FRAUNHOFER INSTITUTE FOR OPEN COMMUNICATION SYSTEMS

Cloud Concepts for the Public Sector in Germany – Use Cases

Peter Deussen, Klaus-Peter Eckert, Linda Strick, Dorota Witaszek

Fraunhofer Institute FOKUS

12.08.2011

Fraunhofer FOKUS

Imprint

Publisher

Fraunhofer-Institute for
Open Communication Systems FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany

Contact

Competence Center Elan:
Electronic Government and Applications
Telephone +49 (0)30 3463-7115
eMail elankontakt@fokus.fraunhofer.de
www.fokus.fraunhofer.de/egov-lab

Authors

Dr. Peter H. Deussen
Telephone +49 (0)30 3463-7345
eMail peter.deussen@fokus.fraunhofer.de

Dr. Klaus-Peter Eckert
Telephone +49 (0)30 3463-7227
eMail klaus-peter.eckert@fokus.fraunhofer.de

Linda Strick
Telephone +49 (0)30 3463-7224
eMail linda.strick@fokus.fraunhofer.de

Dorota Witaszek
Telephone +49 (0)30 3463-7348
eMail dorota.witaszek@fokus.fraunhofer.de

Summary

This document provides a compendium of material. The intention is not to provide a comprehensive overview of current use case activities and their relation to on-going discussions in Germany on Cloud Computing for the public sector, but to offer a basis for publications dedicated to particular audiences and specific situations. Therefore, we tried to refrain from generic arguments but to give a variety of concrete examples which allow carrying the discussion of specific issues from a political and legal level down to their technical implementation. These usage scenarios provide also a context to understand and to classify the more atomic and technically oriented use cases taken from the National Institute of Standards and Technology NIST, the Distributed Management Task Force DMTF, the Cloud Computing Use Case Discussion Group CCUCDG, and Microsoft documents. They moreover identify requirements that are specific for a soft migration to Cloud Computing in this application domain.

Cloud Computing for the public administration is ambitious. Aspects such as legal frameworks, organizational structures, technological potential and constraints, security concerns, consolidation and data protection play a crucial role in the adoption of cloud computing in the public sector. Thus, the introduction of Cloud Computing depends on the solution of technical, organizational and legal issues. The example of the German public sector will serve as a basis for the evaluation of benefits and challenges of Cloud Computing by defining and analyzing a number of use case scenarios. Starting point is the analyses of Cloud Computing definitions and use cases, e.g. those provided by NIST, DMTF, CCUCDG, and Microsoft. In particular, a common actor model is synthesized and extended to meet the requirements of the German public sector. Moreover, a business model configuration will be introduced which outlines possible interactions between citizen, enterprises, and administrations. Furthermore, additional dimensions for the categorization of use cases are identified. Therefore, this work complements existing use case description by the above mentioned organizations towards an “eGovernment perspective” which necessarily has to go beyond business models and technical considerations.

To evaluate this eGovernment perspective under consideration of the current state of applicability of Cloud Computing in the German public sector, a number of interviews with members of eGovernment service providers have been performed. The evaluation results are concluded in a set of theses.

To give typical application examples of how Cloud Computing can be applied in the German public sector three usage scenarios have been described and analyzed.

- Scenario 1 illustrates how data privacy issues can be resolved by separating between personal and non-personal (open) data. Governmental processes which do not rely on personal data can be hosted in public Cloud infrastructures. It provides the basis of a prototype implementation.
- Scenario 2 shows how a Cloud service providing a secure document storage can provide seamless interaction between administrations, enterprises, and citizens, optimize governmental processes by delivering documents in a timely manner, and to enable inter-administration processes by the electronic exchange of documents. It is used as a basis for the definition of templates for the description of use cases and usage scenarios.
- Scenario 3 outlines the idea of interweaving governmental processes and business processes of enterprises (e.g., SMEs) to provide a business incubator for those enterprises. The scenario imposes interesting questions on a collaborative lifecycle management between the several actors.

Contents

1 Introduction

The objective of the paper is to explore the potential benefits and challenges of Cloud Computing by the definition and analysis of a number of use case scenarios. These use cases will be defined from the perspective of the German public sector and address the roles of cloud users and providers. This work therefore tries to complement existing work on use cases towards an "eGovernment perspective" which necessarily has to go beyond business models and technical considerations.

By adding factors and constraints that are significant for the discussion of Cloud Computing in the German public sector, we obtain a picture which is – concerning legal issues such as data privacy or administrative regulations - prototypical for Europe: In fact, Germany is amongst those European member state with the most restrictive legal constraints for the application of IT technology in governmental agencies.

The White Paper identifies use cases which address issues such as interoperability, portability, and data privacy. As application field eGovernment and their requirements to Cloud Computing is taken into account. To identify the most suitable use cases the opinion of some partners of the FOKUS eGovernment lab will be included, especially of those partners with a main focus on public administration service centers such as data centers acting on municipal as well as on federal states level.

This document provides an assembly of facts about cloud computing concepts, use cases and actors. Depending on the target audience one or more white papers will be generated from this basic information. It is structured in two main parts:

- **Part 1: Use case analysis** (Sections 2 to 4). The first part of the paper aims at giving a comprehensive analysis of use cases compiled from several sources. The objectives of this work are to discover those concepts and categorizations which are important, and to identify "gaps" to be able to address use cases suitable for the German public sector. The definition and analysis of the use cases will be performed using various sources, such as:
  - Microsoft use cases provided for NIST (1)
  - NIST use cases, especially "Jumpstart" use cases (2)
  - Architecture and use cases from the DMTF Open Cloud Standards Incubator (3)
  - Use cases from the Cloud Computing Use Case Discussion group[1] (4)
- **Part 2: Use case synthesis** and conclusion (Sections 5 to 7). This second part aims on developing usage scenarios which are relevant for the German public sector. This work has been underpinned by a number of interviews with members from German data centers. In particular, the three identified usage scenarios are describing novel Cloud based services, which are suitable for a prototypical implementation and deployment as pilot projects. For demonstration purpose one of these scenarios is going to be implemented within the FOKUS eGovernment (SOA/Cloud) lab.

Some additional material has been arranged in several annexes, including:

- The questionnaire used in the interviews with German service centres
- A detailed specification of the demonstrator implementation.
- Definition and exemplification of templates for the description and analysis of usage scenarios and use cases.
- Acronyms, Glossary, and References.

[1] http://cloudusecases.org

2 Cloud Definitions and Architectures

This section gives a short state-of-the-art introduction to the definitions and architectures of Cloud Computing that are relevant for this document. The first three Subsections 2.1, 2.2, and 2.3 summarize the major definitions and architectures around Cloud Computing that have been introduced respectively by the National Institute of Standards and Technology (NIST), the Distributed Management Task Force (DMTF), and the Cloud Computing Use Case Discussion Group (CCUCDG). The actor models are of particular interest for the definition of Cloud use cases because each set of use cases depends heavily on the actors that are triggering its execution.

2.1 NIST Basic Definitions of Cloud Computing

The NIST definitions of Cloud Computing (5), (6) are the most agreed and cited definitions that currently exist. They define the utmost common agreement on Clouds and are used as a starting point for the discussion in this document. "*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*"

Five essential characteristics of Cloud Computing are identified:

- ***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 data-center). 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.*

Moreover, three service delivery models are defined:

- ***Cloud Software as a service (SaaS).*** *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). 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.*

- ***Cloud Platform as a service (PaaS).*** *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. 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.*
- ***Cloud Infrastructure as a service (IaaS).*** *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. 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).*

The CCUCDG (4) uses the same service delivery models, but with a slightly different interpretation:

- ***SaaS:*** *The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running.*
- ***PaaS:*** *The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework.*
- ***IaaS:*** *The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them.*

Finally, four deployment models for Cloud infrastructures are described by NIST (5):

- ***Private cloud****. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.*
- ***Community cloud****. The cloud infrastructure is shared by several organizations 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.*
- ***Public cloud****. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.*
- ***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).*

The CCUCDG (4) uses similar deployment model categories, but with a slightly different interpretation:

- ***Private Cloud:*** *A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.*
- ***Community Cloud:*** *A community cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.*

- ***Hybrid Cloud:*** *A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non-business critical information and processing to the public cloud, while keeping business-critical services and data in their control.*
- ***Public Cloud:*** *In simple terms, public cloud services are characterized as being available to clients from a third party service provider via the Internet. The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.*

2.2 DMTF Cloud Reference Architecture and Life Cycle Model

This section gives an introduction to the DMTF architecture together with the associated service life cycle and interoperability concepts. The work of the DMTF is of special interest because it has a clear focus on the life cycle of Cloud Services and provides a comprehensive set of related use cases together with detailed formal specifications of provider interfaces. The glossary provided by the DMTF can be used as a starting point for a common glossary on relevant terms for Cloud Computing.

The *Open Cloud Standards Incubator* of the Distributed Management Task Force has published three White Papers about Cloud Computing. The first paper focuses on *Cloud Interoperability* (6), the second on *Cloud Architecture and Management* (7) and the third on *Use Cases for Cloud Management* (3).

The White Paper on *Cloud Architecture and Management* (7) gives a comprehensive summary of Cloud relevant aspects. It contains a glossary that defines relevant terms such as:

- ***Cloud service:*** *a publicly available service or a private service that is used within an enterprise*
- ***Provider interface:*** *the interface through which consumers of cloud service access and monitor their contracted services. The interface covers service level agreement (SLA) negotiation, service access, service monitoring, and billing. This interface is also the interface through which a cloud service developer interacts with a cloud service provider to create a service template that is added to the service catalogue.*

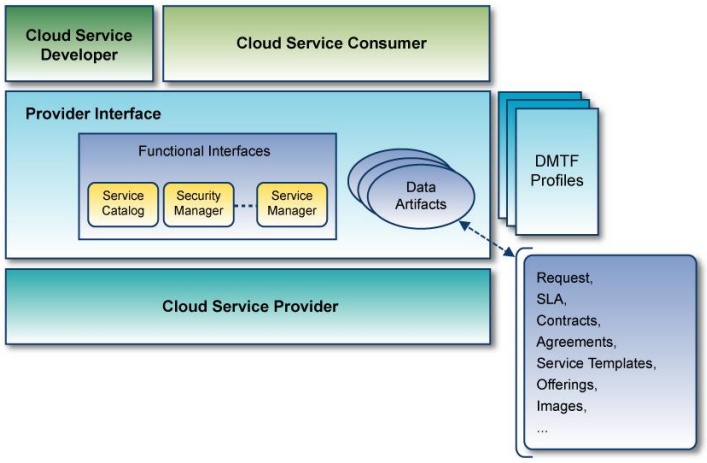


Figure 1: DMTF Cloud Service Reference Architecture (7)

The proper definition of the lifecycle of cloud services allows the identification of exemplary functional interfaces that cloud consumers need to establish with the cloud service provider. The cloud service reference architecture (Figure 1) describes key entities such as actors, interfaces, data artefacts, and profiles with an indication of interrelationships among them.

