of austere data security requirements, especially confidentiality and integrity, is mandatory.

   The local security dashboard may be implemented as a PaaS or SaaS application in the operator cloud.

2. Global security dashboard
   The global security dashboard is represented as an application offering a visualization of the overall health and security status for participating parties within the ASMONIA Collaborative Network, i.e. multiple mobile network operators or trusted third parties like governmental organisations. The status is derived based on data that has been made available from different mobile network operators as well as other sources such as collaborating early warning systems or CERT-information from governmental organizations. This data should be stored within the collaborative cloud by means of DaaS. Concerning security requirements of the global security dashboard, integrity violations present a major impact. Hence fulfilment of high integrity requirements is mandatory. Confidentiality has to be treated with minor priority as long as security mechanisms for the collaborative information exchange remains intact because information for the global security dashboard is ASMONIA-public.

   The global security dashboard may be implemented as a PaaS or SaaS application in the collaborative cloud.

2.1.2 Data storage as a Service

   Most recently and mainly driven by the Storage Networking Industry Association (SNIA), the term Data Storage as a Service (DaaS) has been established, meaning that data storage is

   “delivered over a network of appropriately configured virtual storage and related data services based on a request for a given service level.”
SNIA is a non-profit association aiming for the development of storage solution specifications and technologies, global standards, and storage education.

The SNIA cloud storage reference model is shown in the following figure.

Please note that CDMI as a SNIA standardized protocol is not the only possibility for the realization of interface 3. There are also proprietary protocols from Cloud storage providers as e.g. Amazon S3, Rackspace CloudFiles, Nirvanix and others that could be used instead.

The Cloud Data Management Interface defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud. As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface.

This interface is also used by administrative and management applications to manage containers, accounts, security access and monitoring/billing information, even for storage that is accessible by other protocols. The capabilities of the underlying storage and data services are exposed so that clients can understand the offering.

SNIA distinguishes four different types of cloud storage.

**Block storage**: Block storage is offered via traditional interfaces such as iSCSI that allows mounting a volume by a virtual machine. Amazon EBS (Elastic Block Storage) is a representative in this category.

**File storage**: File storages are very often exported via protocols such as NFS, WebDAV, etc.
**Object storage**: Object storage allows to create, retrieve, update and delete data objects such as files. This is not a file system or real-time data storage system, but rather a long term storage system for a more permanent data such as VM images, log files, backup data, etc. A well-known example for object storage is Amazon Simple Storage (S3).

**Database storage**: This service provides a relational database service from the cloud. Depending on the cloud provider, the service can be implemented using database solutions such as MySQL, Oracle etc. Amazon Relational Database Service (RDS) is an example.

### 2.1.2.1 Data Storage Requirements

The data to be stored in the cloud has different requirements regarding database performance, security, confidentiality, backup strategies, archiving etc. depending on the use case. Those requirements will eventually (i.e. the follow-up deliverable D3.2) be evaluated to decide for the appropriate storage architecture and strategy.

In the chapters hereafter a number of requirements are listed and the meaning of these properties is explained. Please note that how those requirements need to be fulfilled for the specific use cases is studied in chapter 5.

#### 2.1.2.1.1 List of General Data(base) Requirements

General data requirements are the following:

1) **Transaction**
   
   Transaction means "all-or-nothing", i.e. each operation performed in a database must either complete entirely, or has no effect at all. Transaction is usually used in cases, which need to write (update, insert or delete) multi-records simultaneously.

2) **Consistency**
   
   Consistency means "all users see the same data at the same time". Different applications have different requirements on it, strong consistency indicates that all users always see the same data at the same time, middle level indicates that the user who wrote get newest and others may get updates later, low consistency level means all users get newest data eventually.

3) **Concurrency**
   
   Concurrency defines how many requests need to be handled concurrently in the application. Usually small means that the number is thousands, large means from thousands to 10 thousands, huge means more than 10 thousands.

4) **Read & Write Mode**
   
   Read & write mode of the application defines whether the application reads/writes in large and sequential manner, or in small and random way.

5) **Read vs. Write Ratio**
   
   Read-write ratio of the application distinguishes e.g. write once and read frequently, write much less than read, write equal or more than read.

6) **Query Model**
   
   The application's query model means, that the application either queries mostly by primary key, or usually in a complex manner including join, multi-conditions, multi-keys, groups etc.
7) Hit Rate
Hit rate means how many records are retrieved by one query, i.e. one result per query or many records.

8) Data Types
“Data types” means either a large amount of small size files, or few but large files.

9) Persistence
Persistence is divided into 3 categories: long term means that the data will be stored more than 3 year and kept on line, short term means the data will be stored less than 3 years, temporary means the data will be destroyed immediately after usage.

10) Latency
Latency means the response time required by the application: The most stringent demand is in several milliseconds, and the most relaxed demand accepts responses within hours.

11) Scalability
Scalability describes both the total size and the growth rate of the data that the application manages.

12) Availability
Availability describes the availability requirements of data management in percent values.

13) Recovery Time Objective (RTO)
Recovery Time Objective is the duration of time needed for restoring of data after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

14) Recovery Point Objective (RPO)
Recovery Point Objective is the duration of data loss that could be tolerated in fault situations.

15) Content Type
The type of content to be stored, e.g. mostly binary data, or textual data.
<table>
<thead>
<tr>
<th>No.</th>
<th>Items</th>
<th>Description</th>
<th>Blog</th>
<th>Session management</th>
<th>News Portal</th>
<th>Online Payment</th>
<th>Financial</th>
<th>Photo management</th>
<th>ERP</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Transaction</td>
<td>Transaction means &quot;all-or-nothing&quot;, i.e. each operation performed in a database must either complete entirely, or has no effect at all. Transaction is usually used in a case which need to write (update, insert or delete) multi-records simultaneously.</td>
<td>2. No</td>
<td>2. No</td>
<td>2. No</td>
<td>1. Yes</td>
<td>1. Yes</td>
<td>2. No</td>
<td>1. Yes</td>
<td>2. No</td>
</tr>
<tr>
<td>2</td>
<td>Consistency</td>
<td>Consistency means &quot;all users see the same data at the same time&quot;. Different applications have different requirements on it, strong consistency indicate that all users always see the same data at the same time, middle level indicate that the user who wrote get newest and others may get update later, low consistency level means all users get newest data eventually.</td>
<td>3. Weak</td>
<td>1. Strong</td>
<td>3. Weak</td>
<td>1. Strong</td>
<td>1. Strong</td>
<td>3. Weak</td>
<td>1. Strong</td>
<td>3. Weak</td>
</tr>
<tr>
<td>3</td>
<td>Concurrency</td>
<td>Concurrency defines how many requests need to be handled concurrently in the application. Usually small means that the number is thousands, large means from thousands to 10 thousands, huge means more than 10 thousands.</td>
<td>1. Small</td>
<td>2. Large</td>
<td>3. Huge</td>
<td>1. Small</td>
<td>3. Huge</td>
<td>2. Large</td>
<td>1. Small</td>
<td>3. Huge</td>
</tr>
<tr>
<td>4</td>
<td>Read &amp; Write Mode</td>
<td>Read &amp; write mode of the application defines whether the application reads/writes in large and sequential manner, or in small and random way.</td>
<td>N/A</td>
<td>2. Small and high concurrency</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>2. Small and high concurrency</td>
<td>N/A</td>
<td>1. Large and sequential</td>
</tr>
<tr>
<td>6</td>
<td>Query Model</td>
<td>The application's query model means, that the application either queries mostly by primary key, or usually in a complex manner including join, multi-conditions, multi-keys, groups etc.</td>
<td>1. Primary</td>
<td>1. Primary</td>
<td>1. Primary</td>
<td>1. Primary</td>
<td>1. Primary</td>
<td>1. Primary</td>
<td>2. Complex</td>
<td>1. Primary</td>
</tr>
<tr>
<td>7</td>
<td>Hit Rate</td>
<td>Hit rate means how many records are retrieved by one query, i.e. one result per query or many records.</td>
<td>1.1:1</td>
<td>2.1:M</td>
<td>1.1:1</td>
<td>1.1:1</td>
<td>2.1:M</td>
<td>1.1:1</td>
<td>2.1:M</td>
<td>2.1:M</td>
</tr>
<tr>
<td>8</td>
<td>Data Types</td>
<td>Data types means either a large amount of small size files, or few but large files.</td>
<td>N/A</td>
<td>1. Large count and small size</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1. Large count and small size</td>
<td>N/A</td>
<td>2. Small count and large size</td>
</tr>
<tr>
<td>9</td>
<td>Persistence</td>
<td>Persistence is divided into 3 categories: long term means that the data will be stored more than 3 year and kept on line, short term means the data will be stored less than 3 years, temporary means the data will be destroyed immediately after usage.</td>
<td>2. Short term</td>
<td>3. Temporary</td>
<td>2. Short term</td>
<td>2. Short term</td>
<td>1. Long term</td>
<td>1. Long term</td>
<td>1. Long term</td>
<td>Short term</td>
</tr>
<tr>
<td>10</td>
<td>Latency</td>
<td>Latency means the response time required by the application: The most stringent demand is in several milli-seconds, and the most relaxed demand accepts responses within hours.</td>
<td>2. Seconds</td>
<td>1.Milliseconds</td>
<td>2. Seconds +</td>
<td>2. Seconds</td>
<td>2. Seconds</td>
<td>2. Seconds</td>
<td>2. Seconds</td>
<td>2. Seconds</td>
</tr>
<tr>
<td>11</td>
<td>Scalability</td>
<td>Scalability describes both the total size and the growth rate of the data that the application manages.</td>
<td>2. Less than 1T or growth slow</td>
<td>2. Less than 1T or growth slow</td>
<td>2. Less than 1T or growth slow</td>
<td>2. Less than 1T or growth slow</td>
<td>2. Less than 1T or growth slow</td>
<td>1. More than 1T or growth rapidly</td>
<td>2. Less than 1T or growth slow</td>
<td>1. More than 1T or growth rapidly</td>
</tr>
<tr>
<td>12</td>
<td>Availability</td>
<td>Availability describes the availability requirements of data management in percent values.</td>
<td>2.99% and below</td>
<td>N/A</td>
<td>2.99% and below</td>
<td>2.99% and below</td>
<td>1.99% &amp; above</td>
<td>2.99% and below</td>
<td>2.99% and below</td>
<td>2.99% and below</td>
</tr>
<tr>
<td>13</td>
<td>Recovery Time Objective (RTO)</td>
<td>Recovery time objective is the duration of time needed for restoring of data after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.</td>
<td>4. Days</td>
<td>N/A</td>
<td>N/A</td>
<td>4. Days</td>
<td>3. Hours</td>
<td>4. Days</td>
<td>4. Days</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Recovery Point Objective (RPO)</td>
<td>Recovery point objective is the duration of data loss that could be tolerated in fault situations.</td>
<td>4. Weeks</td>
<td>N/A</td>
<td>N/A</td>
<td>3. Days</td>
<td>2. Hours</td>
<td>4. Weeks</td>
<td>3. Days</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Content Type</td>
<td>The type of content to be stored, i.e. mostly binary data, or text data.</td>
<td>1. Text</td>
<td>1. Text</td>
<td>1. Text</td>
<td>1. Text</td>
<td>1. Text</td>
<td>2. Binary</td>
<td>1. Text</td>
<td>1. Text</td>
</tr>
</tbody>
</table>

Figure 11: General Data(base) Requirements
2.1.2.1.2 List of Data Security Requirements

Security requirements comprise confidentiality and integrity properties. Please note that availability is already covered in the previous chapter.

Data confidentiality requirements are the following:

1) Top Secret
   Highly sensitive internal information that could seriously damage the organization, if such information is made public.
   Examples: Disclosure would cause regulatory or contractual liability (e.g. violation of privacy regulation), disclosure would cause severe damage to the reputation or the public image of the organization, disclosure would cause a severe loss of market share or the ability to be first to market, disclosure would cause a loss of an important customer, shareholder, or business partner, disclosure would cause a long-term or severe drop in stock value.

2) Secret
   Sensitive internal information that, if made public or even shared around the organization, could have a severe adverse effect on organizational operations or organizational assets.
   Examples: Disclosure would cause severe damage to operations, e.g. a medium-time system outage, disclosure could cause moderate damage to the organization, disclosure could cause a loss of customer or shareholder confidence, disclosure could cause a temporary drop in stock value.

3) Confidential
   Information of a proprietary nature, normally for proprietary use to authorized personnel only. The unauthorized disclosure of information could be expected to have an adverse effect on operations, assets, or individuals.
   Examples: Disclosure might provide a business advantage over those who do not have access to the same information, might be useful to a competitor, might reveal operational details or information on individual (private) preferences.

4) Sensitive
   Information not approved for general circulation, but freely available within the organization, e.g. not generally known outside the company or available from public sources.
   Examples: Disclosure is unlikely to result in financial loss or damage to operations, assets or individuals.

5) Public
   Information in the public domain, approved for public use inside and outside of the organization.

Data integrity requirements are the following:

1) High
   Highly essential information that could have a catastrophic adverse effect on the organization or the solution as a whole, if unauthorized modification or destruction of information occurs.
Example: (root) certificate, operator passwords.

2) Medium

Medium essential information that could have a serious adverse effect on the organization as a whole, major parts of the organization or (groups of) individuals if unauthorized modification or destruction of information occurs.

Examples: user passwords, etc.

3) Low

Non-essential information that could have very limited to no immediate adverse effect if the unauthorized modification or destruction of information occurs.

Examples: Logging data.

2.1.2.1.3 List of Regulatory and Compliance Standards Requirements

Regulatory and compliance standards requirements are the following:

1) Location

Location means whether there is a need to provide choices on e.g. country level, EU.

2) Archiving

The need to archive the data due to regulation or compliance standards.

2.1.2.2 Potential WP2 Use Cases

At present there is no final description from WP2 on how the cloud will be used in the context of the Integrity Protection (IP) cluster. Potential use cases are the following:

1) Software repository for initial installation or upgrade of mobile network elements

Original network element software as well as updates, patches etc. are stored in the cloud.

The software repository for network elements may be implemented in either the collaborative or the operator cloud, or both.

2) Backup and restore of individual configuration settings for mobile network elements

Individual configuration settings of mobile network elements (configuration files, databases etc.) of mobile network elements are stored in the cloud for backup and restore purposes.

The network element backup/restore functionality may be implemented in the operator cloud.

3) Software repository for mobile end devices

Original end device software and software updates for mobile end devices are stored in the cloud.

The software repository for mobile end devices may be implemented in either the collaborative or the operator cloud, or both.

4) Backup and restore of individual settings for mobile end devices

End users can use the cloud to save individual settings (files, databases etc.) of their mobile devices.
The end device backup/restore functionality may be implemented in either the collaborative or the operator cloud, or both.

5) Blacklist for compromised mobile end devices

Mobile end devices compromised with malicious software may be blacklisted for isolation from the network. Blacklists may be distributed between network operators. Blacklists are subject to both collaborative and operator clouds.

6) Storage of malware samples

Malware samples collected in some sensor elements (e.g. honey-pots) can be stored in the cloud for further investigation.

Malware samples are most likely only stored in operator clouds.