The life cycle of cloud services is the nucleus of the DMTF White Papers. For this reason the papers introduce various stages and artefacts around cloud services and derive use cases and management functionality from these artefacts that are shown in Figure 2 (also, compare Figure 8: DMTF Cloud Service Lifecycle States and Use Cases on page 13). The following stages are defined within the lifecycle:

1. ***Template:*** *A developer defines the service in a template that describes the content of and interfaces to a service.*
2. ***Offering:*** *A provider applies constraints, costs, and policies to a template to create an offering available for request by a consumer.*
3. ***Contract:*** *A consumer and provider enter into a contract for services, including agreements on costs, SLAs, SLOs, and specific configuration options.*
4. ***Provision Service:*** *A provider deploys (or modifies) a service instance per the contract with the consumer.*
5. ***Runtime Maintenance:*** *A provider manages a deployed service and all its resources, including monitoring resources and notifying the consumer of key situations.*
6. ***End of Service:*** *A provider halts a service instance, including reclaiming resources for redeployment to support other service.*

Currently the DMTF describes only a subset of all use cases around the life cycle of cloud services. The complete list of use cases is shown in Figure 5 and will probably extend the cloud service artefacts depicted in Figure 2.

The use cases introduced and specified in (3) are directly related to the different stages of the life cycle of cloud services. The specification contains textual descriptions, sequence charts, detailed class diagrams of the Unified Modelling Language (UML), and textual descriptions for the data artefacts that are exchanged in the use cases. For this reason, the DMTF White Paper (3) comprises technical detailed specifications of use cases and protocols together with a corresponding information model.

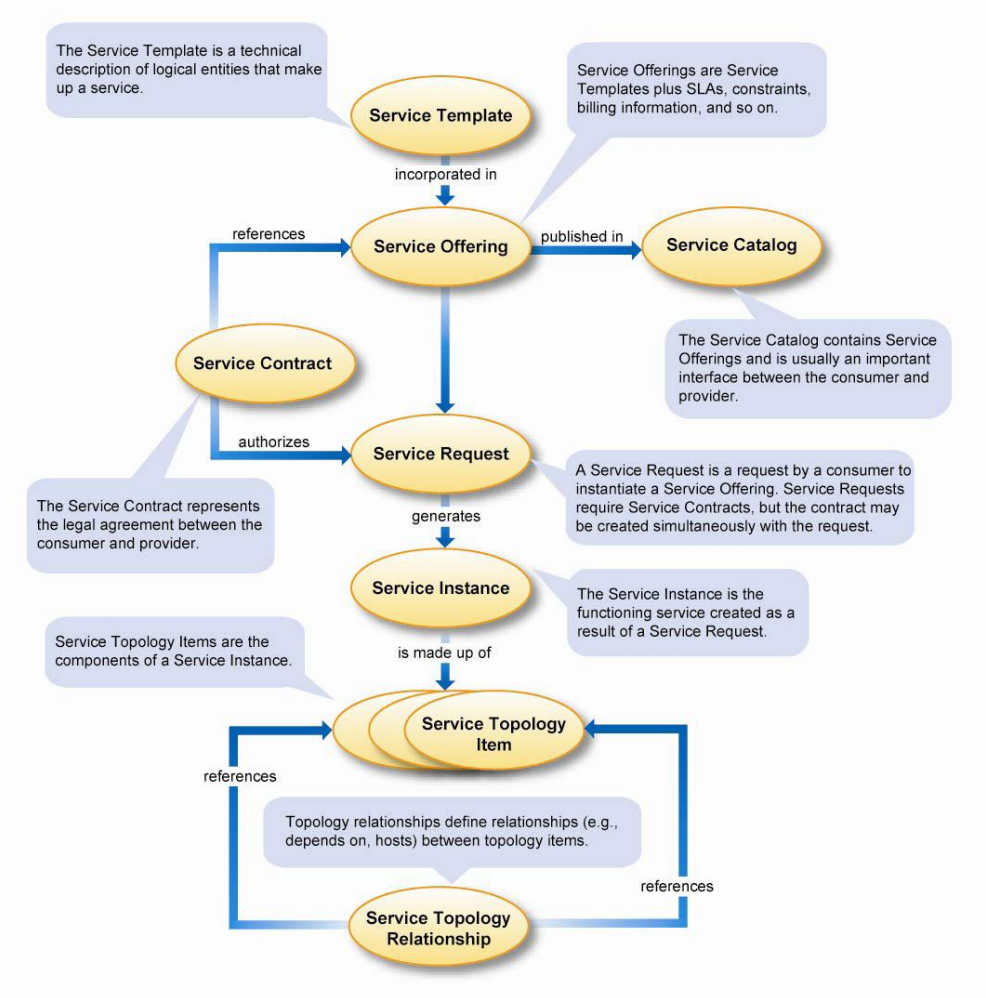


Figure 2: Overview on DMTF Cloud Service Artefacts (3)

2.3 CCUCDG Cloud Computing Taxonomy

The CCUCDG has published a White Paper with the purpose to "*to highlight the capabilities and requirements that need to be standardized in a cloud environment to ensure interoperability, ease of integration and portability*" (4). This group's activity is done following the six principles of the Open Cloud Manifesto (8).

The use cases introduced in the White Paper should:

- *Provide a practical, customer-experience-based context for discussions on interoperability and standards.*
- *Make it clear where existing standards should be used.*
- *Focus the industry's attention on the importance of Open Cloud Computing.*
- *Make it clear where there is standards work to be done. If a particular use case can't be built today, or if it can only be built with proprietary APIs and products, the industry needs to define standards to make that use case possible.*

The White Paper refers to the definitions of delivery models, deployment models and characteristics as introduced by NIST (Section 2.1). Therefore, the terminology used in the White Paper is identical to the terminology used by NIST.

Comparable to the DMTF reference architecture the CCUCDG introduces a so-called *Cloud Taxonomy* as shown in Figure 3. In this diagram, service consumers use the services provided through the cloud, service providers manage the cloud infrastructure, and service developers create the services themselves.

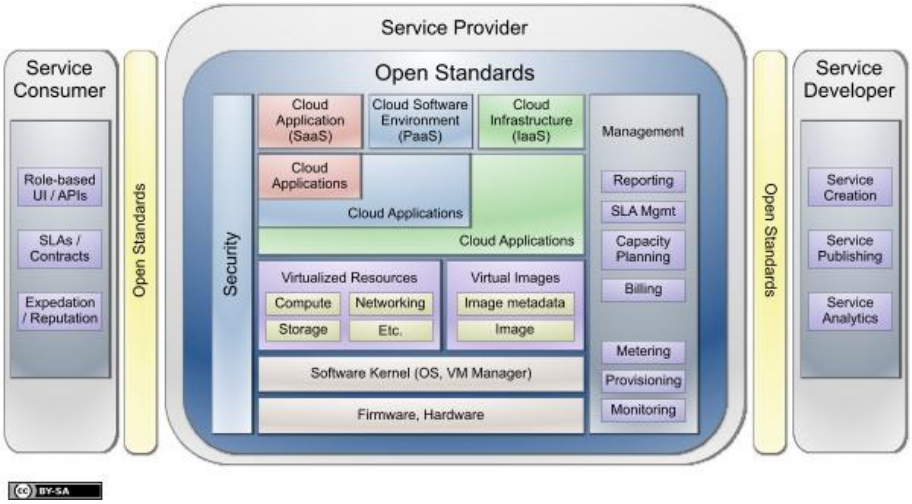


Figure 3: Cloud Computing Taxonomy from CCUCDG (4)

From this Cloud Taxonomy the paper derives a *Standards Taxonomy* (Figure 4) that can be used to categorize Cloud related standards and to identify different types of reference points.

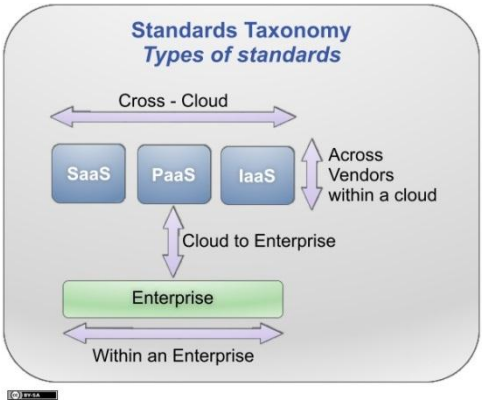


Figure 4: Cloud Standards Taxonomy by CCUCDG (4)

The different types of standards indicate several interoperability issues:

- Across Cloud Service Types
- Within Cloud Service Types
- Between the Cloud and the Enterprise
- Within an Enterprise

In addition to the use cases the White Paper (4) identifies several *security scenarios*. The purpose of this approach is to highlight the security issues that architects and developers should consider as they move to the cloud. The security topics discussed in the paper are:

- ***Regulations:*** *Regulations are not technical issues, but they must be addressed. Laws and regulations will determine security requirements that take priority over functional requirements.*

- ***Security Controls:*** *Although a given consumer might need all of these security controls, consumers should be wary of any cloud provider that makes security-related claims and reassurances without an infrastructure capable of delivering all of them.*
- ***Security Federation Patterns:*** *To implement these security controls, several federation patterns are needed. Cloud providers should deliver these patterns through existing security standards.*

A comparison of *SLA requirements* and a cross-reference between these requirements and the Cloud delivery models (similar to that defined by the NIST) conclude the White Paper.

2.4 Stakeholders and Actors

2.4.1 Cloud Computing Use Case Discussion Group

In the context of Cloud Computing, the CCUCDG (4) defines several actors. The relation between these actors within the Cloud Computing taxonomy is depicted in Figure 3.

1. ***Service Consumer:*** *The service consumer is the end user or enterprise that actually uses the service, whether it is Software, Platform or Infrastructure as a Service. Depending on the type of service and their role, the consumer works with different user interfaces and programming interfaces. Some user interfaces look like any other application; the consumer does not need to know about cloud computing as they use the application. Other user interfaces provide administrative functions such as starting and stopping virtual machines or managing cloud storage. Consumers writing application code use different programming interfaces depending on the application they are writing. Consumers work with SLAs and contracts as well. Typically these are negotiated via human intervention between the consumer and the provider. The expectations of the consumer and the reputation of the provider are a key part of those negotiations.*
2. ***Service Provider:*** *The service provider delivers the service to the consumer. The actual task of the provider varies depending on the type of service:*
   - *For Software as a Service, the provider installs, manages and maintains the software. The provider does not necessarily own the physical infrastructure in which the software is running. Regardless, the consumer does not have access to the infrastructure; they can access only the application.*
   - *For Platform as a Service, the provider manages the cloud infrastructure for the platform, typically a framework for a particular type of application. The consumer's application cannot access the infrastructure underneath the platform.*
   - *For Infrastructure as a Service, the provider maintains the storage, database, message queue or other middleware, or the hosting environment for virtual machines. The consumer uses that service as if it was a disk drive, database, message queue, or machine, but they cannot access the infrastructure that hosts it.*
3. ***Service Developer:*** *The service developer creates, publishes and monitors the cloud service. These are typically "line-of-business" applications that are delivered directly to end users via the SaaS model. Applications written at the IaaS and PaaS levels will subsequently be used by SaaS developers and cloud providers. Development environments for service creation vary. If developers are creating a SaaS application, they are most likely writing code for an environment hosted by a cloud provider. In this case, publishing the service is deploying it to the cloud provider's infrastructure. During service creation, analytics involve remote debugging to test the service before it is published to consumers. Once the service is published, analytics allow developers to monitor the performance of their service and make changes as necessary.*

The role of a service developer is sub-divided into:

- ***Client Application developer:*** *Writes cloud-based client applications for end users;*

- ***Application developer:*** *Writes traditional applications that use the cloud;*
- ***Deployers:*** *Package, deploy and maintain applications that use the cloud. Lifecycle management is a concern here as well;*
- ***Administrators:*** *Work with applications at multiple levels, including deployment and infrastructure management;*
- ***Cloud Providers:*** *Work with the infrastructure beneath their cloud offerings*;

2.4.2 National Institute of Standards and Technology

The NIST (2) provides a fine grained actor model with a flat hierarchy. The definition of the term *actor* corresponds to the definitions in UML and the one introduced by Cockburn (10). For this reason the NIST actors can describe human roles, organizations and technical systems. The understanding of these actors and their obligations is a prerequisite for the understanding of the NIST use cases.