7) Storage of malware patterns

Malware Pattern (i.e. recognisable patterns that can be searched for) can be stored in the cloud. The patterns may be shared between network operators.

Malware patterns may be subject to both collaborative and operator clouds.

8) Log information of SW integrity protection functions for network elements

Negative log information, such as “Integrity check failed for SW module xyz”, as well as positive log information such as “system boot successful”, “remediation successful”, etc. may be stored in the cloud.

Log files are stored only locally in operator clouds.

9) Validation data (potentially data which needs to be protected)

If not contained in SW repositories additional data may be needed for validation, e.g. trusted reference values / signatures / certificates / policies

10) Results from malware analysis, in analogy to 8)

11) Disinfection tools (regarding malware clean up)

### 2.1.2.3 Potential WP4 Use Cases

Potential use cases for measurement and analysis (MA) are the following:

1) Local security dashboard

As aforementioned the local security dashboard offers a visualization of the health and security status for one mobile network operator. Thus it is necessary to collect and store sensor data for the preparation of such a dashboard. Based on the amount of collected data, their respective security requirements and also the diversity on persistency requirements, i.e. short, middle or long term persistence for fulfilling compulsory archiving or enabling audits and forensics, storing within the operator cloud may be advantageous compared to classical storage systems like database clusters or storage area networks also by economical needs.

Because of the criticality of the highly sensitive sensor data belonging to one mobile network operator, the fulfilment of high data security requirements is mandatory.

2) Global security dashboard

As aforementioned the global security dashboard offers visualisation of the overall health and security status for participating parties in the ASMONIA Collaboration Network. Thus it is necessary to collect and store available, preprocessed data of
mobile network operators for the preparation of such a dashboard. This data is collected via the collaborative information exchange. In addition, further information, i.e. vulnerability reports from vendors, CERT-information from governmental organizations and other information from participating third parties within the ASMONIA Collaborative Network, has to be collected via a defined interface. Both, operator status information and additional enrichment information have to be kept ready for the preparation of the global security dashboard. By means of security, especially integrity and availability requirements have to be fulfilled as long as security mechanisms for the collaborative information exchange are adequate and intact.

2.2 Cloud as a means to enhance Availability of Telco Components in Overload and Outage Situations

Figure 12 gives a rough overview over the ASMONIA architecture and the involved clouds, the operator cloud and the collaborative cloud. For more information on the general ASMONIA architecture refer to the deliverable of work package 1.

While both clouds may be used to enhance availability in overload and outage situations, only the collaborative approach of ASMONIA is evaluated, because the optimization of cloud computing systems for operator internal use is not in the focus of ASMONIA. Nevertheless principles, valid for the collaborative cloud, may also apply for operator clouds.

Running of telecommunication applications in the collaborative cloud is more a side line of the ASMONIA research project. It is not directly needed for the main task that is to detect and to mitigate attacks against 4G mobile networks. But one task of the collaborative cloud in the context of ASMONIA is to provide complementary backup storage capabilities for

- the SW of network elements including updates, patches, configuration files, etc.
• images of network elements as Virtual Machines
• databases used in mobile networks

The idea of running telecommunication applications in the collaborative cloud occurred when looking at the bullet ‘complementary backup storage for images of network elements as Virtual Machines’. Why shouldn’t Virtual telecommunication Machines – already stored for purposes of complementary backup in the collaborative cloud – be used to also run in the collaborative cloud and thus diminish the consequences in overload and outage situations as a consequence of attacks against the 4G mobile network? To evaluate the consequences and the requirements will be the task for future work.

For the considerations concerning overload and outage situations it doesn’t matter from a high level point of view whether the collaborative cloud is

• a central cloud, located apart and physically separated from the operator clouds
• a distributed cloud, located inside of the operator clouds, being only logically separated and shared between the associated operators

These are the two main variants, currently discussed in work package 1, which discusses the overall ASMONIA architecture. For more details about the pros and cons of collaborative cloud architectural issues, please refer to the deliverable of work package 1 and to chapter 4.

Regardless whether a central or a distributed cloud architecture is used, the provisioning of ‘overload/outage network capabilities in the collaborative cloud’ has stringent requirements concerning the operator’s original mobile network.

To run in a cloud requires that the corresponding network elements already exist at least in a virtualized form in the mobile operator networks. It can generally not be assumed that mobile network operators will provide in addition a virtualized network element for the collaborative cloud as backup for its traditional counterpart in the mobile operator network. Therefore it is indicated in Figure 12 that at least parts of the operator’s mobile network are at least virtualized and may already run in the operator cloud.

It is also indicated in Figure 12 that not all parts of the mobile network are equally suited for backup in the collaborative cloud in overload and outage situations. As the periphery of the
mobile network (the eNBs) is highly distributed and has furthermore strict latency requirements, it makes no sense to backup these network elements in the more or less central collaborative cloud. And even for the case that an eNB is out of service, only a limited part of users will be affected. Therefore the central parts of the mobile network, that is the Evolved Packet Core and the Packet Data Networks (in this example IMS) are generally seen more applicable to run in the collaborative cloud in overload and outage situations.

But analyzing the central parts of the mobile network and the advantages of a cloud a little bit more in detail leads to the conclusion that not all kinds of traffic are suited to be located in the collaborative cloud. Clouds provide an impressive processing power and are therefore more suited to run network elements that are computationally intensive which applies to the signaling part of the mobile network. It is not intended to run media related network elements in the collaborative cloud because these require a large bandwidth and only a limited processing which is a rather unusual application for a cloud. Therefore the collaborative cloud in ASMONIA is not seen as a kind of transport network.

If the collaborative cloud is envisaged to host critical telecommunication applications like signaling servers or even the HSS, it is stringently required that it is a private cloud with full control over the security features. Community clouds are a special form of private clouds where the capacity of the community cloud is shared between multiple members and where the members with access to the community cloud can be controlled.

Before starting with the overload and outage scenarios, a rough definition of ‘overload’ and ‘outage’ is given in the context of ASMONIA. Overload and Outage situations in the original operator mobile network are related to each other in the following way:

Either a network element, parts of or even the whole network – usually in the state ‘normal’ (see Figure 14) – may transit into the state ‘overload’ or ‘outage’. This may be due to increased user traffic (e.g. at a specific time of day when the resources are not adequate), due to technical failures (like power outages or SW failures) or due to the results of an attack. In the context of ASMONIA the consequences of an attack on the mobile network are in the main focus.

The right part of Figure 14 shows an example of a potential overload/outage scenario. As a result of an attack network elements, parts of or even the whole mobile network may first get in an overload situation and if the attack is powerful enough, there may be a complete outage. During the course of an attack, the mobile network will usually not stably remain in one state but may toggle e.g. between ‘overload’ and ‘outage’. The state ‘outage’ denotes the worst state, where after a gradually decreasing of resources in the state ‘overload’ finally no resources are available at all in the original operator mobile network to deliver the contractually agreed service for the subscribers.
The availability of 4G mobile networks in overload and even more in outage situations can be significantly increased by providing additional resources in the form of telecommunication virtual machines in the collaborative cloud. In case of a massive DoS attack it may be required that the collaborative cloud provides a multitude (e.g. 5 times) of the resources that are available in the original mobile network.

Thereby it is not even aimed that the collaborative cloud provides full performance under all conditions. In outage situations, potentially also emergency situations, the collaborative cloud might deliver only a rudimentary service functionality (e.g. basic voice service) and perhaps only for a reduced range of customers (e.g. VIPs, emergency services).

The mechanisms mentioned above primarily improve the availability of 4G mobile networks. But the availability can further be improved, if the security of the network elements against DoS attacks is enhanced. The security, e.g. in emergency situations, can be enhanced by reducing the code of the telecommunication virtual machines to the required rudimentary functionality thus reducing the attack surface. Nevertheless it may be possible that the exploited vulnerability is exactly in the remaining rudimentary code and in this case the additional resources in the collaborative cloud can as well be attacked as soon as they appear in the mobile network and the outage or emergency situation is only short-termed mitigated. This effect can only be significantly diminished if the telecommunication VM resource in the collaborative cloud is based on a different implementation compared to the operator’s mobile network.

### 2.2.1 Overload and Outage Scenarios for the Collaborative Cloud

The complex network architecture (refer to Figure 15, Figure 16 and Figure 17) of the mobile operator network enables a wide variety of single or concatenated overload and outage scenarios. It is impossible in the context of ASMONIA to evaluate all of them. Therefore three scenarios in the IMS part of a 4G mobile network will be selected as examples. The scenarios range from an overload situation of a single network element (Application Server, AS) over an outage situation of a single network element (Home Subscriber Server, HSS) up to a complete outage of a part of the 4G operator network (IMS signaling part). Scenario 1 was selected because it is very probable that attacks will be directed against application servers. Scenario 2 was selected because attacks against the HSS will have fatal consequences: the complete outage of the 4G mobile network. Scenario 3 was selected because the IMS part of the 4G mobile network will be most challenging concerning performance requirements for the collaborative cloud.
Scenario 1: Overload Situation of an Application Server

The collaborative cloud can be used to provide additional capacity in overload situations. An application server (AS) in IMS, e.g. for messaging, conferencing, video is taken as an example for overload situations.

In the context of ASMONIA – trying to detect and to mitigate attacks against 4G mobile networks – it is assumed that the overload situation is the result of a DoS attack on the application server. It is furthermore assumed that either the DoS attack is not powerful enough or that the application server has built-in defense mechanisms to remain permanently in the state ‘overload’ without going to ‘outage’. Although the worst case ‘outage’ is avoided, the consequence for legitimate users is nevertheless that the service may be significantly impaired.

Scenario 1: AS Overload

→ provide additional capacity in overload situations

Overload situations can of course also occur due to under-dimensioning of resources in the original mobile network. A significant difference to the case ‘under-dimensioning of resources’ is that it needs a multitude of the resources, initially provided in the original mobile network, to mitigate a DoS attack. This puts the requirement on the collaborative cloud that it has to provide a high degree of elasticity for the hopefully relatively rare incident of a DoS attack.

The collaborative cloud seems during ‘normal’ operating conditions only to a certain extent suited as a resource extension for tightly dimensioned mobile networks in order to save money for resources that are only rarely needed, e.g. at the peak-time of a day or at the turn of the year at 0:00. The property of these events is that they occur usually simultaneously for all operators. This means in case of a distributed collaborative cloud architecture (see Figure 13) that all operators would try to get collaborative cloud resources from the associated operators at the same time. To solve the suddenly occurring demand of concurrent resources requires a large elasticity of the collaborative cloud which is in contrast to a tightly dimensioning. Therefore the usage of (tightly dimensioned) collaborative cloud resources is more suited for asynchronous overload events like for example a marketing campaign via SMS messages that might lead to bottlenecks in the messaging servers.
The usage of the collaborative cloud requires some pre-requisites:

- a traffic element (e.g. load balancer) in front of the application server has to distribute the traffic between the application server in the original mobile network and the additional application server in the collaborative cloud
- the lines between the original mobile network and the collaborative cloud must be available to enable a fast reaction
- the management must detect the overload situation in the original mobile network and must activate the additional resources in the collaborative cloud

**Scenario 2: Outage Situation of a Home Subscriber Server**

Figure 16 shows the next scenario, the outage of a single mobile network element like the Home Subscriber Server. This is a gradual increase of the overload scenario. If the DoS attack is powerful enough, the HSS may go completely and perhaps for a longer time in the outage stage.

**Scenario 2: HSS Outage**

⇒ provide backup network element functionality in outage situations

![Figure 16: Scenario 2 – HSS Outage](image)

The HSS contains the user profiles and is necessary for every connection setup. An outage of the HSS means that this resource is no longer available and that the original mobile network will therefore be completely blocked until the HSS gets again into operation. Depending on the duration of the outage this may lead to a significant economical loss for the operator and perhaps to a loss of reputation.

In this situation it would be advantageous to have access to resources in the collaborative cloud, independent from the original mobile operator network. Even if the HSS resource in the collaborative cloud is not able to replace the complete functionality of the original HSS, something like a reduced emergency operation could be provided.

While this solution sounds reasonable from a high-level point of view, there are a lot of unsolved details that have to be evaluated during the ASMONIA research object like for example:
• The HSS is a special purpose HW with specialized security solutions that cannot be 1:1 virtualized. It has to be evaluated whether it is possible to achieve a comparable grade of security with other mechanisms.

• Another problem is that the HSS needs permanently updates of e.g. location or user profile information. But permanently updating requires that the HSS in the collaborative cloud is already permanently active and visible before the outage situation occurs. This is somewhat in contrast to the envisaged approach. Therefore it has to be evaluated whether it is possible to keep the HSS in the collaborative cloud passive and to actualize its databases only in larger intervals (e.g. once a day). As a consequence it is not possible that the HSS in the collaborative cloud replaces the original HSS without a noticeable interruption. In case of an outage the HSS starts with a somewhat out-dated database (one day old) without valid location information so that most of the terminals have to re-register and with the consequence that the latest changes in the user profiles will not be contained in the database.

• As already indicated, the substitute HSS in the collaborative cloud might only provide a reduced performance compared to the original HSS, a kind of emergency operation. But this requires additional functionality in the substitute HSS: either a restriction of services in the user profile or a limited number of users or both. A limitation of users which means either a priorization or a random selection of users is a new property of a mobile network and although technically feasible, it will nevertheless raise new legal questions for the operator.

With the HSS one of the most important and one of the most challenging network elements of a 4G mobile network was selected as an example for the outage scenario. From a today’s point of view it is completely open whether and to what extent the proposed scenario can be realized. This has to be evaluated in the further course of the ASMONIA research project. But even if it is impossible to realize the outage scenario for the HSS, it may nevertheless be possible to realize it for less critical network elements like for example charging servers.

Scenario 3: Complete Outage of the HSS Signaling Part

Figure 17 shows the third scenario where not only a single network element but a complete part of the mobile core network – the IMS signaling part – goes into the outage state and shall be replaced by its counterpart in the collaborative cloud. After activation the IMS signaling part in the collaborative cloud bypasses the original mobile network completely.
**Scenario 3: IMS Sig Part Outage**

- provide backup signaling part functionality in outage situations

---

**Figure 17: Scenario 3 – IMS Signaling Part Outage**

The management of the shared cloud resources (refer to chapter 2.2) has

- to detect the outage of the IMS signaling part
- to activate the IMS signaling part in the collaborative cloud
- to organize the switchover of the signaling traffic from the original mobile network to the collaborative cloud

In contrast to scenario 1&2 there is now an additional requirement concerning the network resources in the collaborative cloud. Background is that the collaborative cloud has now to provide the internal network resources to route the IMS signaling traffic between the different VMs (P/S-CSCF, HSS, ASs, I-CSCF) with the corresponding bandwidth and latency requirements. Integrity and potentially confidentiality have as well to be ensured for the collaborative cloud internal traffic.

**Discussion of Scenario 1 to Scenario 3 in the context of the Collaborative Cloud**

The advantage of the Collaborative Cloud in overload and outage situations is mainly that it provides additional resources (compute, network, storage) by its elasticity and thus maintains the availability of the 4G mobile network. Elasticity is an important aspect because in case of DoS attacks a multitude of the resources (e.g., 5 times) may be needed. This elasticity can be easier provided in a collaborative cloud (shared between multiple operators) than in a single operator network.