- ***Unidentified-user:*** *An entity in the Internet (human or script) that interacts with a cloud over the network and that has not been authenticated.*
- ***Cloud-subscriber:*** *A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud.*
- ***Cloud-subscriber-user:*** *A user of a cloud-subscriber organization who will be consuming the cloud service provided by the cloud-provider as an end user. For example, an organization's email user who is using a SaaS email service the organization subscribes to would be a cloud-subscriber's user.*
- ***Cloud-subscriber-administrator:*** *An administrator type of user of a cloud-subscriber organization that performs (cloud) system related administration tasks for the cloud-subscriber organization.*
- ***Cloud-user:*** *A person who is authenticated to a cloud-provider but does not have a financial relationship with the cloud-provider.*
- ***Payment-broker:*** *A financial institution that can charge a cloud-subscriber for cloud services, either by checking or credit card.*
- ***Cloud-provider:*** *An organization providing network services and charging cloud-subscribers. A (public) cloud-provider provides services over the Internet.*
- ***Transport-agent:*** *A business organization that provides physical transport of storage media such as high-capacity hard drives.*
- ***Legal-representative:*** *A court, government investigator, or police.*
- ***Identity-provider:*** *An entity that is responsible for establishing and maintaining the digital identity associated with a person, organization, or (in some cases) a software program.*
- ***Attribute-authority:*** *An entity that is responsible for creating and managing attributes (e.g., age, height) about digital identities, and for asserting facts about attribute values regarding an identity in response to requests.*
- ***Cloud-management-broker:*** *A service providing cloud management capabilities over and above those of the cloud-provider and/or across multiple cloud-providers. Service may be implemented as a commercial service apart from any cloud-provider, as cross-provider capabilities supplied by a cloud-provider or as cloud-subscriber implemented management capabilities or tools.*

2.4.3 Microsoft's Contribution to NIST

The actors introduced by Microsoft (1) are, like the NIST actors, organized in a flat hierarchy. Because NIST and Microsoft introduced different actors the corresponding use cases are different, too.

- ***Cloud providers:*** *Large public cloud vendors offering cloud hosting services (e.g. Amazon, Google or Microsoft), offering hosed applications running on cloud-like environments, or vendors offering cloud*

platform software and/or hardware deployable in customers' private cloud. This actor category also includes SaaS cloud vendors offering final, hosted software running in their cloud-based data centers.

- ***Cloud application developers:*** *independent software vendors developing or porting applications targeting cloud platforms and environments (includes IaaS/PaaS/SaaS clouds*
- ***Cloud operators/management:*** *People in charge of operation, management and maintenance of the cloud applications*
- ***Cloud users/consumers*** *-> End users*
- ***Cloud identity providers:*** *Cloud services offering federated identity and access control services*
- ***Cloud procurement officers:*** *People in charge of cloud service procurement*
- ***Cloud broker services:*** *Cloud services offering placement and consumer/provider brokering/matching for services offered by other cloud providers.*

2.4.4 Distributed Management Task Force

The DMTF (7) introduced a hierarchical set of actors with the same actors as CCUCDG on the top level of the hierarchy.

- ***Cloud service consumer***
  - approves business/financial expenditures for consumed services
  - maintains accounts for used service instances
  - requests service instances and changes to service instances (typically on behalf of the consumer business manager)
  - provides access to services for service users
- ***Cloud service developer***
  - designs, implements, and maintains service templates
- ***Cloud service provider***
  - an organization that supplies cloud services to one or more internal or external consumers

The DMTF actors are further discussed in the White Paper on Cloud use cases (3). The actor categories can be refined as depicted in Figure 5. The White Paper gives a detailed description of the actors. A short description is given in Figure 6.

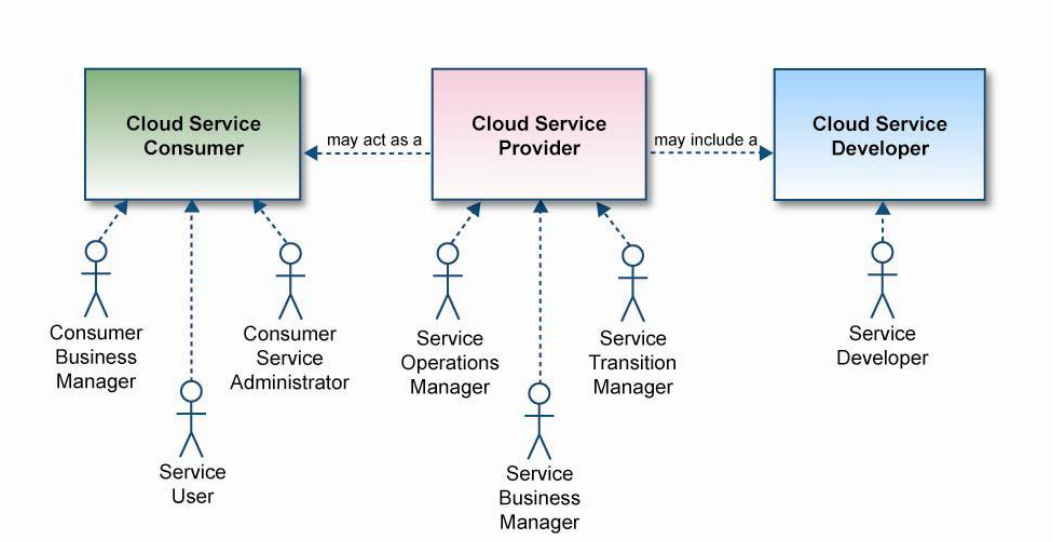


Figure 5: Categories of DMTF Cloud Actors (3)

Actor Category	Actor	Description
Cloud Service Developer	Service Developer	• Designs, implements, and maintains service templates (technical aspect). These templates can be used by providers to create offerings. The person performing this role could be employed by the same organization that is a cloud service provider or cloud service consumer.
Cloud Service Provider	Service Operations Manager	• Manages the technical infrastructure required for providing cloud services • Monitors and measures performance and utilization against SLAs • Provides reports from monitoring and measurement (used for audit and compliance)
	Service Business Manager	• Offers all types of services developed by cloud service developers • Accounts for services potentially offered by service providers themselves and services offered on behalf of cloud service developers • Establishes a portfolio of business relationships, and sets up accounts and terms for cloud service consumers (including the master account, which is the master relationship between the consumer and provider)
	Service Transition Manager	• Enables a customer to use the cloud service, including "onboarding", integration, and process adoption • Defines and creates service offerings based on templates that can be used by cloud service consumers and are populated into the catalog
Cloud Service Consumer	Consumer Business Manager	• Approves business and financial expenditures for consumed services • Accounts for used service instances • Establishes business relationships; sets up accounts, budget, and terms; and so on
	Consumer Service Administrator	• Requests service instances and changes to service instances (typically on behalf of the consumer business manager) • Purchaser of services with the business relationship; creates Service User roles • Creates users (including policies), allocates resources, such as compute and storage, generates reports (usage); performs actions for a specific set of resources
	Service User	• Uses service instances provided by a cloud service provider. The Service User role is distinct from the Consumer Service Administrator role because it has no responsibility for managing the service.

Figure 6: Description of DMTF Cloud actors (3)

3 Cloud Use Case Approaches

3.1 Cloud Computing Use Case Discussion Group

The CCUCDG introduces Enterprise Cloud Usage scenarios that are intended to illustrate the most typical cloud use cases and are not meant to be an exhaustive list of realizations within a cloud environment. The White Paper (4) identifies for each use case the requirements that are necessary to implement the use case. A table linking the requirements to the use cases is given. Therefore a comprehensive list of requirements is provided as part of this table.

The Cloud *usage scenarios* identified by the CCUDG are:

- (CCUS01) End User to Cloud: Applications running on the cloud and accessed by end users
- (CCUS02) Enterprise to Cloud to End User: Applications running in the public cloud and accessed by employees and customers
- (CCUS03) Enterprise to Cloud: Cloud applications integrated with internal IT capabilities
- (CCUS04) Enterprise to Cloud to Enterprise: Cloud applications running in the public cloud and interoperating with partner applications
- (CCUS05) Private Cloud: A cloud hosted by an organization inside that organization's firewall
- (CCUS06) Changing Cloud Vendors: An organization using cloud services decides to switch cloud providers or work with additional providers.
- (CCUS07) Hybrid Cloud: Multiple clouds work together, coordinated by a cloud broker that federates data, applications, user identity, security and other details.

For selected usage scenarios, additional *customer scenarios* are described that explain the relevance of the usage scenario in a certain application domain:

- (CCCS01) Enterprise to Cloud - Payroll Processing
- (CCCS02) Enterprise to Cloud to End User - Logistics & Project Management
- (CCCS03) Private Cloud - Central Government Service in the Cloud
- (CCCS04) Hybrid Cloud - Local Government Services in a hybrid Cloud
- (CCCS05) Enterprise to Cloud to End User – Astronomic Data Processing

In the context of this White Paper the customer scenarios 3 and 4 are of special interest because they focus on (Japanese) eGovernment. As an example Figure 7 shows the configuration of a hybrid Cloud as used in the 4th scenario:

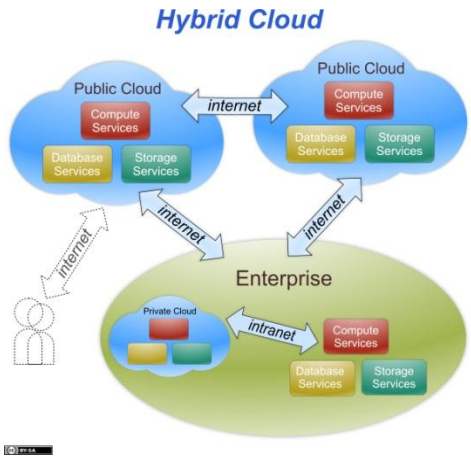


Figure 7: Configuration of a Hybrid Cloud (4)

Comparable to customer scenarios the paper introduces specific real world *security scenarios*:

- Computing Power in the Cloud
- Cloud-based Development and Testing
- Storage in the cloud
- Cross-Reference: Security Controls and Customer Scenarios
- Cross-Reference: Security Federation Patterns and Customer Scenarios

These scenarios show how security control and security federation patterns introduced in the paper can be applied.

3.2 Distributed Management Task Force

The use cases defined by the DMTF's Open Cloud Standards Incubator consider cloud management, especially the life service of Cloud services. The DMTF introduces six lifecycle states of a typical cloud service together with the use cases that are most relevant to each state. The use cases are assigned to the different states as shown in Figure 8. Only the use cases marked by an asterisk (*) are specified in detail in the White Paper (3).

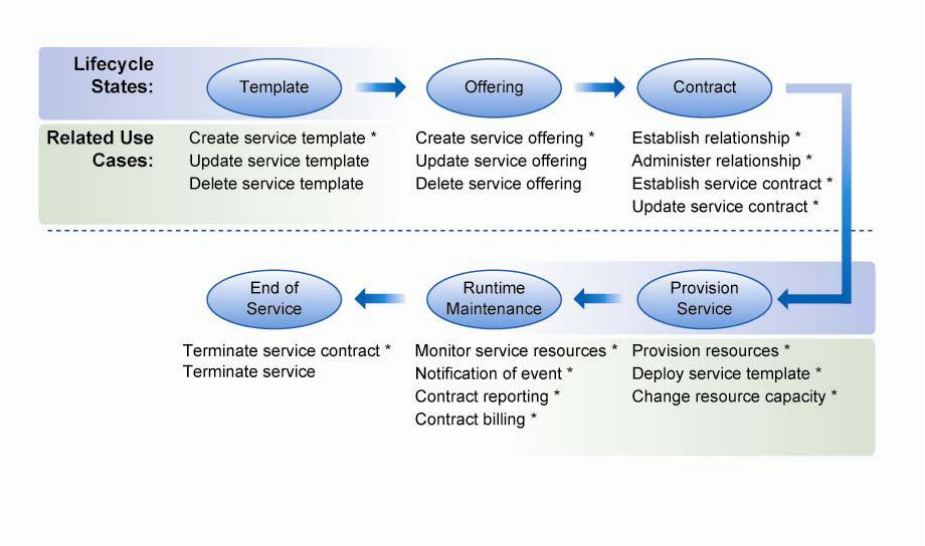


Figure 8: DMTF Cloud Service Lifecycle States and Use Cases (7)

As shown in Figure 8 the White Paper (3) describes the following use cases providing textual specifications of the use cases and the exchanged data artefacts as well as UML sequence diagrams and class diagrams:

- (DMTF01) Establish relationship
- (DMTF02) Administer relationship
- (DMTF03) Establish service contract
- (DMTF04) Update service contract
- (DMTF05) Contract reporting
- (DMTF06) Contract billing
- (DMTF07) Terminate service contract
- (DMTF08) Provision resources
- (DMTF09) Deploy service template
- (DMTF10) Change resource capacity
- (DMTF11) Monitor service resources
- (DMTF12) Create service template
- (DMTF13) Create service offering
- (DMTF14) Notification of service condition or event

Of special interest concerning Cloud interoperability are the interaction patterns introduced in (7). An analysis of various cloud management use cases revealed that each use case could be decomposed into a combination of interaction patterns. An interaction pattern consists of a sequence of messages. For any interaction pattern, the specific messages may vary from use case to use case, but the messages have similar characteristics at an architectural level, particularly the protocol and security considerations.

Figure 9 shows the interaction patterns, grouped in four broad categories.

- ***Identify:*** *A person or entity that interacts with the cloud service provider establishes their identity and receives appropriate credentials, such as a session token. An identity token may also be obtained through an external identity provider that has a trust relationship with the cloud service provider. Operations and data are made accessible to the connection authenticated by the credentials or identity token.*
- ***Administer:*** *These patterns work with the data that describe offerings, users, and other administrative metadata information needed for interactions with the cloud service provider. For example, an administrator or operator may browse a list of available offerings to select one, to update its metadata to configure it for a particular purpose, and to retrieve details about how to access instances of a service that is part of the offering.*
- ***Deploy and update:*** *These patterns (there are actually two types of Negotiate/Provision Resources) are used when selecting services and resources, and then making them into services. Included are any needed negotiations about the amount and type of resource, operations to provision services including the infrastructure that supports them, and tracking the status of what may be long-running operations.*
- ***Steady state:*** *These patterns are used after services and resources have been provisioned and are in use. They include client-initiated requests such as a report request and notifications from a provider about situations that are of interest to a consumer and that may require remediation actions.*

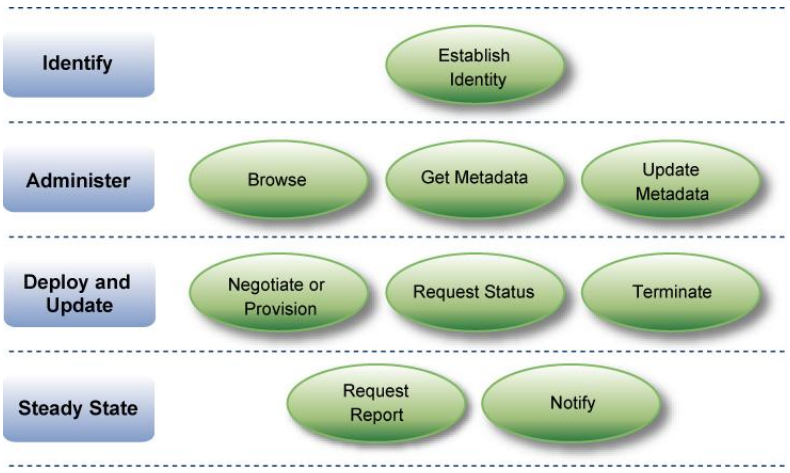


Figure 9: DMTF Categories of Interaction Patterns (7)

The White Paper (7) gives an example how these patterns can be used to implement a use case. Assuming that the pattern can be standardized somehow, they can also be used to define interoperable implementations of the various use cases introduced by DMTF. As well a more detailed technical specification of corresponding *message exchange pattern* is given (7).

3.3 National Institute of Standards and Technology

NIST formally defines the cloud use cases as follows: a description of how groups of ***users*** and their ***resources*** may interact with one or *more cloud computing systems to achieve specific goals.*

The NIST use case should help to answer the following questions (2):

- If a customer wishes to move their workload away from a cloud provider, can that be done at low cost and disruption? I.e., does the cloud provide **portability**?
- Can a customer concurrently employ multiple cloud providers to achieve a single goal at low cost? I.e., does the cloud provide **interoperability**?
- What support for security can cloud providers offer to allay concerns about how customer data is protected from unauthorized disclosure or modification; and what kinds of availability requirements can cloud providers satisfy? I.e., does the cloud provide support for **security**?

Because the agreement on standards to solve these problems is quite time consuming, NIST has started the Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC) project to generate concrete data about how different kinds of cloud system interfaces can support portability, interoperability, and security. The SAJACC intends to perform the following tasks:

- ***Develop*** a set of ***cloud system use cases*** that express selected portability, interoperability, and security concerns that cloud users may have;
- ***Select*** a small set of existing ***cloud system interfaces*** that can be used for testing purposes;
- ***Develop*** a ***test driver*** for each use case and selected system interface, that represents (to the extent possible) the operation of the use case on the selected system interface;
- ***Run*** the ***test drivers*** and document the extent each test driver can run on each selected system interface, and ***document*** any portability, interoperability, or security implications of the test run;
- ***Publish*** all use cases, test codes, and test results on the openly-accessible NIST Cloud Portal (www.nist.gov/itl/cloud), for use by Standards Development Organizations and other interested parties.

In the context of the available White Paper the first two activities are of special interest.

In the presentation (11) about SAJACC the following categorization of use cases is provided:

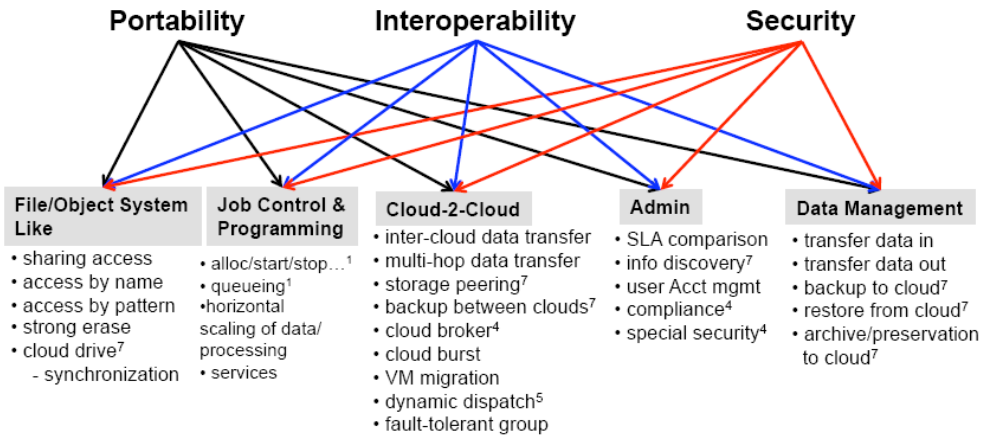


Figure 10: Preliminary Use Case Taxonomy for a Public Cloud (11)

These categories correspond to the three fundamental questions NIST has raised in (2). The use cases can be seen as predecessors of the use cases described below that are derived again from (2). This document uses the following categories:

- Cloud management
- Cloud interoperability
- Cloud security

The description of the use cases follows the ideas of Cockburn (10). It uses the actors introduced in Section 2.4.

- ***Cloud Management Use Cases***
  1. *(NIST01) Open an account:* Cloud-provider opens a new account for an unidentified-user who then becomes a cloud-subscriber
  2. *(NIST02) Close an account:* Close an existing account for a cloud-subscriber
  3. *(NIST03) Terminate an account:* Cloud-provider terminates a cloud-subscriber's account
  4. *(NIST04) Copy data objects into a cloud:* Cloud-subscriber initiates a copy of data objects from the cloud-subscriber's system to a cloud-provider's system. Optionally, protect transferred objects from disclosure
  5. *(NIST05) Copy data objects out of a cloud:* Cloud-subscriber initiates a copy of data objects from a cloud-provider's system to a cloud-subscriber's system. Optionally, protect transferred objects from disclosure.
  6. *(NIST06) Erase Data objects in a cloud:* Erase a data object on behalf of a cloud-subscriber or unidentified-user.
  7. *(NIST07)* VM *Control, Allocate VM Instance:* The cloud-subscriber should have the capability to create VM images that meet its functions, performance and security requirements and launch them as VM instances to meets its IT support needs.
  8. *(NIST08) VM Control, Manage Virtual Machine Instance State:* A cloud-subscriber stops, terminates, reboots, starts or otherwise manages the state of a virtual instance
  9. *(NIST09) Query Cloud Provider Capabilities and Capacities:* A cloud-user makes a structured capability or capacity or price request to one or several cloud-providers and receives a structured response that can be used as input to drive service decisions.
- ***Cloud Interoperability Use Cases***

1. *(NIST10) Copy Data Objects between Cloud Providers:* Copy data objects from a cloud-provider-1's system to a cloud-provider-2's system on the initiative of a cloud-subscriber.
2. *(NIST11) Dynamic operation dispatch to IaaS Clouds*: Invoke operations on the most effective clouds available based on a client-side set of rules that are evaluated at runtime.
3. *(NIST12) Cloud burst from data center to cloud*: Maintain required service levels for an agency's data-center hosted process, by dynamically allocating/deallocating cloud computer or storage resources to service current demands.
4. *(NIST13) Migrate a queuing-based application*: Migrate an existing queue and associated messages from one cloud-provider to another
5. *(NIST14) Migrate (fully stopped) VMs from one cloud provider to another*: Seamlessly migrate an arbitrarily designated stopped virtual machine from cloud-provider-1 to cloud-provider-2.