The sharing of resources such as a collaborative cloud mostly implies also the reduction of costs. But it is currently not clear whether a cost reduction can be achieved because on the other side additional expenditures are necessary like for example a network connecting the operator cloud. These aspects are discussed in more detail in the next two subsections.
2.2.2 Connecting the Operator Cloud with the Collaborative Cloud

It is by far easier to run the telecommunication resources in the collaborative cloud than to connect the original mobile network with the telecommunication resources in the collaborative cloud. For that multiple aspects have to be considered.

In order to enable fast reactions in overload and outage situations, the lines to the collaborative cloud

- must already be available
- must provide sufficient bandwidth to guarantee the availability of the additional collaborative cloud resources
- must provide low latency to fulfill signaling traffic requirements

To get a predictable QoS and an ensured availability of the telecommunication virtual machines in the collaborative cloud, the connectivity of the Public Internet must not be used for interconnection because it delivers only ‘best effort’. Therefore a dedicated transport network with specified requirements (large bandwidth, strict latency and high availability) and the corresponding costs is permanently necessary, although it is only used in hopefully rather rare overload and outage situations. As a consequence also the vulnerabilities and the failure probabilities of the transport network between the original mobile operator network and the collaborative cloud must be taken into consideration.

On the other hand it was one of the main design principles of the Internet to deliver connectivity even during emergency situations due to a distributed design. Therefore it could be taken into account to use the Public Internet as the last choice, if also the envisaged transport network to the collaborative cloud is affected by the DoS attack. Pre-requisite is that the integrity and confidentiality requirements of the traffic can be fulfilled, e.g. by a VPN tunnel. For critical traffic between the original mobile network and the collaborative cloud, e.g. in case of a HSS outage, it may not be acceptable to use the Internet as last choice because of security concerns.

It is also stringently required that the integrity of the traffic to/from the collaborative cloud is ensured. Integrity means: the identity of the resources in the collaborative cloud must be reliably identified (authentication) and the traffic must remain unchanged. If the traffic contains private user data like addresses, telephone numbers or even complete user profiles the traffic must be additionally encrypted so that also the confidentiality of the traffic is ensured.

Although the definition of the ASMONIA Collaboration Gateway (ACGW) is done in work package 1, it is assumed that only the management of the telecommunication resources in the collaborative cloud will be performed via the ACGW and that the signaling traffic towards the collaborative cloud will bypass the ACGW due to performance reasons. The management of the shared cloud resources – that are the mobile operator networks and the collaborative cloud, potentially operated by an independent operator – are evaluated in chapter 2.2.

2.2.3 Practical Operator Considerations for the Collaborative Cloud

Besides the alluring possibilities that may be offered by the collaborative cloud, a telecommunication operator has also to consider practical aspects like the reliability or the security of a solution, the compliance to legal regulations, cost aspects and so on. Some of these practical considerations will be discussed below.
Is any kind of private cloud suited for the Collaborative Cloud?

As mentioned before, especially telecommunication applications with real-time requirements may not be suited to run on any type of private cloud without optimizations. For setup of connections via signaling there are strict latency requirements that must be fulfilled under all conditions. Therefore it may be required that the collaborative cloud has to be optimized for the envisaged telecommunication scenarios and that the usage of any standard private cloud will only be possible in the further future.

Who is the operator of the Collaborative Cloud?

This is a central question for the associated operators. One proposal is that the collaborative cloud is operated by a neutral instance where neutral instance is usually seen as a governmental operator. But this would be a big problem for the telecommunication operators in the context of user data preservation. A better solution from the telecommunication operator’s point of view would be to launch a common company of the associated operators to operate the collaborative cloud.

Security Considerations

Despite of the fact who is operating the collaborative cloud, security considerations and especially data privacy are generally a fundamental problem and a big challenge for a specific operator when using an external collaborative cloud. In the collaborative cloud the networks of different telecommunication operators and perhaps even of non-trusted telecommunication operators are connected. But telecommunication operators must be compliant to legal regulations (in Germany first of all the ‘Telekommunikationsgesetz, TKG’) and they are liable to adhere to these legal regulations. Therefore it is a stringent requirement that the networks of the different telecommunication operators in the collaborative cloud are strictly isolated from each other so that data privacy is guaranteed. This means that the collaborative cloud must be TKG-compliant.

Miscellaneous

The argument for a collaborative cloud usually is that the sharing of resources between multiple operators will offer cost advantages. But if looking closer to the telecommunication scenarios in overload and outage situations there are also some effects that may diminish or even neutralize the cost advantages.

The close connection of telecommunication operator clouds with the collaborative cloud and the relying on telecommunication resources in overload and outage situations requires something like regular functionality tests. This kind of functionality tests are expensive and may diminish the effectiveness of the collaborative cloud.

In case of outages as a result of a DoS attack usually a multitude of the resources of the telecommunication operator cloud (e.g. 5 times more resources) is necessary in the collaborative cloud to mitigate the DoS attack. This requires high bit rate lines for the interconnection between both clouds that must be permanently available and cause therefore also permanent cost.

To use different implementations of the same application in the telecommunication operator cloud and in the collaborative cloud in order to increase the security in case of attacks (thereby hopefully avoiding having the same vulnerabilities) has as well some practical impacts. It will usually be more expensive to provide two different independent implementations of the same application. A further aspect is: If the applications in the telecommunication operator cloud and in the collaborative cloud are really different, then
intensive and therefore expensive inter-operability tests are required in advance and they must be repeated with every upgrade.
3 Management of shared cloud resources

The management of shared cloud resources describes the functionalities that a cloud computing system needs to offer in order to provide a customer – be it a person or a computer system – with resources. This chapter is not intended to be a full description of the functionalities of a typical cloud computing system and it will not describe every functionality in detail that is needed to provide resources. We will focus on certain aspects that are if not really unique then at least very specific for a cloud computing system used in ASMONIA that is capable of supporting the cloud scenarios presented in chapter 2.

As explained earlier in Chapter 1.3, we expect two different types of cloud systems to exist in the ASMONIA context, i.e. a collaborative cloud and one or several operator clouds. Each of the cloud systems needs to have its own management of shared resources, yet for mobile network operator one single system for the management of his cloud resources is desirable. Hence, there will be the need for the management systems of the different clouds to exchange information.

The usage of cloud systems in ASMONIA is strongly motivated by the desire to enhance the availability and the security of the infrastructure in a mobile network operator environment. The functionalities defined here in form of use cases reflect this motivation.

1. Moving a telecommunication component into a cloud
2. Moving a virtualized component to another cloud
3. Scaling a component in a cloud
4. Generating free resources through redistribution

In this chapter these use cases and the requirements they imply will be discussed in more detail.

3.1 Moving a telecommunication component into a cloud

This use case describes how an infrastructure component of a mobile network operator is transferred from the physical infrastructure into a virtual environment provided by a cloud. At the current stage it has not been decided upon, which telecommunication components are most suited for a replacement with virtual ones. But as the non-functional requirements and the security requirements strongly depend on the actual component to be transferred, it is not possible to describe them here in full detail. This chapter will focus on the description of the functional requirement, i.e. the use case, and point out some issues that require further investigation.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Moving a telecommunication component into a cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The system administrator substitutes a virtual telecommunication component for an existing telecommunication component.</td>
</tr>
<tr>
<td>Actors</td>
<td>System administrator</td>
</tr>
</tbody>
</table>
| Assumptions                                  | • For the physical telecommunication component exists a virtual image  
                                              | • The virtual image of the telecommunication component is up to date  
                                              | • The telecommunication component does not need special hardware |
A virtual environment (a cloud) is available, in which the virtual image can be started.

**Steps**

1. The administrator tells the system which component he wants to replace, and also which virtual image he wants to use as a substitute.
2. The system starts the virtual image containing the virtual component.
3. The system configures the network, substituting the ip address of the virtual component for the address of the physical component.
4. The system shuts down the physical component.

**Variations**

Depending on the actual physical component, which is going to be replaced, the steps may differ.

**Non-functional**

The non-functional requirements depend on the actual physical component, which is going to be replaced.

**Issues**

- Handling and deployment of virtual images (see section 3.1.1)
- Choosing an adequate virtualization method (see section 3.1.2)
- Network issues (see section 3.1.3)
- Privacy and data issues (see section 3.1.4)
- Implementation and Interoperability issues (see section 3.1.5)

This chapter focuses on the virtualization of telecommunication components as the second cloud scenario evolves mainly around those. But in a more general sense this use case can be adjusted to cover all sorts of backend components and as such support both cloud scenarios. But as the telecommunication components are more specific for ASMONIA this generalization is left out here.

### 3.1.1 Handling and deployment of virtual images

Generally there are two possibilities when a component is going to be replaced with a virtual component. Either the virtual image already exists, i.e. has been created beforehand, as described above in the use case. Or the virtual image needs to be created right before the replacement takes place.

The following steps describe the general process for the creation of a virtual image:

1. Choose suitable operating system (i.e. Linux or Windows)
2. Determine needed performance and configure the virtual machine
3. Start the virtual machine
4. Install the application or copy the application to the virtual machine
5. Copy the latest data to the virtual machine
6. Save the virtual machine image

This process can either be used for the just-in-time creation of images or for a creation of the images beforehand. Both approaches will be discussed in the following sections.
Just-in-time creation

The advantage of creating images just-in-time is that the image is always up-to-date. There is no additional effort involved in order to keep the application data up-to-date. But of course there is also a downside, and this is the time aspect. The creation of an image takes some time, and especially in usage scenarios dealing with overload and outage situations time matters.

Although challenging, it does not seem impossible to implement a solution using just-in-time creation of the virtual image. This includes the choice of steps that can be prepared with little effort in order to gain time for the replacement process.

A problem of this approach is that if the component to be substituted is compromised, the virtual component will also be compromised.

Prepared Images

Another possibility is to prepare the images beforehand and store them ready for whenever they are needed, e.g. an overload or outage situation occurs. The advantage of this approach is the reduced time effort for the actual substitution. The virtual image is already prepared and ready to use. Another advantage is that if the component has been compromised it is not necessarily the case that the virtual component is also compromised.

The downside of this approach is the effort needed to keep the application data up-to-date. A point for further investigation here is to find out, what is an acceptable compromise between updating an image and running on old versions. In some outage situations it might be sufficient to restore a basic infrastructure and basic services.

3.1.2 Choosing an adequate virtualization method

The section above already discussed the creation of virtual images. But it focused on the point of time and the duration of the creation. This section will discuss some possibilities concerning the way how a virtual image is created.

Essentially there are again two different methods. Either the virtual image is created of the entire component, or a virtual image of the required operating system is created and the applications representing the functionalities of the telecommunication component are copied or installed into this image. The former has the advantage that there is no additional effort needed for the creation of the virtual image. There is no need to customize the operating system, assuming this has been done before, when the applications were installed. And the application data is also up-to-date. But depending on the frequency of changes in the application data, this might turn out to be a disadvantage, namely if the application data is already outdated at the time the creation of the virtual image is done. Additionally if the component is corrupted at the time the virtual image is created, the image will also be corrupted.

In the latter case, when the virtual image is created of a clean operating system, there is additional effort involved. The operating system might need to be customized or hardened, the application needs to be installed and up-to-date application data need to be copied. Yet this creation process inherits a certain modularity and allow that certain steps are being prepared well ahead before they are needed.

3.1.3 Network issues

When moving telecommunication components into a cloud one should note that additionally to compute resources network resources are needed. The demands on the network resources may vary. It's possible that there will be the need to have a certain guaranteed
network bandwidth or latency from the compute resources to the mobile provider network or that the compute resources need a guaranteed network bandwidth or latency to other compute resources in the cloud.

Depending on the architecture of the cloud, both issues might turn out to be quite complex (see chapter 4.1.2). Nevertheless, without a further detailing of the requirements regarding network connections this issue cannot be resolved. But as the requirements depend on the actual telecommunication component that is going to be transferred to the cloud, we can only state that this is the starting point for further investigation.

3.1.4 Privacy and data issues

Depending on the telecommunication component that is replaced with a virtualized one it is possible that customer data is also transferred into the cloud. If the cloud is under the jurisdiction of the operator, i.e. an operator cloud, and only accessible from inside the mobile operator network this is not an issue. But if this is not the case and the component is transferred into a collaborative cloud or any other cloud that is beyond the borders of the mobile operator network this becomes an issue.

The reason why this becomes an issue worth discussing has to do with some regulatory requirements (see chapter 7) that regulate the handling of personal data. Additionally, the storing of customer data outside the boundaries of its network is something that to the best of our knowledge no mobile operator has done before.

3.1.5 Implementation and Interoperability issues

The use case presented in this chapter is one of the basic functionalities needed for the ability to mitigate overload and outage situations through the use of cloud computing systems. So far so good, but if a telecommunication component in its physical existence is vulnerable for a certain attack, its virtual existence will be vulnerable for the same attack. So in the case of an outage situation caused by an exploit of a vulnerability the virtual component that is started to mitigate the outage will be attacked immediately and sent kingdom come.

One possible solution to resolve this issue is to use a different implementation of the telecommunication component in the cloud, i.e. the implementation of the physical component and the implementation of the virtual component are different. In this case it is at least less likely that both implementations are vulnerable by the same exploit.

But this solution comes with some drawbacks. If two different implementations of one telecommunication component are used alternatively, it is important that all other components of the mobile operator network are able to function with both components without the need to reconfigure them whenever the implementation of the component is swapped.

It also complicates testing of the provider network, which is usually necessary whenever components are updated or changed in some manner. To ensure the correct functioning of the system a system test using all components needs to be executed. Now if two implementations for the same component are used interchangeably the system test needs to run twice with each implementation. This gets more complicated of course the more components are virtualized in this way, for example five components with two respective implementations would result in the need for 32 different combinations for the system test.
3.2 Moving a virtualized component to another cloud

In this use case an already virtualized component is moved from one cloud infrastructure to another. A basic requirement for this use case to occur is the existence of at least two cloud infrastructures that are available for the expected user, i.e. a mobile network operator. In the context of ASMONIA we can assume that this is the case, because as explained in chapter 1.3, we expect the existence of the collaborative cloud and some operator clouds.

Similar to the use case discussed above the requirements depend to a certain degree on the actual component that is moved to the cloud. In the first cloud scenario this could be any backend component, in the second cloud scenario this would be some kind of telecommunication component. But a final conclusion about which telecommunication components are most suited for the use in a cloud has not been reached. So we will focus in this chapter on the functional requirements and point out aspects that require further investigation regardless of which kind of component might be moved.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Moving a virtualized component to another cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The system administrator moves a virtualized component running in a cloud infrastructure to another cloud infrastructure.</td>
</tr>
<tr>
<td>Actors</td>
<td>System administrator</td>
</tr>
</tbody>
</table>
| Assumptions               | • A virtual image of a component is running in a cloud infrastructure  
                           | • The component does not need special hardware  
                           | • A second virtual environment (cloud) is available, in which the virtual image can also be started |
| Steps                     | 1. The administrator tells the system which virtual component he wants to move and to which cloud he wants to move it.  
                           | 2. The system transfers the virtual image of the component to the target cloud and starts the image.  
                           | 3. The system configures the network, substituting the ip address of the virtual component in the new cloud for the address of the virtual component in the old cloud.  
                           | 4. The system shuts down the virtual component in the old cloud. |
| Variations                | Depending on the actual component, which is going to be moved, the steps may differ. |
| Non-functional           | The non-functional requirements depend on the actual component, which is going to be moved. |
| Issues                    | • Duration of the copy process (see section 3.2.1)  
                           | • Handling of old copies (see section 3.2.2)  
                           | • Considering Backups (see section 3.2.3)  
                           | • Interoperability of virtual images (see section 3.2.4)  
                           | • Privacy and data issues (see section 3.2.5) |
3.2.1 Duration and timing of the copy process

Copying a virtual image from one cloud to another cloud cannot be achieved instantaneously. Depending on the size of the virtual image and the network connection between the cloud infrastructures this may take several minutes or even up to hours.

There are actually two main problems with the copy process. Both are somewhat connected to the situation in which one may want to use this use case. The idea behind this use case is that when an overload or outage situation arises and the resources in the operator cloud become scarce it may be useful to be able to shift some of the virtual components already running in the operator cloud – thus using up resources – into the collaborative cloud, where more resources might be available.

Now in an overload or outage situation the network traffic can be expected to be higher than usual. Adding even more traffic by copying one or several components from one cloud to another might not be the best idea. Trying to solve this problem leads to the idea of keeping virtual images ready at hand for whenever they are needed, as a kind of backup system that only needs to start up to be able to take over. Then however the need for a good management of the virtual images arises. Keeping track that the images used for this mechanism are up-to-date is not trivial. It also depends strongly on the component itself, what kind of application data it uses and how often this data changes. It will require further investigation which components are suitable for such a mechanism.

The other problem that has already been mentioned is the duration of the copy process. Without further external pressure a duration of the copy process in the range of minutes or hours is only somewhat annoying, but in an overload or outage situation such a duration is simply not acceptable. But this problem is related to the problems discussed in section 3.1.1 and solutions for those problems might also be applicable to the situation here.

3.2.2 Handling of old copies

The moving of a virtual component is realized by copying the virtual image from one cloud to another. Usually the difference between moving a file and copying a file lies in the fact that the original file is deleted when the file is moved whereas it remains untouched when it is copied. So far it is not clear how this should be handled when a virtual component is moved, both methods seam feasible.

When the original file is deleted, no further thought needs to be spent on how to keep the original image synchronized with the new image that now represents the active telecommunication component. This comes at the price that the same copying process needs to be executed when the telecommunication component is moved back. And we expect this to be the most common case, because our rationale behind the use case states that the use case can be used as a means to mitigate an overload situation. As such the implication is that after the overload situation is resolved the component can be moved back into the original cloud.

3.2.3 Considering Backups

As already mentioned above (refer to 3.2.1), the network resources might be the most affected part in an overload or outage situation and adding more traffic by copying one or more virtual components from one cloud to another might not be a good idea. One idea to solve this problem might be to use the cloud as a backup system for the virtual components. The cloud could store backups regularly and use one that is not entirely up-to-date but that would be acceptable for an overload or outage situation in which only a reduced service can be guaranteed, to realize the moving process. In such a case it’s an interesting question how changes in the application data during the overload or outage situation are tracked and
merged back to the original virtual image in the original cloud. As already mentioned, this usage scenario will require further investigation to find out which components are suitable for such a mechanism.

### 3.2.4 Interoperability of virtual images

In the area of cloud computing it is the case that different cloud systems are using different virtualization solutions. Now, if a virtual image should be transferred from one cloud to another it is possible that the image can’t be started in the new cloud environment, because a different virtualization solution is used.

This problem can be addressed by providing possibilities to convert virtual images from one format to another. Internally a management system for virtual images would most likely use one single format and use import and export functionalities, e.g. to convert the virtual images from the internal format into the format needed for the target cloud system. A good candidate for such an internal format is the Open Virtualization Format (OVF) of the Distributed Management Task Force (DMTF) [OVF]. OVF is a packaging standard for virtual appliances, which can be used to deploy virtual images across multiple platforms.

### 3.2.5 Privacy and data issues

The privacy and data issues that have been described in section 3.1.4 also apply for this use case. But there is an interesting facet in this case. In contrary to the use case “Moving a telecommunication component into a cloud” the telecommunication component already resides in a cloud. This means that the question changes from “is this component allowed to run in a cloud?” to “is this component allowed to run in this specific cloud?”.

### 3.3 Scaling a component in a cloud

One of the central goals when moving infrastructure components from a physical infrastructure into a virtual environment provided by a cloud is to achieve an efficient and easy to use mechanism to scale the components. The requirements for the scaling mechanism depend on the individual components that need to be scaled. In this use case we focus on the general methods needed to provide a scaling mechanism.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Scaling a component in a cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>The system administrator orders the system to add more resources to a selected telecommunication component.</td>
</tr>
<tr>
<td><strong>Actors</strong></td>
<td>System administrator</td>
</tr>
</tbody>
</table>
| **Assumptions**| • The virtual image runs in an virtual environment (a cloud)  
• Sufficient resources for scaling the component are available  
• The component does not need special hardware |
| **Steps**      | 1. The administrator tells the system which component he wants to add resources to and how many resources.  
2. The system adds the appointed amount of resources to the component |
| **Variations** | Depending on the component, which needs additional resources, the steps may differ. |
| **Non-**       | The non-functional requirements depend on the component, which needs |
3.3.1 Choosing a load balancing system

A standard mechanism for the creation of high performance systems is the usage of some form of load balancing. The load balancer essentially acts as a manager passing the requests he receives to any free worker he has registered. The number of workers needed depends on the number of requests the manager receives and typically varies over time.

Another method for load balancing is the usage of a queue. In this case the manager puts every request he receives into one queue. The workers frequently check if the queue holds requests, take them and process them.

Both load balancing methods work best with stateless requests, so that any request can be processed by each worker. Load balancing gets more complicated when user sessions are involved. Whether stateless requests are sufficient or user sessions are needed depends on the actual telecommunication component. Which one of both methods is more suitable for a specific component will also need further investigation.

3.3.2 Identifying overload situations

As mentioned above load balancing is a standard mechanism for systems with high demands on performance. A delicate matter in any load balancing approach is the number of workers available for a load balancer. Depending on the expected load peaks the system has to be designed in a way that it can survive the peaks. If the number of workers is fixed, most of the time the system will either be oversized or undersized.

In a virtualized environment as provided by a cloud the number of workers is an adjustable parameter. If more workers are needed they can be easily added and if too many workers are active their number can be reduced. To realize such functionality it is important to be able to identify possible overload situations. This is usually done by monitoring the system and defining thresholds for some parameters. If a threshold is overstepped some event is triggered and the monitoring system either calls a management system or handles the situation by itself. Typical parameters for a load balancing mechanism are the number of requests received per second and the average response time of the workers.

Such a system should work the other way around as well and make it possible to release resources when they are not needed any more.

3.3.3 Scalability of resources

An important issue in this scenario is the scalability of resources. Depending on the actual component that an administrator wants to scale, the resources needed for the scaling process may differ. We’ll describe shortly which resources there are and how the scaling process looks like:

- **Storage** is the easiest resource to scale. It can be extended or reduced without the prior shutdown of any system or component.
• Cpu and ram cannot be scaled independently. Usually there are only a couple of combinations offered by a cloud environment. And if a virtual machine really needs more cpu power or more ram, it must be shut down first and restarted with the required configuration.

• Scaling network is possible in two ways. Either the underlying physical server has several physical network connections. Scaling the network then results in the virtual machine getting access to another network connection. Or network resources are virtually choked from the first and by scaling the network the threshold is lifted.

• The instance is not really a resource like a cpu or storage. An instance is a virtual machine which is running in a cloud and is using the other resources described in this list (storage, cpu, ram, network). Scaling an instance will most likely be done by adding another identical instance and balancing the load between the old and the new instances.

3.4 Generating free resources through redistribution

This use case deals with a problem rarely discussed in the cloud computing context: The problem of what to do, when there are no more resources available to allocate. In the ASMONIA context this question is highly relevant simply because we expect that we will have to deal in most cases with private or community clouds.

Although it is possible to own a private cloud that has enough resources so that this use case may never occur, it is more likely that a private cloud will have to deal with this problem at some point. If no more resources are available to allocate, redistribution must be performed. Therefore it can be useful to prioritize the running and starting components. In the following possible methods to prioritize components and methods for redistributing components are described.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Generating free resources through redistribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The system administrator tells the system how many resources he needs and gets the resources after the system redistributes its resources.</td>
</tr>
<tr>
<td>Actors</td>
<td>System administrator</td>
</tr>
</tbody>
</table>
| Assumptions | • The component runs in a virtual environment (a cloud)  
• The cloud has no more free resources available to either scale or start a component  
• The component does not need special hardware  
• The component has no special regulatory requirements |
| Steps | 1. The administrator tells the system which component he wants to scale or to start and how many resources he needs.  
2. The system checks if there are enough resources to handle the request, but detects that there are not enough resources.  
3. The system checks the priority of the components currently consuming resources from the cloud with the priority of the component the administrator wants to start or scale.  
4. The system tells the administrator that it can free resources by using one of several means on one or more components with low priority. Alternatively: If it discovers that the priority of the request is lowest, it rejects the request. |
5. The administrator chooses from the presented components and means those he wants the system to execute on the chosen components.

6. The system frees the resources by executing the chosen means on the chosen components.

7. The use case “Moving a telecommunication component into a cloud” or use case “Scaling a component in a cloud” is called.

<table>
<thead>
<tr>
<th>Variations</th>
<th>Depending on the current situation in the cloud and the amount of resources needed, the steps may vary.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-functional</td>
<td>-</td>
</tr>
</tbody>
</table>
| Issues | • How to prioritize components (see section 3.4.1)  
• Means to free resources (see section 3.4.2) |

3.4.1 How to prioritize components

When it comes to prioritizing components several aspects come to mind. First of all is the question how the priority of a component can be decided. The priority of component should reflect its importance in comparison to all other components who want to consume resources. This is something we cannot decide, because we currently do not know which components could be moved to the cloud. Also the priorities will most likely depend on the architecture of the provider network and other factors.

Another aspect of priorities is the range of their influence. This needs a little more explanation. The ASMONIA environment consists of multiple users and multiple clouds, i.e. operator clouds and one collaborative cloud. If all users assign priorities to their components in all clouds they use, at a certain point a decision might be needed for a question such as: “Given the component with priority a, is there a component with a priority lower than a?”. Which components in which cloud will now be compared to the priority a?

We decided to allow for two cases. The first one is what we call priorities across users. In this case all components in the same cloud are checked for their priorities when a decision is needed. The second one is what we call priorities per user. In this case only the components in the same cloud that belong to the same user are checked.

Another interesting aspect is the question of who assigns priorities. If the users do so themselves, the doors are open for abuse, simply by assigning all components with the highest priority. Deciding about a suitable system for priorities will be a point of further research.

3.4.2 Means to free resources

After reaching the conclusion that one component has a higher priority than some other components in the same cloud, what is the system supposed to do to free resources?

In the ASMONIA context three means seem possible:

1. Stop a component with low priority
2. Reduce the amount of resources used by a low priority component
3. Move a low priority component into a different cloud
The first possibility seems rather drastic, but quite easy to accomplish. The second one is more generous version of the first, but more difficult to do it right. If too many resources are withdrawn from a component the component itself might stop working. If too little resources are withdrawn this might not be enough to satisfy the request of the administrator.

The third one is the most specific for the ASMONIA context. Realizing that one typical user, a mobile network operator, in ASMONIA has access to two clouds, i.e. his own operator cloud and the collaborative cloud, this new option for freeing resources appears. The situation then is as follows. The operator wants to free resources in one cloud by moving a low priority component into the other cloud. This makes use of the use case “Moving a virtualized component to another cloud” (section 3.2).

When this option is chosen the data and privacy issues arise. Is that specific component allowed to be moved into the other cloud?

These means to free resources and their applicability to the telecommunication components that can be used in a cloud will need some further research.
4 Collaborative Cloud Provider Models

The collaborative cloud concept of ASMONIA has been introduced in chapter 1.3. In this chapter the collaborative cloud concept and various aspects of it are discussed. The focus lies on presenting the consequences one has to face when some high level design questions are solved in certain ways. The cloud computing paradigm can be used in many ways and the resulting security implications depend strongly on the chosen deployment model and the chosen cloud provider. Therefore we will classify the possible deployment models combined with a categorized cloud provider and use this as a basis for an analysis of the resulting security implications. Additionally we will evaluate the feasibility of the presented possibilities.

4.1 Cloud Composition

In cloud computing it is generally agreed upon that the cloud infrastructure is provided by one single cloud provider to a customer, i.e. one company owns the complete infrastructure. And indeed this has been a major difference between cloud computing and grid computing, in which universities and more generally research institutions, share resources in the way that each institution provides some of the resources [FOSTER]. It is debatable if this difference still holds true. The edges are blurring, e.g. a smaller cloud provider in the IaaS domain may rent additional resources from another cloud provider in order to mitigate punctual scarcity of resources.

The composition of the cloud infrastructure in a way similar to grid computing is a valid option for ASMONIA. To be more specific this is a valid option for the collaborative cloud, since this cloud is shared among all the ASMONIA participants. The composition of the collaborative cloud presents a high level design question with consequences, organizational issues as well as technical issues.

4.1.1 Architectural Approaches

We have identified three possible architectural approaches for the composition of a collaborative cloud:

1. Central Collaborative Cloud
2. Distributed Hierarchical Collaborative Cloud
3. Peer-to-Peer Collaborative Cloud

These three architectural approaches and some common aspects of them will be discussed in detail in the following sections.

4.1.1.1 Central Collaborative Cloud

In the central collaborative cloud approach the collaborative cloud is composed of a homogeneous infrastructure regarding hard- and software as well as networking capabilities. The cloud provider exposes its services to the user with a uniform quality of service, regardless of the internal structuring of the cloud infrastructure. This may seem trivial as this exhibits an attribute usually conceived as typical for a cloud. But especially for a collaborative cloud composed of resources residing at the facilities of different companies a guarantee for high bandwidth seems not trivial at all. We will discuss this topic later in section 4.1.2.

The central collaborative cloud offers its services through one central access point. From the perspective of the ASMONIA collaboration network this will simplify the access control. If one dedicated party provides the collaborative cloud, i.e. hosts the complete infrastructure, this party will also hold the responsibility for the correct operation and further development.
Theoretically it is also possible to create a central collaborative cloud by sharing the resources from two or more sharing parties. But in order to realize that all sharing parties need to use the same software to create the cloud infrastructure or they have to use interoperable software, which can create one homogeneous cloud. In the light of missing standards in the domain of cloud computing the latter is deemed to be impossible. Alas, the former also seems problematic, as it forces the sharing parties to deploy some software without having much influence on the choice, or none at all if they join ASMONIA later on. This presents a burden, which might prevent the participation of some companies in ASMONIA.