- ***Cloud Security Use Cases***
  1. *(NIST15) User Account Provisioning*: The cloud-subscriber requires to provision (create) user accounts for cloud-subscriber-users to access the cloud. Optimally, the cloud-subscriber requires the synchronization of enterprise system-wide user accounts from enterprise data center-based infrastructure to the cloud, as part of the necessary process to streamline and enforce identical enterprise security (i.e., authentication and access control policies) on cloud-subscriber-users accessing the cloud.
  2. *(NIST16) User Authentification* in the Cloud: The cloud-subscriber-users should be able to authenticate themselves using a standard-based protocol, such as SAML, OpenID or Kerberos, to gain access to the cloud application/service. Alternatively, the cloud-subscriber-user should be able to transparently log in to the cloud.
  3. *(NIST17) Data Access Authorization Policy Management* in the Cloud: A cloud-subscriber-administrator should be able to manage (add/delete/change) data access authorization policies for data stored in the cloud. Note: this capability is essential to fulfill the use case of sharing access to data in a cloud.
  4. *(NIST18) User Credential Synchronization Between Enterprises and the Cloud*: The cloud-subscriber requires changes to user credentials in the enterprise's identity provider system to be automatically communicated to the corresponding infrastructure in the cloud-provider's system to ensure the integrity of access and conformance to enterprise policies are maintained in near real time. This is an extension and optimization of the use case for User Account Provisioning.
  5. *(NIST19) eDiscovery*: To maintain data objects and their metadata, which are stored and processed in a cloud, so that the data provenance can be known, and to provide data to an authorized legal-representative on request. The cloud-provider must be able to collect a snapshot of data about the cloud-subscriber.
  6. *(NIST20) Security Monitoring*: Conduct ongoing automated monitoring of the cloud-provider infrastructure to demonstrate compliance with cloud-subscriber security policies and auditing requirements.
  7. *(NIST21) Sharing of access to data in a cloud*: A cloud-subscriber makes access to objects stored in a cloud-provider selectively available to other cloud-subscribers and unidentified-users.

Moreover, several candidates for future investigation have been identified, i.e. use cases will be refined and added to the three categories introduced above.

- Future Use Case Candidates
  1. *(NIST22) Cloud Management Broker*: Provide a cloud-user a unified and enhanced management interface to multiple cloud-providers. The essential features of a cloud-management-broker are a unified interface, federated cloud-subscriber credentials for multiple cloud-providers and federated access to multiple cloud-provider programming interfaces.

2. *(NIST23) Transfer of Ownership* within a Cloud: Cloud-subscriber-1 transfers the ownership of some data objects from cloud-subscriber-1 to cloud-subscriber-2 in a cloud-provider.
3. *(NIST24) Fault-Tolerant Cloud Group*: Synthesize a highly-reliable service using the facilities of multiple cloud-providers.

3.4 Microsoft's Contribution to NIST Use Cases

In (1), Microsoft introduces a set of use cases for Cloud Computing as feedback for the SAJACC activities of NIST. These use cases are focussing on *platform-centric use cases* for the lifecycle of a cloud application. They consider maintaining, porting and building cloud applications on top of an IaaS or PaaS cloud platform. SaaS-centric use cases and consumer and citizen centric use cases will be provided later. The use cases are pragmatic and practice oriented. They are focussing on the tasks to migrate existing applications to the cloud and from one cloud to another.

1. *(MS01) Move three-tiered application from on-premises to cloud: Starting from typical on-premises, 3-tier enterprise application (Web front-end tier + Business logic/workflow tier + Database tier) and deploy/move to the cloud.*
2. *(MS02) Move three-tiered cloud application to another cloud: Start from a typical IaaS cloud-based, 3-tier enterprise cloud application (Web front-end tier + Business logic/workflow tier + Database tier + user authentication) and deploy it to another cloud.*
3. *(MS03) Move parts of an on-premises application to cloud to create a "hybrid" application: Hybrid cloud applications: parts of the on-premises application are moved to the cloud separating data from processing. Application will then partly run on-premises, and partly in the cloud.*
4. *(MS04) Hybrid application with shared user ID and access services: Same as number three, but in addition the user ID and access is shared between on premises and cloud. This requires common user ID and access control between cloud and on-premises infrastructure with either on-premises directory access or identity federation.*
5. *(MS05) Move hybrid application to another cloud with common infrastructures: Cloud portions of a hybrid cloud application are moved from cloud A to cloud B which supports common infrastructures and VM packages. Same requirements as number three; requires readily available platform neutral data access formats.*
6. *(MS06) Hybrid cloud application that uses platform services: Similar to number three except that in this case the cloud application architect chooses to implement cloud components of a hybrid application using platform services available from the cloud platform provider such as structured or unstructured cloud storage or identity and access control services.*
7. *(MS07) Port cloud application that uses platform services to another cloud: Porting an application that uses services provided by the cloud platform to another cloud platform implies same requirements as number six.*
8. *(MS08) Create cloud application with components that run on multiple clouds: Architect chooses to develop a cloud application with components that run on multiple clouds simultaneously. For example, compute cloud node uses services of a storage cloud provider at run time to store/access data and possibly uses a third party cloud provider to obtain weather, market, news streams or vertical, application specific data.*
9. *(MS09) Cloud application workload requires use of multiple clouds (Cloudburst): Sometimes referred to as a Cloud burst scenario, application normally running on-premises or in a private cloud needs to elastically run on other clouds in the cases of short term, but significant increase in user demand load. Cloud tenants can use both their own private clouds as well as hosted/public clouds as the workload may require. VMs and applications can migrate between private cloud and public/hosted clouds and can seamlessly be managed from either side regardless of their location.*

10. *(MS10) Users can "shop around" for cloud services: Users and developers shop across hosted or public cloud offerings for best price/performance ratio, while optimizing against other considerations, using automated and well-formed, standardized Service Level Agreements.*

4 Cloud Use Case Analysis and Categorization

4.1 Analysis of Actor Models

In this section the different actor models provided by CCUCDG, DMTF, NIST, and Microsoft are compared and evaluated. A common hierarchical model will be defined.

4.1.1 Actor Models and Use Cases

4.1.1.1 Cloud Computing Use Case Discussion Group

The CCUCDG identifies *Enterprise Cloud Usage scenarios* (use case) and sample *Customer scenarios* from a user's point of view. Both scenario types have a high granularity and cannot be compared directly to the use cases identified by the other organisations. Those use cases have a finer granularity and are introduced from a technical, operational point of view.

Table 1: CCUCDG actors

Actors	Primary Actor	Usage scenario / Customer scenario
Service provider, Service developer	Service consumer	(CCUS01) End User to Cloud/ Payroll Processing
Service provider, Service developer	Service consumer	(CCUS02) Enterprise to Cloud to End User/ Logistics & Project Management, Astronomic Data Processing
Service provider, Service developer	Service consumer	(CCUS03) Enterprise to Cloud
Service provider, Service developer	Service consumer	(CCUS04) Enterprise to Cloud to Enterprise
Service provider, Service developer	Service consumer	(CCUS05) Private Cloud/ Central Government Service in the Cloud
Service provider, Service developer	Service consumer	(CCUS06) Changing Cloud Vendors
Service provider, Service developer	Service consumer	(CCUS07) Hybrid Cloud/ Local Government Services in a hybrid Cloud

The CCUCDG actors can be grouped as follows. The various types of service developers are not distinguished in the above mentioned usage scenarios:

Table 2: CCUCDG actor categories

Actor category	Actor
Service provider	Service provider
Service developer	Client Application developer
	Application developer
	Deployer
	Administrator
	Cloud Provider
Service customer	Service consumer

4.1.1.2 Distributed Management Task Force

The DMTF use cases are related to stages in the life cycle of a Cloud service. Most use cases are triggered by the Cloud Service customer.

Table 3: DMTF actors

Actors	Primary Actor	Use Case
Service Business Manager	Consumer Business Manager	(DMTF01) Establish Relationship
	Consumer Business Manager	(DMTF02) Administer Relationship
Service Business Manager	Consumer Business Manager	(DMTF03) Establish Service Contract
Service Business Manager	Consumer Business Manager	(DMTF04) Update Service Contract
Service Business Manager	Consumer Service Administrator, Consumer Business Manager	(DMTF05) Contract Reporting
Consumer Business Manager	Service Business Manager	(DMTF06) Contract Billing
Service Business Manager	Consumer Business Manager	(DMTF07) Terminate Service Contract
Service Operations Manager	Consumer Service Administrator	(DMTF08) Provision Resources (from a contracted pool)
Service Operations Manager	Consumer Service Administrator	(DMTF09) Deploy Service Template
Service Operations Manager	Consumer Service Administrator	(DMTF010) Change Resource Capacity
Service Operations Manager	Consumer Service Administrator	(DMTF1) Monitor (Service) Resources
	Service Developer	(DMTF12) Create Service Template
	Service Business Manager	(DMTF13) Create Service Offering
Consumer Service Administrator, Consumer Business Manager		(DMTF14) Notification of Service Condition or Event

For the DMTF actors the following relationships can be identified:

Table 4: Relationships between DMTF actors

Type	CS Consumer	CS Provider	CS Developer
Business	Consumer Business Manager	Service Business Manager	
Operation	Consumer Service Administrator	Service Operations Manager	
Usage	Service User		
Development			Service Developer

The DMTF actors can be grouped as follows:

Table 5: DMTF actor categories

Actor category	Actor
Cloud service provider	Service Business Manager
	Service Operations Manager
Supporting external actor	Service Developer
Cloud service customer	Consumer Business Manager
	Consumer Service Administrator
	Service User

4.1.1.3 National Institute of Standards and Technology

The NIST use cases identify associated actors including the triggering (primary) actor. Most use cases are triggered by a cloud-subscriber or a cloud-user and performed by the cloud-provider and supporting actors. Therefor the majority of the use cases are defined from the viewpoint of a user of cloud services who has a business relationship with the cloud provider.

Table 6: NIST actors

Actors	Primary Actor	Use Case
Cloud-provider	Unidentified-user, Cloud-subscriber,	(NIST01) Open an account
Cloud-provider Payment-broker	Cloud-subscriber Unidentified-user,	(NIST02) Close an account
Cloud-subscriber Unidentified-user,	Cloud-provider	(NIST03) Terminate an account
Cloud-provider, Transport agent	Cloud-subscriber	(NIST04) Copy data objects into a cloud
Cloud-provider, Transport agent	Cloud-subscriber, Unidentified-user	(NIST05) Copy data objects out of a cloud
Cloud-provider	Cloud-subscriber, Unidentified-user	(NIST06) Erase Data objects in a cloud
Cloud-provider	Cloud-subscriber	(NIST07) VM Control, Allocate VM Instance
Cloud-provider	Cloud-subscriber	(NIST08) VM Control, Manage Virtual Machine Instance State
Cloud-provider	Cloud-user	(NIST09) Query Cloud Provider Capabilities and Capacities
Cloud-provider, Transport-agent	Cloud-subscriber	(NIST10) Copy Data Objects between Cloud Providers
Cloud-provider	Cloud-subscriber	(NIST11) Dynamic operation dispatch to IaaS Clouds
Cloud-subscriber Cloud-management-broker	Cloud-provider	(NIST12) Cloud burst from data centre to cloud
Cloud-provider Cloud-management-broker	Cloud-subscriber	(NIST13) Migrate a queuing-based application
Cloud-provider Cloud-management-broker	Cloud-subscriber	(NIST14) Migrate (fully stopped) VMs from one cloud provider to another
Cloud-provider, Cloud-subscriber-administrator	Cloud-subscriber	(NIST15) User Account Provisioning
Cloud-provider, Cloud-subscriber, Identity-provider	Cloud-subscriber-user	(NIST16) User Authentication in the cloud
Cloud-provider, Cloud-subscriber, Cloud-subscriber-user, Identity-provider	Cloud-subscriber-administrator	(NIST17) Data Access Authorization Policy Management in the Cloud
Cloud-provider, Cloud-subscriber-administrator	Cloud-subscriber	(NIST18) User Credential Synchronization Between Enterprises and the Cloud
Cloud-provider, Cloud-subscriber, Transport-agent	Legal-representative	(NIST19) eDiscovery
Cloud-provider	Cloud-subscriber	(NIST20) Security Monitoring

Cloud-provider, Unidentified-user	Cloud-subscriber	(NIST21) Sharing of access to data in a cloud
Cloud-provider, Cloud-management-broker	Cloud-user	(NIST22) Cloud Management Broker
Cloud-provider	Cloud-subscriber	(NIST23) Transfer of Ownership within a Cloud
Cloud-provider	Cloud-subscriber	(NIST24) Fault-Tolerant Cloud Group

The NIST actors can be grouped as follows:

Table 7: NIST actor categories

Actor category	Actor
Cloud service provider	Cloud-provider
Supporting external actor	Transport-agent
	Payment-broker
	Cloud-management-broker
	Legal-representative
Cloud service customer	Cloud-subscriber
	Cloud-subscriber-administrator
	Cloud-subscriber-user
	Cloud-user
	Unidentified-user

4.1.1.4 Microsoft Use Cases

In the Microsoft use cases all actors involved in the use case are identified. The actor that is triggering the use case is not explicitly identified. It is assumed that the Cloud operator works on behalf of the Cloud provider.

Table 8: Microsoft actors

Actors	Primary Actors	Use Case
Cloud provider	Cloud operator, Cloud application developer	(MS01) Move three-tiered application from on-premises to cloud
Cloud provider	Cloud operator, Cloud application developer	(MS02) Move three-tiered cloud application to another cloud
Cloud provider	Cloud operator, Cloud application developer	(MS03) Move parts of an on-premises application to cloud to create a “hybrid” application
Cloud provider, Cloud identity provider	Cloud operator, Cloud application developer	(MS04) Hybrid application with shared user ID and access services
Cloud provider	Cloud operator, Cloud application developer	(MS05) Move hybrid application to another cloud with common infrastructures
Cloud provider	Cloud operator, Cloud application developer	(MS06) Hybrid cloud application that uses platform services
Cloud provider	Cloud operator, Cloud application developer	(MS07) Port cloud application that uses platform services to another cloud
Cloud provider	Cloud operator,	(MS08) Create cloud application with components that run on

	Cloud application developer	multiple clouds
Cloud provider	Cloud operator, Cloud application developer	(MS09) Cloud application workload requires use of multiple clouds (Cloudburst):
Cloud provider, Cloud procurement officers, Cloud broker services	Cloud users / consumers	(MS10) Users can “shop around” for cloud services

The Microsoft actors can be grouped as follows:

Table 9: Microsoft actor categories

Actor category	Actor
Cloud service provider	Cloud provider
	Cloud operator / manager
Supporting external actor	Cloud application developer
	Cloud procurement officers
	Cloud broker services
	Cloud identity provider
Cloud service customer	Cloud user / consumer

4.1.2 Evaluation of the Actor and Use Case Definitions

CCUCDG uses the three basic categories service customer, service provider and service developer. The service developer role is divided into several sub-roles that are not considered explicitly in the usage scenarios. The usage scenarios are triggered by the service customers. Usage scenarios are quite abstract and focus on different deployment models and configurations.

DMTF identifies Cloud service customer, service providers and service developers. The use cases focus on the life-cycle of Cloud services. Therefor several use cases are triggered by service customers. The approach distinguishes administrative and technical relations between providers and customers. DMTF defines an actor hierarchy. Use cases and associated operations and data types are specified in detail using UML as a specification language.

NIST identifies Cloud service customers, - providers and external supporting actors such as developers. A detailed role model is defined for service customers and to some extend for external actors. The detailed customer model allows the definition of administrative and of technical use cases. The NIST use cases are sub-divided into management, interoperability and security related use cases.

Microsoft uses the same categories as NIST with a focus on external actors. Most use cases are triggered from an internal Cloud operator. The identified use cases are technical ones.

Although all approaches use similar categories the intention of the use cases are different. High level usage scenarios, Cloud service life-cycle use cases, a mixture of administrative and technical use cases, and pragmatic "important" use cases are identified and described. All approaches distinguish Cloud service providers, service customers, and external actors such as developers and identity providers. The granularity of these roles and there definitions are somehow different.

Assuming that the following aspects are of special importance for the implementation of Cloud service in the German public sector

- Interoperability
- Security
- Data import and export
- Move applications to the cloud

the following use cases are of special importance:

Table 10: Important use cases

Source	Actors	Primary Actor	Use Case
CCUCDG	Service provider, Service developer	Service consumer	(CCCS03) Private Cloud/ Central Government Service in the Cloud
	Service provider, Service developer	Service consumer	(CCUS06) Changing Cloud Vendors
	Service provider, Service developer	Service consumer	(CCCS04) Hybrid Cloud/ Local Government Services in a hybrid Cloud
NIST (data)	Cloud-provider, Transport agent	Cloud-subscriber	(NIST04) Copy data objects into a cloud
	Cloud-provider, Transport agent	Cloud-subscriber, Unidentified-user	(NIST05) Copy data objects out of a cloud
	Cloud-provider	Cloud-subscriber, Unidentified-user	(NIST06) Erase Data objects in a cloud
NIST (interop)	Cloud-provider, Transport-agent	Cloud-subscriber	(NIST10) Copy Data Objects between Cloud Providers
	Cloud-subscriber Cloud-management-broker	Cloud-provider	(NIST12) Cloud burst from data center to cloud
	Cloud-provider Cloud-management-broker	Cloud-subscriber	(NIST14) Migrate (fully stopped) VMs from one cloud provider to another
NIST (security)	Cloud-provider, Cloud-subscriber, Identity-provider	Cloud-subscriber-user	(NIST16) User Authentication in the cloud
	Cloud-provider, Cloud-subscriber, Cloud-subscriber-user, Identity-provider	Cloud-subscriber-administrator	(NIST17) Data Access Authorization Policy Management in the Cloud
	Cloud-provider, Unidentified-user	Cloud-subscriber	(NIST21) Sharing of access to data in a cloud
	Cloud-provider, Cloud-subscriber, Transport-agent	Legal-representative	(NIST22) eDiscovery
	Cloud-provider	Cloud-subscriber	(NIST23) Transfer of Ownership within a Cloud
Microsoft	Cloud provider	Cloud operator, Cloud application developer	(MS01) Move three-tiered application from on-premises to cloud
	Cloud provider	Cloud operator, Cloud application developer	(MS03) Move parts of an on-premises application to cloud to create a “hybrid” application
	Cloud provider, Cloud identity provider	Cloud operator, Cloud application developer	(MS04) Hybrid application with shared user ID and access services

Of course the life-cycle related use cases identified by DMTF are of interest in the public sector, too. Nevertheless it is not clear, if there are any specific aspects in the public sector concerning the life-cycle of Cloud services. This question has to be answered separately when the specification of such use cases is completed. As depicted in Figure 8 there are still several use cases that have not been specified. Especially use cases about the migration of Cloud services between Cloud providers have not been identified at all.

4.1.3 Extension of the Actors Models with Respect to German Electronic Government

In a second step the following actors derived from a German eGovernment perspective have to be added to the actor model.

- The ***Citizen*** who use Cloud services provided by a ***governmental Cloud provider***. In Germany, special policies for dealing with personal data apply. For instance, citizen's rights are:
  - Disclosure of stored personal data, from which sources these data originate, and for which purposes they are stored.
  - Correction if false personal data are stored
  - Authorization of transmission of personal data to third parties
  - Deletion of blocking of personal data
  - Complaint at the responsible ***data protection official***.
- ***Enterprise***. A commercial institution in the role of a customer of Cloud services. The crucial difference to a ***citizen*** in the role of a customer is that data protection rules for enterprise data are less restrictive.
- ***Government agency.*** An agency who uses Cloud services to support its internal processes. These services might be provided by a ***private sector provider*** or a ***public sector provider***. It is crucial to understand that in Germany, governmental agencies using Cloud (or otherwise outsourced services) have responsibilities different from private businesses: In general, the responsibility for the realization, efficiency, and security of the core tasks an agency is concerned with (i.e., providing services to citizens) has to remain (in a legal sense) at the agency itself. This implies that those agencies are in charge to monitor and control the execution of processes at the provider. Within a government agency, we have two more concrete roles:
  - Governmental service administrator. The actual person who performs service management tasks on behalf of a government agency.
  - Governmental ***service user.*** Official using a Cloud service to perform administrative tasks.
- ***Governmental Cloud provider:*** A Cloud provider who provides Cloud services to a government agency; either a ***public sector provider*** or a ***private sector provider***.
  - ***Public sector provider.*** A Cloud provider who provides Cloud services to a government agency, or a ***citizen*** or an ***enterprise*** on behalf of a ***government agency***, and belongs to the public sector. In Germany, it is (with a small number of exceptions) not possible that a ***public sector provider*** has private sector customers. Hence, services provided to citizens are necessarily on net costs.
  - ***Private sector provider.*** A Cloud provider who provides Cloud services to a government agency, or a ***citizen*** or an ***enterprise*** on behalf of a ***government agency***, and belongs to the private sector. A private sector provider might have private sector customers as well, and employ proper business models.
- ***Data protection official/authority***. Person within an institution (e.g., an enterprise) or an institution responsible to oversee the implementation of and compliance with data protection policies. In Germany, every company has to have a data protection official. Data protection authorities are moreover established both on state and on federal states level of the German governmental structure. IT providers have to

deliver quite comprehensive information, e.g., on hard- and software, monitoring data, established procedures, etc. to those authorities.