### 4.1.1.2 Distributed Hierarchical Collaborative Cloud

A distributed hierarchical collaborative cloud is composed of resources from two or more parties. In contrary to the central collaborative cloud approach we expect the inner structuring of the cloud to have an influence on the quality of service especially of the networking resources (see section 4.1.2).

In this architectural approach the collaborative cloud is accessed through one central logical access point. The logical access point constructs an abstraction layer, which is able to communicate with the access points of several different cloud installations. This way the sharing parties may choose the cloud software which fits their needs best, of course with the constraint that the cloud software needs to be supported by the logical access point. An initial set of cloud software will be selected when the logical access point is designed. But the design should also account for the possibility to support additional software later on. Depending on the supported cloud infrastructures it will be necessary to define a certain amount of common services, supported by all infrastructures. These services will then be accessible through the logical access point.
Although the distributed hierarchical collaborative cloud approach only makes the assumption that it is composed of resources from several sharing parties, it is most likely that the resources are provided by some sort of cloud themselves. In any case the collaborative cloud needs a way to communicate with the resource pool in order to consume or free resources.

In a distributed scenario with a logical access point the common resource management of the different clouds needs some thought. First of all, when the access point offers the cloud services to the users it needs some information from the connected clouds about the resources available. This can either be achieved by acting as a broker or by collectively managing the resources of all connected clouds. Acting as a broker would require the access point to query the cloud for available resources whenever a user requests a service. If the access point manages the resources collectively it can answer user requests immediately. The cost for this will be the costs for bookkeeping and for the regular checks to ensure that the stored information is still correct.

From an organizational perspective it seems that in a scenario where all sharing parties are regarded as equals, the existence of a central component such as the logical access point does not fit perfectly well into the organizational concept. Central components need someone operating them, and most likely someone who further develops them. If the responsibilities are not properly distributed and clear to all parties the success of the system is put at risk. But placing the responsibility on one party will distinguish this party from the others and in doing so destroy the equality of the sharing parties.

4.1.1.3 Peer-to-Peer Collaborative Cloud

Usually a cloud provides one point of access from which consumers may access the services provided by the cloud. The architectural approaches presented so far also did the same
thing. They foresaw one single point of access for the services offered by the cloud. But this is not the only possible solution for the design of a cloud, an architecture without any central component is also a valid option and leaves us basically with a peer-to-peer concept.

![Figure 20 Architectural view of the peer-to-peer collaborative cloud](image)

Each cloud that participates in creating the collaboration cloud will need to run an abstraction layer that allows the communication between the clouds and some sort of shared resource management. If the access points of all connected clouds exchange information and are able to consume services from each other than an ASMONIA user might use any of the access points to consume any service in the collaborative cloud. In that way the central access point is also eliminated and with it a potential bottleneck and single point of failure.

### 4.1.2 Homogeneity regarding network resources

During the discussion of the architectural approaches the aspect of homogeneity in a cloud infrastructure was already mentioned. In this document the term homogenous cloud denotes a cloud, whose inner structuring does not have any influence on the quality of service of its provided cloud services.

In a way a cloud (IaaS) represents a resource pool with different kinds of resources, most often called storage, compute and network resources. These can be provided in different flavors, e.g. compute resources with one core, compute resources with two cores, etc. The flavors are presented to the user and whenever he requests a resource he does so by requesting a certain flavor of it. Yet which physical resources are used for the user request the service defined by the flavor of the resource is not influenced. This is a general assumption made in cloud computing. For the cloud scenario presented in chapter 2.2 the network resources are the most important resources. Thus the term homogeneity was used in order to be able to describe the expected aberrations from this standard assumption when discussing the architectural approaches.
We assume that a collaborative cloud created by using the central collaborative cloud approach will be homogenous. Contrary to that, we expect both other approaches, i.e. the distributed hierarchical collaborative cloud approach and the peer-to-peer collaborative cloud approach, to result in inhomogeneous cloud infrastructures. Therefore we assume that the way how resources are allocated will become important, so that the need for an investigation of suitable allocation algorithms arises. Also the flavors in which network resources can be offered as a resource for the users will need further inquiry. Deciding on certain values of bandwidth will not suffice, there may also be a need for a more detailed split-up, e.g. in intra-cloud network bandwidth and user-to-cloud bandwidth. The user-to-cloud bandwidth becomes an especially important point in the peer-to-peer approach, when there are more than one possible access points for a cloud user.

4.1.3 Dynamics of resource allocation

In cloud infrastructures the provisioning of the requested resources is an important issue and generally deals with the amount of time needed for the provisioning and potential limits, which try to ensure that the service is not damaged by excessive resource consumption. However this section will not discuss these topics. They will be further investigated in future research, when the design of the cloud infrastructure in ASMONIA will become more concrete. The goal of this section is the discussion of another aspect of resource allocation. Instead of taking the perspective of the user and assessing the dynamics of the resource allocation for the user, we will take the perspective of the collaborate cloud and review the dynamics involved when resources for the collaborative cloud are provided by one or more sharing parties. A distinct examination of this aspect for each architectural approach (chapter 4.1.1) seems necessary.

Generally there exist two possibilities regarding the dynamics of resource allocation for the collaborative cloud. Either the sharing parties determine at the very beginning the number of resources they want to share and this number does not vary during the operating of the collaborative cloud, i.e. it remains static, or the number may vary during the operating. When the number is static it seems likely that the resources are solely kept for the purpose of sharing these resources in the collaborative cloud and the degree of utilization depends only on the collaborative cloud. In the case of the dynamic approach it seems more likely that the resources are also used for a different purpose than the provisioning of the collaborative cloud with resources. For example it might be the case that the sharing party has an operator cloud and shares parts of the operator cloud in the form of resources with the collaborative cloud.
The use of a dynamic approach implies also the possibility to reduce the amount of shared resources. This means that the sharing party may withdraw its resources from the collaborative cloud and add them again to its operator cloud. This way the sharing party may share the idle resources from his operator cloud and recollect them, when needed. It seems obvious that in such a scenario there needs to be some agreements for withdrawal of resources from the collaborative cloud. These agreements may coincide with the agreements for the withdrawal of resources, which may be necessary for some use cases in the resource management (see 3.4.2). But this is not a requirement and it's perfectly possible to define deviant agreements.

Central Collaborative Cloud

In regard to the dynamics of the resource allocation it does matter how the central collaborative cloud approach is realized. In the case that there is only one party, which provides the complete cloud infrastructure including all available resources of the collaborative cloud, the dynamic approach for resource allocation fits just as perfectly as the static approach, though the dynamic approach may have advantages for the degree of utilization.

![Diagram](image)

*Figure 22 Resources for collaborative cloud are dedicated for the collaborative cloud only. The resources for the operator clouds are kept separate.*

However, if the central collaborative cloud approach is realized by the combination of resources from two or more sharing parties, the dynamic approach for resource allocation does not work well. This is because the sharing parties need a fully functioning operator cloud of their own, which includes not only shared resources but also separate ones that are used exclusively in the operator cloud. Of course this is only true, if we assume that the operator wants to be able to use the resources easily and return them to the central collaborative cloud afterwards.

Distributed Hierarchical Collaborative Cloud

Concerning the distributed hierarchical collaboration approach both approaches for resource allocation seem possible. However a drawback of the dynamic approach for resource allocation is that the handling of the resource information will be more complicated. In the case of static approach all requests are handled by the abstraction layer and its logical access point. Although it is certainly possible to construct the system in such a way that the abstraction layer also provides services for the withdrawal of resources, the question remains if the sharing parties want to use the logical access point in order to get resources back to
their operator cloud. It seems more likely that a sharing party will want to trigger such requests from a management layer in his own corporate network that covers both his operator and the collaborative cloud.

![Collaborative Cloud Diagram](image)

Figure 23 Collaborative cloud shares resources with the respective operator clouds. Percentage and total amount of resources shared may vary.

**Peer-to-Peer Collaborative Cloud**

For the peer-to-peer collaborative cloud approach most the argumentation is identical as for the distributed hierarchical collaborative cloud approach. In both cases we are dealing with a combination of fully functional operator clouds that combine resources to create the collaborative cloud. The only difference is that the sharing party may use its own access point provided by the abstraction layer deployed on top of his operator cloud for the adjustment of resources.

4.1.4 Balancing usage and provision of resources

The provisioning and usage of a collaborative cloud in itself is a form of cooperation that consists of the provisioning and sharing of resources and the usage of these shared resources. In this context some policies are needed to ensure ongoing cooperation. They should address some organizational issues, for example how many resources a sharing party needs to share, and if every party is supposed to share the same amount of resources or any at all. Also the question, if there is a way or a need to reward sharing of resources should be addressed. However such questions are not in the focus of this document, but may be investigated later on in the ASMONIA project context.

4.2 Cloud Provider Categories

In the context of the ASMONIA project we will use three categories of cloud providers:

1. **Third party cloud provider**

   A third party cloud provider is a cloud provider who owns a cloud infrastructure and offers his cloud service to his customers. This is quite a narrow definition because it excludes e.g. SaaS providers, who don’t own the cloud infrastructure their service is running upon.
Although the first impression is that the third party provider has nothing to do with the ASMONIA participants, it is also possible that the third party provider is a joint-venture of the ASMONIA participants.

2. Community member
   A community member is a mobile network operator which takes part in the collaboration process offered by the ASMONIA project. This definition is also intentionally narrow. At the time of writing, the project committee has not finally decided who may be allowed to become an ASMONIA community member but this will be part of a future publication of work package 1 (D1.1).

3. Government agency
   In this case the cloud provider is a government agency of the Federal Republic of Germany either owning the cloud infrastructure or being responsible for the provision of the infrastructure.

Note that in the cases of the cloud provider being a community member or a government agency there would be the possibility that the cloud provider does not own the cloud infrastructure but rents it from a third party. This has of course security implications, but for the sake of simplicity we are going to assume that whenever a third party is involved in any way then the category is third party. For future work we intend to come back at this point and reevaluate the implications.

4.3 Cloud Provider Models

The term cloud provider model denotes a combination of deployment models [NIST_CDEF], cloud provider categories (see chapter 4.2) and the architectural approaches for the cloud composition (see chapter 4.1). The focus here lies solely on organizational aspects of these combinations and their possible influence on the ASMONIA project. In some cases security implications are mentioned, but we will not present a detailed security analysis for the provider models. In future work we will decide on an architectural approach and review the security implications of this approach as well as more detailed security requirements of the more detailed use cases. For the following discussion, we will use the three different architectural approaches as a structure.

As the collaboration aspect is of special interest for the ASMONIA project, we will assess the cloud provider models along the criterion how well they seem suited for the realization of a collaborative environment, i.e. we will focus on the collaborative cloud (see chapter 1.3). The involvement of the government in the provider models is another point of interest for us. Depending on the trustfulness of the government in question (in our case Germany) the cloud system may gain a higher customer acceptance than otherwise.

4.3.1 Provider Models for a Central Collaborative Cloud

As described in chapter 4.1.1.1, it will be most likely the case that one party is providing the complete cloud infrastructure, when the central collaborative cloud approach is chosen. In this case the resulting Provider models can be derived straightforward from the deployment models and the provider categories:

1. Third party central public cloud model
   When the central collaborative cloud is deployed on a public cloud infrastructure owned by a third party, this is basically the same as consuming services from a public cloud provider. Thus, the same security concerns regarding for example data security apply.
Such a scenario might mean that some usage scenarios will very likely not be possible, because of confidentiality concerns of the mobile network operators. But this provider model also has its advantages when it comes to the overload and outage usage scenarios.

In the sector of telecommunication it is not uncommon for overload situations to arise simultaneously overall providers. This occurs e.g. regularly on New Year’s Eve. On such occasions one would expect all mobile network operators who participate in ASMONIA to consume services from the cloud, which results in a high peak of resource consumption. A large third party cloud provider might be able to meet such a peak.

2. Third party central community cloud model

Similarly to how the third party central public cloud model essentially deals with the usage of a public cloud provider this model deals with the usage of private cloud provider. Though in this case the ASMONIA consortium needs to contract the private cloud provider and in doing so, according to the cloud computing definition of NIST [NIST_CDEF] the private cloud provider becomes a community cloud provider.

There are two essential differences compared to the third party central public cloud provider model. First of all, in the case of the third party central community cloud model, no other party is using the cloud infrastructure. This means that the collaborative cloud is running on dedicated hardware and that guest-hopping attacks [ENISA_CCRISK] from an external attacker are not possible. Another consequence of the fact that the collaborative cloud is running on dedicated hardware is, that the ASMONIA consortium will have to pay for the resources even when they are idle.

3. Community member central public cloud model

This model describes the case when a community member of the ASMONIA community is a public cloud provider and hosts the collaborative cloud on its public cloud infrastructure. The same security concerns that apply in the third party case are applicable in this case.

One needs to keep in mind that ASMONIA is about the collaboration of mobile network operators and so to speak about the collaboration of competitors. That is why we do not believe that the participants will have more trust in the cloud infrastructure, when it is run by an ASMONIA member or in other words a competitor.

4. Community member central community cloud model

This model describes the case when a community member of the ASMONIA community is either a private cloud provider or rents a private cloud from a third party and hosts the collaborative cloud on it. As already mentioned above for the third party central community cloud model, the private cloud becomes a community cloud, when used by ASMONIA.

Compared to the third party central community cloud model, it might be possible for the ASMONIA community to bargain that the consortium only needs to pay for used resources.

5. Government agency central public cloud model

This model depends on a government agency that provides a public cloud infrastructure to host the collaborative cloud in that infrastructure. In Germany this is currently not the case and no plans for such a thing to happen are currently proclaimed. From our perspective it seems more likely that a government agency operates a private or community cloud.
6. Government agency central community cloud model

As already mentioned above no government agency has currently proclaimed to utilize cloud computing in a way that would enable the agency to act as a cloud provider. Thus also the case of a private or community cloud provided by a government agency would involve negotiations with the respective agency.

In such a scenario, where an agency provides the cloud infrastructure for mobile network operators, the aspect of data retention and legal interception becomes interesting. Especially in usage scenarios where components of the telecommunication infrastructure are virtualized and run in the collaborate cloud, depending on the respective components the government has direct access to sensitive data.

4.3.2 Provider Models for a Hierarchical Distributed Collaborative Cloud

In chapter 4.1.1.2 the hierarchical distributed collaborative cloud approach was described to combine the resources of two or more parties to one collaborative cloud. It was further discussed in chapter 4.1.3 that for a dynamic approach it will be necessary to have fully functional operator clouds, which share some of their resources to create the collaborative cloud. Going back to the definition of cloud computing by NIST (chapter 1.1) this qualifies the collaborative as a hybrid cloud.

A further differentiation of a hybrid cloud is not provided by NIST. Yet for the situation in the ASMONIA project a further differentiation seems necessary. We will accomplish this by introducing provider models for a hierarchical distributed collaborative cloud and discussing some of their aspects:

7. Community organized distributed cloud model

This model describes a hybrid collaborative cloud built by separate fully functional operator clouds and an additional abstraction layer. The operator clouds may differ in size. There exists only one constraint regarding the software that is deployed on the operator clouds to create the cloud infrastructure. The software needs to be on the list of supported cloud infrastructures of the abstraction layer. This implies of course that the subset of functionalities needed by the abstraction layer is provided by the respective software.

In this case only community members share resources from their operator clouds. No third party or government agency participates. As such all community members are equal. As described earlier in chapter 4.1.1.2 the hosting as well as the further development of the abstraction layer seems to present one of the major challenges.

8. Community organized distributed cloud model including government agencies

This model describes a hybrid collaborative cloud built by separate fully functional operator clouds and an additional abstraction layer just like the model presented above. The difference is that this time at least one government agency participates in the resource sharing.

In contrary to the ASMONIA members who are competitors of themselves the government agency represents an impartial party. From this perspective the government agency would be a perfect fit for handling the abstraction layer or any other central component.

9. Community organized distributed cloud model including third parties
This model describes a hybrid collaborative cloud built by separate fully functional operator clouds and an additional abstraction layer just like the two other models presented above. In this case at least one ‘third party’ participates in the resource sharing.

Similarly to the government agency in the case of the "community organized distributed cloud model including government agencies" the third party may act as an impartial party in this model. It seems more likely that the further development and hosting of the central components is taken over by a third party, if the third party is a joint-venture of the ASMONIA participants rather than having no affiliation with the participants.

4.3.3 Provider Models for a Peer-to-Peer Collaborative Cloud

The provider model needed for a peer-to-peer collaborative cloud (chapter 4.1.1.3) describes another possible model for the hybrid cloud (chapter 1.1). A further differentiation for the peer-to-peer approach along the provider categories does not seem necessary at this point.

This is because the peer-to-peer approach does not include any central components. All parties participating in the resource sharing are treated equally. They all use the same abstraction layer to access the collaborative cloud and they may all participate in the further development of it.

Although all participants would benefit from using the same software, this is not entirely necessary. It is perfectly possible to create different implementations, for example if there is a company policy for the use of certain programming languages.
5 General Requirements for the Support of Cloud Scenarios

5.1 General requirements for the Support of Cloud based Data Storage and Data Evaluation Solutions

In this chapter general requirements for the support of cloud based data storage and data evaluation solutions are listed. The requirements are the result of interviews with the other work packages and assumptions we had to make about their needs, which were not very clear at this early stage. The requirements listed here serve as a basis for future work, but will be adjusted when more information is available.

This chapter is divided into two sections: one section for the general requirements of derived use cases for integrity protection (WP2), the other section for the general requirements of the use cases for measurement and analysis (WP4). For background information refer to section 2.1.2.1.1 for the used general data properties, section 1.1.1.1.1 for the description of WP2 use cases and to section 2.1.2.3 for the description of WP4 use cases. In the following tables the requirements are applied to the use cases of WP2 and WP4. Every table contain in the columns the use cases and in the rows the general data requirements regarding database performance, security, confidentiality, backup strategies, archiving, etc.

5.1.1 Potential WP2 use cases

The general requirements for potential WP2 use cases are shown in Table 1.
<table>
<thead>
<tr>
<th>Index</th>
<th>Items</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Software Repository for mobile network elements</td>
</tr>
<tr>
<td>1</td>
<td>Transaction</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Consistency</td>
<td>Weak</td>
</tr>
<tr>
<td>3</td>
<td>Concurrency</td>
<td>Small</td>
</tr>
<tr>
<td>4</td>
<td>Read &amp; Write mode</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Read vs. Write ratio</td>
<td>1:N</td>
</tr>
<tr>
<td>6</td>
<td>Query model</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Hit rate</td>
<td>1:1, 1:M</td>
</tr>
<tr>
<td>8</td>
<td>Data types</td>
<td>Large count and small size</td>
</tr>
<tr>
<td>9</td>
<td>Persistence</td>
<td>Long</td>
</tr>
<tr>
<td>10</td>
<td>Latency</td>
<td>Seconds</td>
</tr>
<tr>
<td>11</td>
<td>Scalability</td>
<td>Less than 1T or growth slow</td>
</tr>
</tbody>
</table>
### Table 1: General requirements for potential WP2 use cases

<table>
<thead>
<tr>
<th></th>
<th>Availability</th>
<th>99.9% and above</th>
<th>99.9% and above</th>
<th>99% and below</th>
<th>99% and below</th>
<th>99,9% and above</th>
<th>99% and below</th>
<th>99% and below</th>
<th>99% and below</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Recovery time objective (RTO)</td>
<td>Hours</td>
<td>Hours</td>
<td>Days</td>
<td>Days</td>
<td>Hours</td>
<td>Days</td>
<td>Days</td>
<td>Days</td>
</tr>
<tr>
<td>14</td>
<td>Recovery point objective (RPO)</td>
<td>Days</td>
<td>Hours</td>
<td>Days</td>
<td>Days</td>
<td>Hours</td>
<td>Days</td>
<td>Days</td>
<td>Days</td>
</tr>
<tr>
<td>15</td>
<td>Content Type</td>
<td>Binary data</td>
<td>Binary data</td>
<td>Binary data</td>
<td>Binary data</td>
<td>Textual data</td>
<td>N/A</td>
<td>N/A</td>
<td>Textual data</td>
</tr>
</tbody>
</table>
5.1.2 Potential WP4 use cases

The general requirements for potential WP2 use cases are shown in Table 2.

<table>
<thead>
<tr>
<th>Index</th>
<th>Items</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Local Security Dashboard</td>
</tr>
<tr>
<td>1</td>
<td>Transaction</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Consistency</td>
<td>Weak</td>
</tr>
<tr>
<td>3</td>
<td>Concurrency</td>
<td>Small</td>
</tr>
<tr>
<td>4</td>
<td>Read &amp; Write mode</td>
<td>Large and sequential</td>
</tr>
<tr>
<td>5</td>
<td>Read vs. Write ratio</td>
<td>Write much less than read</td>
</tr>
<tr>
<td>6</td>
<td>Query model</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Hit rate</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>Data types</td>
<td>Large count and small size</td>
</tr>
<tr>
<td>9</td>
<td>Persistence</td>
<td>Temporary - Long</td>
</tr>
<tr>
<td>10</td>
<td>Latency</td>
<td>Seconds</td>
</tr>
<tr>
<td>11</td>
<td>Scalability</td>
<td>More than 1T or growth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rapidly</td>
</tr>
<tr>
<td>12</td>
<td>Availability</td>
<td>99,9% and above</td>
</tr>
<tr>
<td>13</td>
<td>Recovery time objective (RTO)</td>
<td>Seconds</td>
</tr>
<tr>
<td>14</td>
<td>Recovery point objective (RPO)</td>
<td>Weeks</td>
</tr>
<tr>
<td>15</td>
<td>Content Type</td>
<td>Textual data</td>
</tr>
</tbody>
</table>

Table 2 General requirements for potential WP4 use cases

5.2 General Requirements for the support of Cloud based Telecommunication Resources in Overload and Outage Situations

In this chapter assumptions and requirements for the support of collaborative cloud based telecommunication resources in overload and outage situations are listed. For background information and reasoning please refer to chapter 2.2. All assumptions and requirements are strictly related to overload and outage situations. Therefore this addition is omitted in the assumptions and requirements below.

Assumption 1:

The telecommunication network elements that are intended to run in the collaborative cloud must already be available in a virtualized form in the operator mobile network.
Assumption 2:
Only the central parts of the 4G mobile network (Evolved Packet Core, IMS; please refer to Figure 15, Figure 16 and Figure 17) are regarded suitable to run in the collaborative cloud. Because of its large geographical distribution and because of strict latency requirements, the Evolved UTRAN is not seen suitable for the more or less central collaborative cloud.

Assumption 3:
The collaborative cloud shall not instantiate mobile network elements with real-time media traffic. Therefore only network elements with computationally intensive tasks shall use the collaborative cloud. This applies for the signaling part of the 4G mobile networks.

Assumption 4:
The collaborative cloud doesn’t claim to provide full performance under all conditions. In outage situations, potentially also emergency situations, the collaborative cloud might deliver only rudimentary service functionality (e.g. basic voice service) for a perhaps only reduced range of customers (e.g. VIPs, emergency services).

Assumption 5:
It is assumed that the ASMONIA Collaboration Gateway (ACGW) performs only the management of the telecommunication resources in the collaborative cloud and that the signaling traffic towards the collaborative cloud will therefore bypass the ACGW. Background of this assumption is that the ACGW shall not be overloaded with non-ASMONIA related traffic.

Requirement 1:
If the collaborative cloud is envisaged to host critical telecommunication applications like for example the HSS, it is stringently required that the collaborative cloud is a private cloud with full control over the security features and the associated members.

Requirement 2:
The collaborative cloud must provide a high degree of elasticity to mitigate overload and outage situations caused by DoS attacks. During a DoS attack a multitude of the resources, available in the original telecommunication mobile network, may be required.

Requirement 3:
Load balancers are needed to distribute the traffic between the resources in the original mobile network and the collaborative cloud.

Requirement 4:
The lines between the original mobile network and the collaborative cloud must be available in advance to enable fast reactions.
Requirement 5:
In most cases the lines between the original mobile network and the collaborative cloud must provide high bandwidth and low latency to guarantee the availability and functionality of the additional collaborative cloud resources. Only in rare cases like for example a Web server with user self care management the delivery of best effort may be sufficient. (*This excludes largely usage of Public Internet for interconnection, because it delivers only 'best effort'.*)

Requirement 6:
Traffic to/from the collaborative cloud needs integrity protection: this means reliable identification of the collaborative cloud resources and traffic must remain unchanged. If traffic contains private user data, it needs additionally confidentiality protection and must be encrypted.

Requirement 7:
If a complete part of a mobile network runs in the collaborative cloud, then the network resources in the collaborative cloud between the different telecommunication VMs have to fulfill the same requirements (high bandwidth, low latency, integrity and confidentiality protection) as the lines between the original mobile network and the collaborative cloud.

Requirement 8:
The management of the shared cloud resources has to detect overload and outage situations and must activate the additional resources in the collaborative cloud.

Requirement 9:
If the additional resources in the collaborative cloud provide only a reduced performance for a limited number of users, then a selection mechanism for identifying valid users must be implemented.

Requirement 10:
As telecommunication operators must be compliant to national legal regulations, also the collaborative cloud must be compliant (keyword: TKG compliance)
6 Security Requirements for the Support of the Cloud Scenarios

At present many standardization bodies, industry organizations as well as national agencies and initiatives are working on assessments and recommendations for cloud computing security. It is difficult to gain an overview about all those activities. Moreover, it is impossible to refer to single documents covering certain areas of cloud computing security, but instead different sources of information have to be taken into account.

There is already some very good material available on cloud computing threats and risks. The most valuable documents are from ENISA and CSA.

ENISA performed a security assessment [ENISA_CCRISK] based on three use-case scenarios: 1) SME migration to cloud computing services, 2) the impact of cloud computing on service resilience, 3) cloud computing in e-Government (e.g., eHealth).

In addition to the guide CSA also provided a threat identification deliverable [CSA_TOPTHREATS] to be seen as complimentary to the above mentioned ENISA document [ENISA_CCRISK].

There are also some sources with recommendations for cloud computing security controls.

The Cloud Security Alliance (CSA) published a guide [CSA_GUIDE21] with practical recommendations and key questions to make a transition of applications, data and IT infrastructure from on-premise to public cloud offerings as securely as possible.

The CSA Cloud Controls Matrix [CSA_CCM] is a catalog of cloud security controls aligned with key information security regulations, standards, and frameworks. The matrix is based upon the CSA Security Guidance for Critical Areas of Focus in Cloud Computing and is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

The German Federal Agency for IT Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) published a draft listing minimum security requirements for cloud computing providers [BSI_MIND].

The following figure illustrates the taxonomy used to study the security requirements for cloud computing infrastructures and its usage.

The figure also shows who is responsible for which area of cloud computing security, namely the cloud provider is responsible for areas 1 to 3, the cloud customer for areas 4 to 6 and the end user for area 7.
The taxonomy includes the following seven security areas.

Areas 1 to 3 are in the responsibility of the cloud provider:

1. Cloud infrastructure and infrastructure management
   This area is solely under the control of the cloud provider. The security requirements may be documented in SLAs towards the customers. Furthermore the security controls may be audited by external firms possibly also on customer request.

2. Cloud resources and resource management
   This area is also in the responsibility of the cloud provider. However in contrast to the area “Cloud infrastructure and infrastructure management” this area defines security controls which are configurable by the cloud customer. Eventually those security controls are exported via APIs.

3. Cloud APIs
   This area is also in the responsibility of the cloud provider. This area defines the security requirements for the APIs, e.g. authentication measures, encryption techniques, etc.

Areas 4 to 6 are in the responsibility of the cloud customer:

4. Cloud data
This area defines security controls applicable for the cloud customer to ensure confidentiality, integrity and availability of cloud data.

5. Cloud applications
This area defines security controls applicable for the cloud customer to ensure the security of cloud applications.

6. Cloud customer clients
This area defines security controls applicable for the cloud customer clients. Basically different types of clients fall into this category.

Resource management client: The cloud customer can manage cloud resources via management API, e.g. launch a VM image, configure access control for cloud resources, etc.

Storage client: The cloud customer may want to use cloud storage and thus needs to create, retrieve, update or delete (CRUD) data items in the cloud. Those operations are very often called CRUD operations. The storage client may be used directly by the cloud customer or inherently in an application. The security controls are equally valid for both cases.

Application management client: The cloud customer may want to manage the application, respectively the VM in case of IaaS, via protocols such as SSH, RDS, HTTP(S), etc.

Area 7 is in the responsibility of the end user:

7. End user
This area defines security controls applicable for the end user of a cloud application. Please note that in this context the end user may either by a natural person e.g. accessing a web GUI (for example the ASMONIA dashboard) via a Browser, or an application using e.g. a web service offered via an application API (SOAP, REST, etc.).

6.1 Cloud Infrastructure and Management
This chapter deals with security requirements for cloud providers.

Hereafter those requirements are listed which are applicable for the cloud infrastructure and the infrastructure management and which are not controllable by any means for cloud customers.