The three main actor categories identified above are Cloud service providers, Cloud service customers and supporting actors. Focussing on the NIST and Microsoft approaches we get the following table that is extended and refined with the specific actors defined above.

Table 11: Extended actor model

Source	Actor category	Actor	German specific actors
Cloud service provider			
NIST		Cloud-provider	Governmental Cloud provider
			Public sector provider
			Private sector provider
Microsoft		Cloud provider	
Microsoft		Cloud operator / manager	
Supporting external actor			
NIST		Transport-agent	
NIST		Payment-broker	
NIST		Cloud-management-broker	
NIST		Legal-representative	
Microsoft		Cloud application developer	
Microsoft		Cloud procurement officers	
Microsoft		Cloud broker services	
Microsoft		Cloud identity provider	
			Data protection official
			Data protection authority
Cloud service customer			
NIST		Cloud-subscriber	Enterprise
			Government agency
NIST		Cloud-subscriber-administrator	Governmental service administrator
NIST		Cloud-subscriber-user	Governmental service user
NIST		Cloud-user	Citizen
NIST		Unidentified-user	

The newly introduced actors show the separation between public and private sectors and the necessity of a data protection official in the German public sector.

4.2 Use Case Taxonomy

The use cases that have been introduced in section 3 and discussed in section 4.1 can be divided into the *usage scenarios* introduced by CCUCDG and *technical use cases* as introduced by DMTF, NIST and Microsoft. The *usage scenarios* can be instantiated by complex *customer scenarios* such as the scenarios introduced by CCUCDG or the scenarios mentioned by ENISA in (12). The *technical use cases* can be subdivided in *life-cycle* related use cases as introduced by DMTF, *management*, *security* and *interoperability* related use cases as introduced by NIST and *portability* related use cases as introduced by Microsoft.

Customer scenarios and technical use cases can be considered as orthogonal. The implementation of any customer scenario requires the consideration of a subset of the technical use cases. It has to be analysed, if it is possible to define already mappings between the generic usage scenarios and the technical use cases.

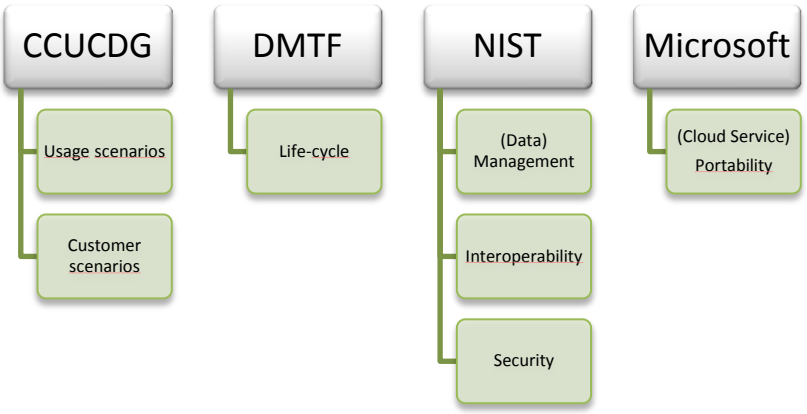


Figure 11: Use case classification

This high level categorization of cloud use cases is shown in Figure 11. A detailed taxonomy based on the categorization of actors and use cases provided in Section 4.1 is shown in Figure 12. The customer scenarios are not shown in this figure; the use cases ("leaves") are partially combined.

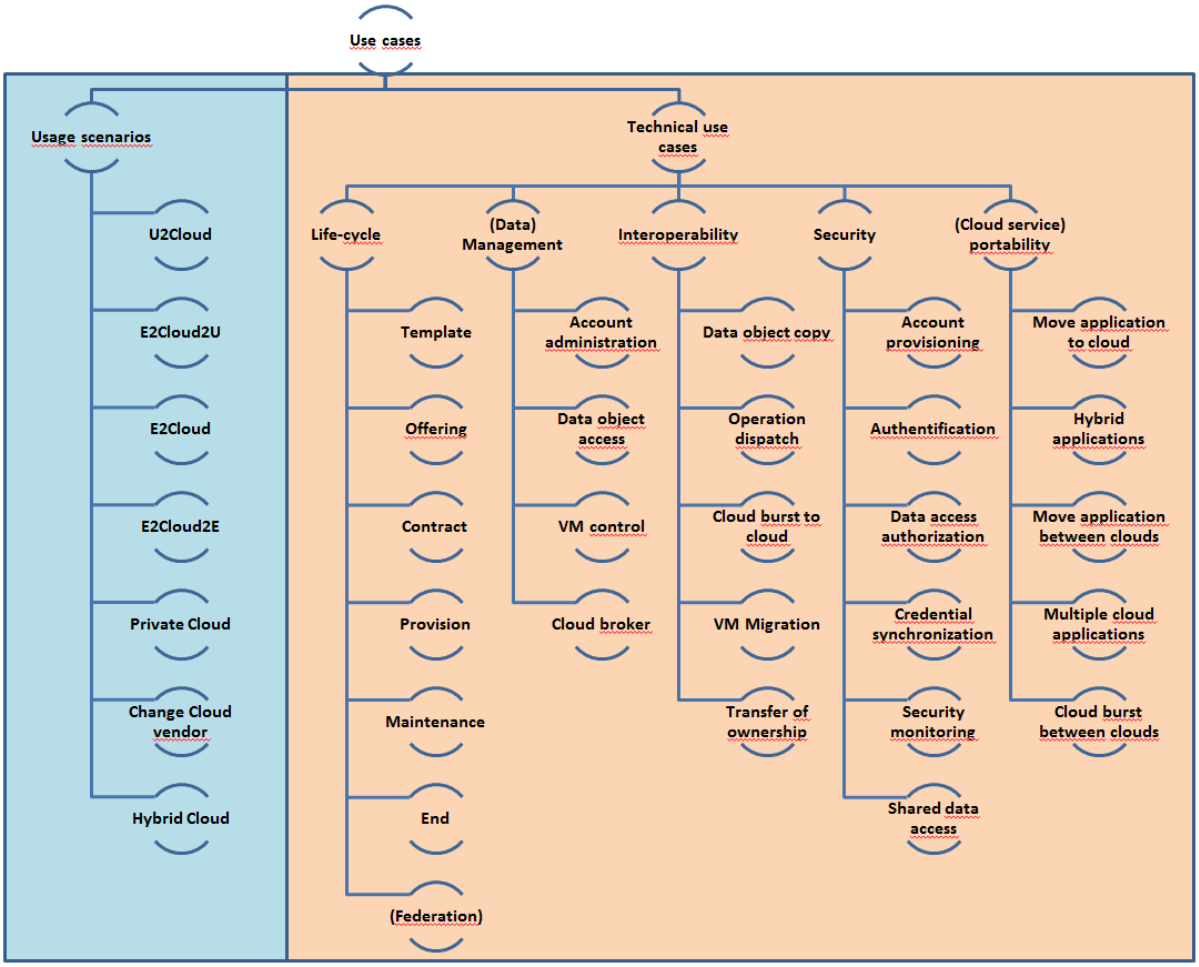


Figure 12: Use case taxonomy

Figure 12 provides a two-dimensional view on use cases. One dimension focuses on application scenarios, the other dimension on technical aspects. As already mentioned it has to be analysed if a direct mapping between usage scenarios and use cases is possible or if it only is possible to map real world customer scenarios to the technical use cases.

4.2.1 Additional Dimensions

To evaluate the technical use cases and to identify those which are relevant for the German public sector additional dimensions of the Cloud space have to be considered.

- The ***deployment model*** (private, public, hybrid, community) may be restricted depending on the public sector usage scenario.
- The traditional ***service delivery models*** (IaaS, PaaS, SaaS) together with future delivery models such as *data as a service*, process *as a service*, *knowledge as a service*, etc., help to categorize usage scenarios as well as technical use cases.
- Specific *business models* such as G2Cloud, G2Cloud2E, G2Cloud2C, G2Cloud2G, (G=government, C=citizen, E=enterprise) can be used to refine the *usage scenarios* considering the additional actors introduced in Table 11.
- The difference between private and public sector Cloud providers have to be distinguished, too.
- The *roles* of the external actors summarized in Table 11 have to be considered.
- Additional *non-functional properties* of Cloud services (*cross issues*) such as availability, performance, resilience, accounting and billing, together with SLA policies may be considered.

4.2.2 Public Sector Business Models

The four business models identified above can be characterized as follows. The configurations of the associated basic scenarios are included from (4) for clarification. The term *Enterprise* used in the CCUCDG usage scenarios has been replaced by *Government*. *Public Cloud* has to be replaced by simply *Cloud* without any specific attribute.

- The rationales for a **Government to Cloud (G2Cloud)** business model comprise cost reduction and consolidation of IT-environment such as the introduction of shared services that are catalyst for this business model. Citizens are using public sector services provided by the government agency with being aware that some back-office services are running in the Cloud.

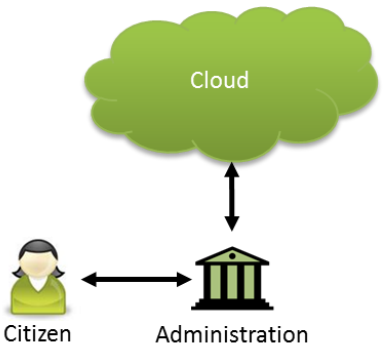


Figure 13: G2Cloud configuration

- The **Government to Cloud to Enterprise (G2Cloud2E).** Electronic procurement, applications, notifications, access to open data, processes and workflows between government and enterprises may trigger the implementation of this business model.

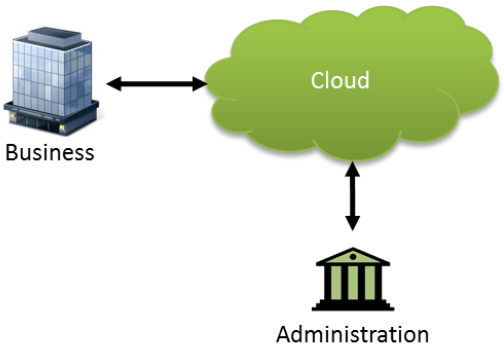


Figure 14: G2Cloud2E configuration

- **Government to Cloud to Citizen (G2Cloud2C)**. Electronic applications, notifications, eParticipation, eCollaboration, access to open data, tax return, and complaint/concern management may be triggering customer scenarios.