Similar requirements can also be found in [BSI_MIND] and [CSA_CCM]. Therefore those documents should be consulted in addition to this document.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.1.1</td>
<td>Uninterruptable power supply</td>
<td>Data centers should be designed for UPS (Uninterruptable Power Supply) even in the event of a total power outage.</td>
<td>[BSI_MIND]</td>
</tr>
<tr>
<td>SEC.1.2</td>
<td>Connection to the Internet</td>
<td>Data centers must be connected to the internet via multiple network providers.</td>
<td>[BSI_MIND]</td>
</tr>
<tr>
<td>SEC.1.3</td>
<td>Disaster redundant data centers</td>
<td>Disaster redundant data centers must be provided ensuring that a disaster in one data center does not affect the other.</td>
<td>[BSI_MIND]</td>
</tr>
<tr>
<td>No.</td>
<td>Title</td>
<td>Details</td>
<td>Source</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>SEC.1.4</td>
<td>Permanent monitoring of data center facilities</td>
<td>24x7x365 monitoring of the data center facilities.</td>
<td>[BSI_MIND]</td>
</tr>
<tr>
<td>SEC.1.5</td>
<td>Independent audit of data center facilities</td>
<td>Physical security must be audited by an independent firm.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.6</td>
<td>Isolation of resources</td>
<td>Resources allocated by the provider shall not interact with any other resource not owned by the same customer.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.7</td>
<td>Secure transfer of VMs</td>
<td>Protection of VMs during transfer, e.g. live migration or initial transfer.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.8</td>
<td>Firewall</td>
<td>A firewall must be provided to protect against well known DoS attacks.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.9</td>
<td>IP spoofing</td>
<td>It must be ensured that VMs cannot send spoofed network traffic.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.10</td>
<td>Data redundancy</td>
<td>Data must be redundantly stored and permanently monitored for integrity. In case of failure data must be automatically restored.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.1.11</td>
<td>Data remanence</td>
<td>Data must be effectively and completely removed to be deemed ‘destroyed.’ Therefore, techniques for completely and effectively locating data in the cloud, erasing/destroying data, and assuring the data has been completely removed or rendered unrecoverable must be available and used when required.</td>
<td>[CSA_GUIDE21]</td>
</tr>
<tr>
<td>SEC.1.12</td>
<td>Incident Management</td>
<td>Providers must be capable to detect and handle security incidents both from internal sources (e.g. malware in the cloud) as well as from external sources (e.g. DoS attacks against cloud).</td>
<td>[CSA_CCM]</td>
</tr>
<tr>
<td>SEC.1.13</td>
<td>Incident Reporting</td>
<td>Security incidents must be reported immediately.</td>
<td>[CSA_CCM]</td>
</tr>
<tr>
<td>SEC.1.14</td>
<td>ISO/IEC 27001/27002</td>
<td>Cloud providers seeking to provide mission critical services should embrace the ISO/IEC 27001 standard for information security management systems. If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.</td>
<td>[CSA_GUIDE21]</td>
</tr>
<tr>
<td>SEC.1.15</td>
<td>SAS 70 Type II</td>
<td>Providers should have this audit statement at a minimum, as it will provide a recognizable point of reference for auditors and assessors. Since a SAS 70 Type II audit only assures that controls are implemented</td>
<td>[CSA_GUIDE21]</td>
</tr>
</tbody>
</table>
as documented, it is equally important to understand the scope of the SAS 70 audit, and whether these controls meet your requirements.

SEC.1.16  External audits  The cloud provider must allow external audits.  Not specific

SEC.1.17  Safe Harbor  The cloud provider should participate in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union.  Not specific

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.2.1</td>
<td>Configurable IP packet filter rules in firewall</td>
<td>It must be possible to manage IP packet filter rules in firewall by customers themselves.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.2</td>
<td>Network zones support</td>
<td>Network zones /sub-domains must be configurable in order to support: a) Grouping of systems with similar security requirements b) Providing perimeter security (for example with a DMZ between internal and external network c) Separate front-end and back-end functionality and databases.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.3</td>
<td>Secure VPN access</td>
<td>Cloud provider should offer VPN restricted access to resources.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.4</td>
<td>VM and Data location display</td>
<td>The cloud provider should provide information about the location of where the VM have been launched and where the data are stored.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.5</td>
<td>VM and Data location choice</td>
<td>The cloud provider should allow control over the location of where to launch the VM and where to store the data.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.6</td>
<td>Data location</td>
<td>There must be assurance that the data, including all of its copies and backups, is stored only in geographic locations permitted by contract and/or SLA.</td>
<td>[CSA_GUIDE21]</td>
</tr>
<tr>
<td>SEC.2.7</td>
<td>Data encryption</td>
<td>Data must be encrypted with customer individual private keys thus</td>
<td>Not specific</td>
</tr>
<tr>
<td>No.</td>
<td>Title</td>
<td>Details</td>
<td>Source</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SEC.2.8</td>
<td>Secure remote shell access</td>
<td>ensuring that employees of the cloud provider cannot decrypt any data.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.9</td>
<td>VM backup and restore</td>
<td>VM images shall be configured such that remote shell access is only possible using keys.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.10</td>
<td>Data backup and restore</td>
<td>Providers must provide means for backup and restore of VMs.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.11</td>
<td>Data backup and restore</td>
<td>Cloud providers must ensure that backup of data happens and that data are restorable.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.12</td>
<td>Logging of management actions</td>
<td>Every management action must be logged.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.13</td>
<td>Event management logs for audits and relevant security events</td>
<td>Security violations at a system (e.g. authentication failures, unauthorized access attempts) must be logged.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.14</td>
<td>Push of log files</td>
<td>It must be possible to configure pushing of log files to external destinations, e.g. via e-mail.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.15</td>
<td>VM health supervision</td>
<td>Providers must support supervision of VMs.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.16</td>
<td>Consistent monitoring data</td>
<td>Cloud providers must supply consistent formats to monitor cloud applications and service performance and make them compatible with existing monitoring systems.</td>
<td>[OC_MANIFESTO]</td>
</tr>
<tr>
<td>SEC.2.17</td>
<td>Central credential management</td>
<td>It must be possible to manage accounts and related public and private credentials from a central location.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.18</td>
<td>Contact possibilities</td>
<td>It must be possible to contact support team via phone and mail.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.19</td>
<td>Key rotation</td>
<td>It must be possible to rotate keys on a regular basis. Multiple concurrent keys must be supported at a time.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.20</td>
<td>Access control to resources</td>
<td>Providers must implement controls preventing the accidental or malicious access, use, modification or destruction of resources under their care. Further, all authorized access must be audited and regularly reviewed in order to promote accountability and ensure that actions are taken in accordance with their stated security policy.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.2.20</td>
<td>Multiple users with role based access control</td>
<td>It must be possible to create multiple users per account and manage roles and permissions for each of those</td>
<td>Not specific</td>
</tr>
</tbody>
</table>
Table 4: Security Requirements for Cloud Resources and Resource Management

6.3 Cloud APIs
This chapter deals with security requirements for cloud providers.
Hereafter those requirements are listed which are applicable for the cloud APIs.

Table 5: Security Requirements for Cloud APIs
6.4 Cloud Data

This chapter deals with security requirements for cloud customers. In the context of the ASMONIA project those requirements are relevant to support the use cases listed in 1.1.1.1.1 and 2.1.2.3.

Please note that data encryption and integrity protection could be inherently provided by the cloud platform. Refer to requirements SEC.2.7 and SEC.1.10. In those cases it might not be necessary that encryption and integrity protection is implemented by the customer. Hereafter those requirements are listed which are applicable for the cloud data.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.4.1</td>
<td>Separation of sensitive and non-sensitive data</td>
<td>Segment out sensitive data from non-sensitive data into separate databases in separate security groups when hosting an application with highly sensitive data.</td>
<td>[REESE_20R]</td>
</tr>
<tr>
<td>SEC.4.2</td>
<td>Encryption of non-root file systems</td>
<td>Use only encrypted file systems for block devices and non-root local devices.</td>
<td>[REESE_20R]</td>
</tr>
<tr>
<td>SEC.4.3</td>
<td>Encryption of file system key</td>
<td>Pass in the file system key encrypted at instance start-up.</td>
<td>[REESE_20R]</td>
</tr>
<tr>
<td>SEC.4.4</td>
<td>Encryption of content in storage</td>
<td>Encrypt everything stored in cloud storage using strong encryption. (This may not be necessary if customer individual encrypted storage is supported by the cloud provider.)</td>
<td>[REESE_20R]</td>
</tr>
<tr>
<td>SEC.4.5</td>
<td>Signing of content in storage</td>
<td>Sign everything stored in cloud storage. (This may not be necessary if customer individual signing of storage content items is supported by the cloud provider.)</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.4.6</td>
<td>Secure handling of decryption keys and forced removal once not needed</td>
<td>Never allow decryption keys to enter the cloud—unless and only for the duration of an actual decryption activity.</td>
<td>[REESE_20R]</td>
</tr>
</tbody>
</table>

Table 6: Security Requirements for Cloud Data

6.5 Cloud Applications

This chapter deals with security requirements for cloud customers. In the context of the ASMONIA project those requirements are relevant to support the use cases listed in 2.1.1.2.

Hereafter those requirements are listed which are applicable for the cloud applications.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.5.1</td>
<td>No reliance on particular VM</td>
<td>Design your systems so that you do not rely on a particular VM structure for</td>
<td>[REESE_20R]</td>
</tr>
</tbody>
</table>
### Analysis of Requirements for the Deployment of Cloud Systems

**No.** | **Title** | **Details** | **Source**
---|---|---|---
SEC.5.2 | Source address filtering of traffic | Specify source addresses when setting up your instance; only allow global access for global services like HTTP/HTTPS. | [REESE_20R]
SEC.5.3 | Encryption of network traffic | Encrypt all network traffic. | [REESE_20R]
SEC.5.4 | Strong authentication of network traffic | Perform strong authentication of all network traffic preferably using keys. | Not specific
SEC.5.5 | Usage of host-based firewall | Install and configure a host-based firewall system like ipfilter, iptables. | Not specific
SEC.5.6 | Installation of a network based IDS (NIDS) | Install a network intrusion detection system like snort. | Not specific
SEC.5.7 | Installation of a host based IDS (HIDS) | Install a host-based intrusion detection system like OSSEC. | [REESE_20R]
SEC.5.8 | Usage of hardening tools | Leverage system hardening tools like Bastille Linux, SELinux, etc. | [REESE_20R]
SEC.5.9 | System design for patch roll-out | Design things so you can roll out a security patch to an AMI and simply relaunch your instances. | [REESE_20R]
SEC.5.10 | Disabling of password based authentication for SSH | Do not allow password-based authentication for shell access and use keys instead. | [REESE_20R]
SEC.5.11 | Verification of VM's host key for SSH | Verify the VM's host key when connecting to the SSH server in order to prevent man-in-the-middle attacks. | Not specific
SEC.5.12 | Disabling of root account | Disable root account and use sudo to acquire higher privileges. | Not specific
SEC.5.13 | No credentials in VMs | Do not store any credentials in VMs running on public cloud infrastructure. | [REESE_20R]
SEC.5.14 | Support of SAML | SAML shall be supported in order to offer a SSO solution for cloud applications. | Not specific
SEC.5.15 | One service per instance | Run only one service per VM instance. | [REESE_20R]

**Table 7: Security Requirements for Cloud Applications**

#### 6.6 Cloud Customer Clients

This chapter deals with security requirements for cloud customers.

Hereafter those requirements are listed which are applicable for the cloud customer clients.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
</table>
SEC.6.1 | Regular full backups | Regularly pull full backups and store | [REESE_20R] |
<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.6.2</td>
<td>Instance snapshot in case of a security breach</td>
<td>If a compromise is suspected, backup the root file system, snapshot the block volumes, and shut down the instance. (Forensics on an uncompromised system can be performed later.)</td>
<td>[REESE_20R]</td>
</tr>
<tr>
<td>SEC.6.3</td>
<td>Separation into multiple accounts (production vs. testing)</td>
<td>Segment the infrastructure into multiple accounts, i.e. do not mix production servers in the same accounts as QA, development, testing, or R&amp;D work.</td>
<td>[REESE_SPRAWL]</td>
</tr>
<tr>
<td>SEC.6.4</td>
<td>Regular verification of cloud resources configuration</td>
<td>Verify on a regular basis that the configuration of the cloud resources has not been changed. This is especially important since cloud resources can be managed via different channels, e.g. web console and APIs. Thus if for example the web console access has been hacked this might not be visible immediately to the customer if normally management is only done via APIs. Therefore some type of intrusion detection for the cloud resource management is needed.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.5</td>
<td>No credentials in end user devices</td>
<td>Do not store any cloud credentials in end user devices such as Notebooks, PCs, USB sticks etc.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.6</td>
<td>Secure storage of credentials</td>
<td>Store the credentials securely and allow only authorized access.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.7</td>
<td>Usage of password generation tool</td>
<td>Use a password generator tool to generate strong random passwords with at least 20 characters length.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.8</td>
<td>Automatic renewal of credentials</td>
<td>Provide an automated procedure to generate new credentials after a configurable time interval.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.9</td>
<td>Security groups</td>
<td>Use security groups (i.e. named set of firewall rules) to configure IP traffic to/from VMs completely in order to isolate every tier, even internally to the cloud.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.6.10</td>
<td>SSH access limited to own location</td>
<td>Configure the firewall such that SSH access to the VMs is limited to own location.</td>
<td>Not specific</td>
</tr>
</tbody>
</table>

Table 8: Security Requirements for Cloud Customer Clients

6.7 End User

This chapter deals with security requirements for end users.
<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Details</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC.7.1</td>
<td>No credentials in end user devices</td>
<td>Do not store any application credentials in end user devices such as Notebooks, PCs, USB sticks etc.</td>
<td>Not specific</td>
</tr>
<tr>
<td>SEC.7.2</td>
<td>Usage of password generation tool</td>
<td>Use a password generator tool to generate strong random passwords with at least 20 characters length.</td>
<td>Not specific</td>
</tr>
</tbody>
</table>

*Table 9: Security Requirements for Cloud Customer Clients*
7 Regulatory Requirements for the Support of the Cloud Scenarios

This chapter investigates upon the potential regulatory obligations regarding security and privacy in the context of data storage of a cloud platform, see also [ULD]. The investigation remains at a higher level of abstraction and does not go into details of certain relevant laws.

By cloud platform it is herein understood to encompass what is labeled as PaaS (Platform-as-a-service) or serviced cloud platform, as well as IaaS (Infrastructure-as-a-service) or serviced cloud infrastructure, or a combination of both IaaS and PaaS. A less well known variant of a cloud computing platform is given by Data storage-as-a-service (DaaS) where the cloud service cares for short- and/or long-term archiving and backups of the stored data, thus DaaS could be considered as a serviced network(ed) file/repository system.

It should be pointed out that typically regulatory obligations do not just hold for data storage but also for corresponding data processing in the processing elements as well as data transfer to and/or from the cloud platform; data transfer may occur between the user and the cloud, but also intra-cloud among several sites of the same cloud provider or perhaps inter-cloud between different cloud providers. Such aspects as data processing or data transfer may well deserve additional considerations from the legal and from the security point of view which are left as for further study.

Regulatory obligations generally apply on a global level to wherever the cloud platform is actually hosted or is being provided while the specific regulations to apply depend on the actual country considered. This could be true in principle for any country where the cloud platform is involved to any extent possible. It may be obvious that the cloud platform may not comprise just a single legal domain, but might actually cover multiple legal domains whenever the cloud platform is actually a distributed one hosted or being served by one or multiple cloud providers situated in more than one country and where accordingly, the data stored in the cloud is distributed across several cloud providers and/or across different legal domains. In consequence, several laws (potentially even diverging) could apply simultaneously in an inter-country cloud platform situation and this can result in substantial difficulties and burden, see [MS].

This consideration focuses on the obligations naturally imposed upon a public cloud service provider, notwithstanding that further legal obligations may additionally be imposed upon a private cloud provider (e.g. in-house cloud within an enterprise), or indirectly upon manufacturers and solution providers that supply equipment and/or solutions towards a cloud provider. It is being observed that far more regulations apply to public service providers (henceforth also public cloud providers) than to private enterprises (private clouds), yet private clouds should not be considered entirely free of any regulations. However, certain regulations are found just exclusively in public clouds such as the need for data retention and lawful interception.

Hybrid clouds are a combination of private and public clouds, and consequently hybrid clouds are also subject to legal obligations.

In addition to that, certain legal obligations may reside upon authoritative instances and legal institutions (such as national regulators, policy makers, national agencies and the like).

Since this scope of globally distributed cloud providers is by far too wide (i.e. too many countries to consider) to make any reasonable assessments, it is hereby assumed for simplicity and as a starting point that the cloud platform at least covers the legal domain of Germany, while coverage of other legal domains of a cloud platform should not be ruled out per se. Henceforth, this essay assumes one or more cloud providers that are all situated entirely within the legal domain of Germany. This assumption however should not lead to the conclusion that the regulatory situation in Germany regarding clouds had any representative
character in the sense “compliance with German laws implies compliance anywhere else”: this is most often just not the case!

It should be acknowledged that

- Assumingly the notion of a cloud provider may not be strictly well defined in current legal terms. At the time of this writing, the author is not aware of any dedicated “cloud laws or acts”, yet several jurisdictions are underway of preparing specific regulations in that regard; see e.g. [BSI], and [FEDRAMP].

However, it is assumed that a cloud provider could be considered as a special incarnation of a service provider (offering cloud services) and/or of an operator (offering a mixture of services and/or transport facilities). For this very reason, all current regulations may be subject to considerations.

- A cloud service may comprise and cover services spanning a multitude of businesses such as including sectoral applications (e.g. telecommunications, health care, banking, energy, governmental agencies’ communications, security services (emergency and disaster recovery facilities, and more). As such, any such sectoral regulations may become subject to cloud providers when serving such sectors.

- It should be clear that any analysis, including any made assessments are purely a (personal) interpretation of the base material potentially subject to misinterpretations, and potentially being incomplete, or being irrelevant at least. Still, the analysis is being carried out with the best technical security expertise at least, yet the author admits to lack much understanding of legal terms or legal practices, especially in other legal environments than Germany. By no means should this analysis claim any correctness with respect to any made legal conclusions, even such conclusions may yet occur. As such, this document should not to be taken as any form of being considered as legally binding; no such responsibility can be taken here at all, but if required should be sought then from some authorized legal counselors instead. In conclusion, this document and corresponding material should be considered as being of informative character only.

- Other countries may have diverging obligations and laws as pertaining to the set scope herein.

- This document does not attempt to identify draft, potentially new and forthcoming regulations in the context of cloud computing, albeit such discussions are taking place on various political levels (see [BSI], [FEDRAMP]). Likewise, the document does not consider de facto legislation such as Google streetview’s quasi regulatory rules.

- Cloud platform – while a rather recent and novel term – may find various correspondences in other related and similar concepts such as “Outsourcing”, hosted applications or Application Service Provider (ASP), and data processing on demand (Auftragsdatenverarbeitung/BDSG, or commissioned data processing). Hence, legal obligations as applicable to those concepts may well be reconsidered for cloud platforms too.

- In many regards (and probably from the legal and regulatory point of view), cloud platforms are not so much different than what is well known from the classic data (processing) center. As a premise, any obligations upon data centers most likely also apply to cloud platforms.

- This chapter focuses on legal and regulatory obligations, but leaves aside any voluntary measures such as industry/international standards and best practices. While additional security and privacy requirements can be drawn from such standards
and best practices, none of them are mandatory by their own. However, in rare cases, legal texts sometimes reference such standards.

Without loss of generality it is further assumed that the cloud provider(s) offering a cloud service are all storing the data on their cloud platform. Such data could be subject to personally identifiable information (aka PII) to include any personal data (for which the legal obligations of data protection laws apply) as well as any other non-PII data which may be sensitive in the security sense, or which may have just a non-sensitive character and for which non specific security and/or data protection laws apply.

With regard to personal data, data protection and security the following laws in Germany specifically apply:

7.1 Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG)

Date of publication: 1 September 2009
Website: http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG_idFv01092009.pdf

The BDSG implements the European Data Protection Directive (95/46/EC), and transfers the directive into national law.

Purpose of this BDSG Act is to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data.

This Act shall apply to the collection, processing and use of personal data by private and public bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities. Additional state data protection laws (LDSG) apply in Germany for public agencies of the Government or of the German states.

BDSG forbids in principle the collection, processing and usage of personal data, unless there is a definite legal basis (by law or contract) for doing so, or the affected person has given (explicit, affirmative) consent (typically written, using subject's free decision) to allow the collection, processing and usage of personal data.

BDSG declares the principle to adhere to data minimization and data avoidance; i.e. to avoid entirely or reduce personal data to as little as possible; while encouraging using anonymization and pseudonymization techniques.

The scope of BDSG covers personal data, which is legally defined as any data that relates to a person, or possibly can be related to a person; e.g. Tel#, email address, IP address), and also anonymous data where the person is not known; but does not apply to data of legal entities (companies, enterprises).

"Special categories of personal data" (racial origin, health data etc) is granted an extra level of protection.

It should be noted that BDSG may not be required in case that the personally-identifiable data has sufficiently been anonymized, and assuming that such anonymized data cannot be used somehow to re-identify a person. Pseudonymization of personal data (which also is a required option of BDSG) is not considered equivalent to anonymization, and hence BDSG always applies for PII data even if that data is pseudonymized.

A designated data protection officer (DPO) is required for all commercial enterprises (private bodies) with more than 9 employees that process personal data with computers, or
companies, that have a focus in the area of processing of personal data (such as market researchers for example).

BDSG grants principle and undeniable rights to individuals to obtain information and on correction or incorrectly stored personal data.

Finally, the BDSG also includes norms requiring certain technical and organizational protection measurements, when processing personal data. The level of technical protection necessary is intended to be adaptive; i.e., it changes as new technology becomes available.

Overall, BDSG addresses security and privacy aspects such as:

- Data protection
- Interception
- Electronic consent
- 3rd party information relay
- (Targeted) Advertising
- State-of-the-art privacy measures
- Authenticity; authentication
- Confidentiality, encryption (also Vorsperre/dedicated encryption)
- Authorization
- Logging
- (Secure) delete, correction
- Compliance, certification
- Testing
- User consent
- personal data separation
- personal data consolidation/linkage(aliasing pseudonym – real ID)
- 3rd party
- Pseudonymity/ anonymity
- personal data disclosure
- security concept
- data/information minimization
- user profile disclosure/ information
- Transparency of personal data processing on mobile media
- Data protection audit.

7.2 Telecommunications Act (Telekommunikationsgesetz - TKG)

Date of publication: 25. December 2008
The purpose of this Act is, through technology-neutral regulation, to promote competition and efficient infrastructures in telecommunications and to guarantee appropriate and adequate services throughout the Federal Republic of Germany. The act addresses public telecommunications network operators and providers of publicly available telecommunications services.

This Act serves to transpose the following EU Directives:


Privacy aspects are covered in the following clauses:

- Chapter 2 - Access Regulation - § 17 - Confidentiality of Information
  - PART 3 - CUSTOMER PROTECTION
    - Section 47 - Provision of Subscriber Data
- Chapter 2 – Numbering - Section 66 – Numbering
  - PART 6 - UNIVERSAL SERVICE - Section 85 - Suspension of Service
  - PART 7 - PRIVACY OF TELECOMMUNICATIONS, DATA PROTECTION, PUBLIC SAFETY
    - Section 89 - Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy
    - Section 90 - Misuse of Transmitting Equipment
- Chapter 2 - Data Protection - Section 91 - Scope
  - Section 92 - Transfer of Personal Data to Foreign Private Bodies
  - Section 93 - Duty to Provide Information
  - Section 94 - Consent by Electronic Means
  - Section 95 - Contractual Relations
  - Section 96 - Traffic Data
Overall, TKG addresses security and privacy aspects such as:

- Blocking/scanning/ filtering to counter illegal usage
- Common scrambling algorithm
- Access control
- Youth protection code/PIN
- Calling party numbering/ identification and integrity
- Public safety of telecommunications
- E.112; emergency call
- Service suspension
- telecommunications privacy/secrecy
- Data protection
- Interception
- Electronic consent
- 3rd party information relay
- (Targeted) Advertising
- Data Retention
- Calling number identification/ restriction
- State-of-the-art security measures
- State-of-the-art privacy measures
- Lawful interception
- Risk Management, Risk analysis
- User consent
- Pseudonymity/ anonymity.

7.3 Telemedia Act (Telemediengesetz - TMG)

Date of publication: 26.02.2007

The TMG applies for all electronic information- and communications services. TMG does not overrule the TKG. TMG regulates the telemedia; i.e. electronic media information that is part of a commercial service offering.

TMG replaces TDG and TDDSG; TMG incorporates several statements/obligations of the Mediendienstestaatsvertrages (MDStV).
Privacy aspects are covered in the following clauses:

- Section 3 – Responsibility - §7 General principles
- Section 4 – Data Protection - § 11 Provider-User Relationship
- § 12 Principles
- § 13 Duties of the Service Provider
- § 14 Personal base data
- § 15 Personal usage data

Overall, TMG addresses security and privacy aspects such as:

- Data protection
- Electronic consent
- 3rd party information relay
- (Targeted) Advertising
- State-of-the-art privacy measures
- Authenticity; authentication
- Confidentiality, encryption (also Vorsperre/dedicated encryption)
- Authorization
- Logging
- (Secure) delete, correction
- Compliance, certification
- User consent
- personal data separation
- personal data consolidation/linkage(aliasing pseudonym – real ID
- 3rd party
- Pseudonymity/ anonymity
- personal data disclosure
- security concept
- data/information minimization
- user profile disclosure/ information
- Transparency of personal data processing on mobile media
- Data protection audit.

A plethora of additional laws and obligations (all not investigated further herein) may likely pertain to the set scope at least in Germany such as the criminal code (StGB); protection of minors (JuSchG); FÜV (Telecommunications supervisory); Emergency call (NotrufV); Corporate Governance, Stock corporation and risk management (KonTraG, AktG); Equity, Banking system, Solvency (Basel II, KWG); VolP LI (ÜbÜbVoIP); G10 act, protection of dignity and minors in broadcasting and telemedia + youth protection guidelines (JMStV+...
JuSchRiL); and Signature acts (SigG, SigÄndGes, SigV), consumer protection laws, – just to name a few.

Specifically for STaaS and cloud-based storage of data, further legal obligations may likely be of relevance such as Abgabenordnung (AO) for archiving of tax-sensitive data, Handelsgesetzbuch (HGB) for storage/archiving of business bookkeeping data, financial data (KWG), and social secrets (SGB).

Further data protection laws persist within the 16 countries (Länder) of Germany, in the information freedom act (IFG), and the ordinance concerning the Technical and Organizational Implementation of Measures for the Interception of Telecommunications (TKÜV).
8 Conclusion

This document showed how cloud computing systems can be used to support the various parts of the ASMONIA project. In chapter 2 two abstract cloud scenarios for the usage of cloud computing systems in ASMONIA were presented and possible use cases were derived from them. In preparation for the design of the system architecture of a cloud computing system that is capable to fit the needs of the ASMONIA project, some architectural considerations were presented and discussed. Subsequently, a more detailed description of general, security and regulatory requirements was given.

This document does not contain a complete requirements analysis for the usage of cloud computing systems in ASMONIA. But it is a first step towards it. The benefits of the usage of cloud computing systems in ASMONIA were illustrated by the cloud scenarios. This can be seen as a confirmation that the original plan of the ASMONIA project to use cloud computing in this context was right and that the way ahead seems still promising. The presentation of the requirement categories that need to be considered for the design of the system will help in the discussions with the stakeholders to elicit the needed requirements.

8.1 Outlook

In the future we will work on consolidation of the use cases derived from the cloud scenarios. From the use cases we will derive the functional and non-functional requirements, i.e. in our terms the general, security and regulatory requirements, and use them to create the system architecture of a cloud computing system. The design of the system will require input from different parts of ASMONIA, and range from input for the use cases to input for the integration of the cloud computing system into the overall ASMONIA architecture.
References


[CDMI] SNIA, "Cloud Data Management Interface Version 1.0", April 2010


[CSA_CCM] Cloud Security Alliance, "Cloud Controls Matrix V1.0", April 2010
<http://www.cloudsecurityalliance.org/guidance/CSA-ccm-v1.0.0.xls>


<http://www.cloudsecurityalliance.org/topthreats/csatopthreats.v1.0.pdf>


[MS] "Microsoft: Cloud computing troubled by EU data rules"

<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>

<http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-
Analysis of Requirements for the Deployment of Cloud Systems
WP 3.1 Deliverable (public)
D31-1.0


Glossary and Abbreviations

Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controls</td>
<td>Security Controls are management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.</td>
<td>[NISTGLOSSARY]</td>
</tr>
<tr>
<td>Risk</td>
<td>Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.</td>
<td>[NISTGLOSSARY]</td>
</tr>
<tr>
<td>Threat</td>
<td>Threat is any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.</td>
<td>[NISTGLOSSARY]</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.</td>
<td>[NISTGLOSSARY]</td>
</tr>
</tbody>
</table>
| Data Storage as a Service (DaaS) | DaaS is a cloud service supporting:  
  - delivery over a network of appropriately configured virtual storage and related data services, based on a request for a given service level  
  - delivery of virtualized storage and data services on demand over a network.                                                                 | [CDMI] |

Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4G</td>
<td>4th Generation</td>
</tr>
<tr>
<td>ACN</td>
<td>ASMONIA Collaboration Network</td>
</tr>
<tr>
<td>ACGW</td>
<td>ASMONIA Collaboration Gateway</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>AS</td>
<td>Application Server</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik</td>
</tr>
<tr>
<td>CDMI</td>
<td>Cloud Data Management Interface</td>
</tr>
<tr>
<td>CRUD</td>
<td>Created, Retrieved, Updated, Deleted</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Session Control Function</td>
</tr>
<tr>
<td>DaaS</td>
<td>Data storage as a Service (refer to glossary)</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>EBS</td>
<td>Elastic Block Storage</td>
</tr>
<tr>
<td>ED</td>
<td>End Device</td>
</tr>
<tr>
<td>eNB</td>
<td>eNodeB</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>I-CSCF</td>
<td>Interworking - CSCF</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IP</td>
<td>Integrity Protection</td>
</tr>
<tr>
<td>MA</td>
<td>Measurement &amp; Analysis</td>
</tr>
<tr>
<td>NE</td>
<td>Network Element</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>OCCI</td>
<td>Open Cloud Computing Interface</td>
</tr>
<tr>
<td>P-CSCF</td>
<td>Proxy - CSCF</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RDC</td>
<td>Remote Desktop Connection</td>
</tr>
<tr>
<td>S-CSCF</td>
<td>Signaling - CSCF</td>
</tr>
<tr>
<td>SMI-S</td>
<td>Storage Management Initiative Specification</td>
</tr>
<tr>
<td>SNIA</td>
<td>Storage Networking Industry Association</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>SWIP</td>
<td>SW Integrity Protection</td>
</tr>
<tr>
<td>TKG</td>
<td>Telekommunikationsgesetz</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2011-05-09</td>
<td>Final version.</td>
</tr>
</tbody>
</table>