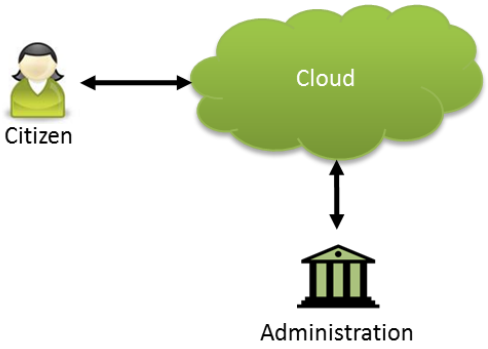


Figure 15: G2Cloud2C configuration

- Government to Cloud to Government (G2Cloud2G) refines again E2Cloud2E. Electronic support for federated, cross-governmental process, shared repositories and information systems and the electronic collaboration between public sector agencies in general are catalyst for this business model.

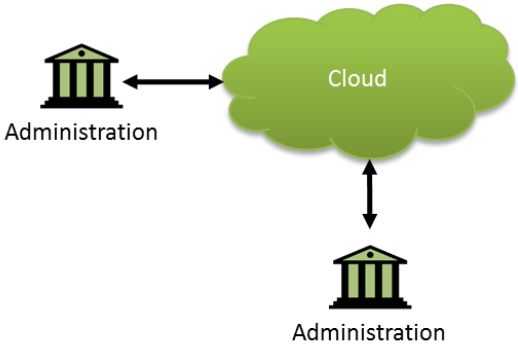


Figure 16: G2Cloud2G configuration

It has to be considered that some of the above mentioned triggers for the business models are first of all triggering the implementation of electronic government in general. They do not explicitly require the introduction of Cloud Computing, although Cloud Computing may support these models as technological or economic enabler.

4.2.3 Requirements

In the following sub-sections discuss the requirements in dependence of the chosen usage scenario.

4.2.3.1 G2Cloud

A outsources processes involving any kind of data. The data are accessed only by employees of the government agency (Governmental service users). In this situation the general regulations defined in the *BSI Baseline Protection Catalogs* (12) that have been explained above have to be considered.

4.2.3.2 G2Cloud2E

A government agency outsources processes involving *personal* and *protected enterprise data*. The data are accessed by employees of the government agency (Governmental service users) and by employees or processes of the enterprise (Enterprise service user).

However, the interaction between enterprises and administration includes a lot of issues: Security and work safety, tax reporting, defense and public safety, environmental protection, data concerning hygienic and sanitary issues (in particular if food processing and gastronomy is involved), drugs and pharmaceutical products, etc.

A concrete example is the set of processes for income tax reports. Additionally to security and resilience, data protection becomes an issue. Again, the *BSI Baseline Protection Catalogs* (12) give a collection of requirements:

- Prioritization of technical and organizational measures for problem detection, analysis, solution, and reporting
- Judicial aspects (data protection regulations)
- Lifecycle management of processes: planning an conception, deployment, operation, termination (see below)
- Monitoring of the legal situation (e.g., to take changes in data protection regulations into account)
- Technology-monitoring (newly detected vulnerabilities, new authorization mechanisms, etc.)
- Definition of responsibilities
- Geographical location of date storage devices (within EU, additionally, the location of data need to be traceable)
- Regulatory requirements: Control of lawfulness of usage and storage of personal data, implementation of citizen's rights, necessity of data processing, etc.
- Technical measures: Entrance control (premise), access control, transmission control, input control, etc. Those measures need to be implemented and validated by compliance audits by the customer (i.e., the government agency) or a certification agency.
- Staff training and information
- Reporting. This includes system level configuration, user accounts, authorization profiles, software changes, data backup and recovery measures, file system changes, usage of administration tools, logging of unauthorized access efforts and violation of authorizations, data input, data transmission, data usage (in particular in connection with automated processes), deletion of data, software and service usage. The recipient of those logs is the responsible data protection authority or a certification agency (e.g., for annual checks).
- Deletion of personal data. This is of particular importance because according to German regulations, data are allowed to be stored only if a concrete (lawful) reason for that is given. It is not possible to collect data for possible future usage. This requires that data are deleted if the concrete reason for storing them is no longer valid.

4.2.3.3 G2Cloud2C

A government agency outsources processes involving *personal data*. The data are accessed by employees of the government agency (Governmental service users) and by the citizen.

A concrete example is the set of processes for tax collection. Additionally to security and resilience, data protection becomes an issue. Again, the general regulations defined in the *BSI Baseline Protection Catalogs* (12) that have been explained above have to be considered.

4.2.3.4 G2Cloud2G

A government agency outsources processes involving any kind of data. The data are accessed by employees of both government agencies (Governmental service users).

Only a limited number of approaches to realize this usage scenario are currently available. One of the most recent federated inter-government scenarios is the implementation of the European Services Directive (14), (15). The Services Directive facilitates the establishment of a business in Europe (EC). This concerns cases in which a legal or a natural person intends to establish a new business in a European country. But it also benefits to providers who want to establish a new business in its own Member State, as they will take advantage of simplified rules and procedures. Under a general obligation for Member States to simplify procedures and formalities some very specific obligations are established by the Directive. It requires Member States to set up "*points of single contact*" (PSC), i.e. one-stop shops through which service providers can obtain all relevant information and complete all procedures relating to their activities. It requires Member States to ensure that all these procedures and formalities can be completed from (remote) distance and by electronic means. For this reason the Member States including Germany have started to implement electronic processes between the PSC and public authorities. Such processes are blueprints for electronic G2G communication that can be supported using a common Cloud infrastructure. Other activities like the "*European Internal Market Information System*" IMI (16) or the German "*Deutsches Verwaltungsdiensteverzeichnis (DVDV)*"[2], a shared repository providing information about available public services that is operated by the German Central IT-Department, are examples for the collaboration and sharing of information between government agencies.

Nevertheless several reasons are make the implementation of the G2Cloud2G usage scenario quite difficult:

- German regulations for the interaction of several government agencies are based on the exchange of printed documents; written form is the mandatory authentication mechanism.
- Another regulation states that personal data which are collected for different purposes (and in particular by different authorities) need to be stored and processed independently of each other. A strong interpretation of this basic principle renders IT-cooperation in Germany to be very difficult. For this reason, the German constitution has been extended by a general admission of such cooperation. The precise scope of this extension is however under discussion.
- Budgeting is another issue, in particular, if institutions from different federal states in Germany are concerned. The general objection here is that if such an institution uses resources of another one, then it accesses indirectly budget from another state.
- To overcome this problems, a number of organizational forms have been defined, i.e., **agencies under public law** on federal states level, and **special purpose associations** on municipal level. The establishment of such an organization however comprises a major governmental act which cannot be motivated by efficiency considerations only.

If additionally a public Cloud is involved, difficulties become even larger:

[2] Please refer to http://www.bit.bund.de/BIT/DE/Zentrale__Dienste/DVDV/

- If an institution selects a particular private sector provider to interact with another government agency to implement a cooperation, it creates a market advantage for this provider, since the other agency is bound to contract the same provider.
- Compliance to data protection regulations becomes more difficult.

4.3 Requirements from the eScience Community

This section summarizes the user requirements identified by the Venus-C project in (17) and compares them with the requirements identified from the German public sector. The Venus-C project will provide an infrastructure (PaaS) for eScience development.

The Venus-C deliverable (17) contains preliminary descriptions of the requirements identified so far during the analysis of eScience specific use cases in the Venus-C user scenarios. Several applications have been analyzed and corresponding use scenarios have been identified. These scenarios combine computing needs in high-throughput and high-performance paradigms, workflow management, intensive data, and integration with external sources and different types of users. Most of the scenarios

- use some degree of parallel computation approach,
- require accessing external sources of data and network connections, and
- require authenticated access mainly through login and password. Anonymous access is not demanded.

The execution granularity is highly variable and the applications are data intensive. The deliverable defines an identification procedure for these requirements and drafts it at the level of general use cases such as execution, data management, security and logging. The key requirement concerning security and logging is to log and account all actions performed in the Venus-C platform.

A more detailed definition of requirements will be provided in future deliverables. The eScience related requirements for an eScience-cloud-platform can hardly be compared with the public sector related requirements discussed in this White Paper, because it addresses different issues influenced by eScience Grid computing environments. Nevertheless a deeper look into future Venus-C deliverables may be worthwhile.

5 Possible Use Cases for the Public Sector in Germany

5.1 Interviews

To evaluate the current state of applicability of Cloud Computing in the German public sector and to identify possible usage scenarios, a number of interviews with members of eGovernment service providers have been performed. For that, a questionnaire has been developed (see Appendix 8) and used as a framework to guide the interviews.

The interviews that have been held have used the questionnaire as a guideline to steer the discussion, not as a rigid frame. Depending on particular situations certain topics have been discussed more deeply than others. Hence, a question-by-question documentation of the interviews is not suitable. We therefore provide summaries for the four main blocks of the questionnaire.

5.1.1 Participants

The following public sector IT service provider have been interviewed (actual company names has been replaced by placeholders):

- **DZ1** main customer is the federal state governance one of the German federal states. In provides public sector services in the domains public safety (INPOL[3]), civil status administration, financial management (salary issues and budgeting), and enterprise resource management. Moreover, it operates IP telephony and email services for the federal state administration.
- **DZ2** has been founded as a *municipal special purpose association and* provides administrative services for three administrative districts with 35 cities. Additionally, it has more than 600 customers located all over Germany. It offers more than 180 services in the application area of personal management, resident's administration and registration, passport, civil status administration, etc.
- **DZ3** is a consolidation of several data centers under the umbrella of an *agency under public law*. It acts mainly on federal state level, but has also customers on municipal level. It offers administrative services in a variety of domains, for instance financial management, resident's administration, agriculture, public safety, geodata, enterprise resource management and business intelligence, etc.

5.1.2 Document Interoperability

The first part of the interviews is aimed at determining to what degree standardized electronic data respectively document[4] formats are used, and if workflows for document management are supported. Another question is whether electronic documents are exchanged with other data centers. Both DZ1 and DZ2 use XML-based standards for data and document representation based on the XÖV framework[5] in case appropriate standards already exist. DZ3 uses several proprietary interfaces defined by the supported public sector services.

The DZ1 maintains (and provides via public sector software applications) a comprehensive electronic workflow system for document management, archiving, and exchange based on XDomea[6]. Interfaces to other processes

[3] INPOL is the information system for federal state polices in Germany.
[4] Typical documents are applications, forms, certificates and notifications. Documents can be stored either in standardized formats such as PDF or in data formats such as XML or CSV.
[5] XÖV is a framework to define XML based standards for data representation in the public sector. See http://www.bit.bund.de/BIT/DE/Standards__Methoden/XOEV/node.html?__nnn=true.
[6] XDomea is a XÖV-based format for data and document exchange within administrative workflows.

and the integration of legacy systems are supported. An example for a process where such a workflow is important is the computing and pay-out of salaries, where documents need electronically enriched by various information (from several sources): The current salary class of the employee, possible incentives and bonuses (human resource management), tax and insurance composition (staff administration), issuing of the payment and production of records.

XÖV-based data are used to integrate processes with other data centres. For instance, the XÖV standard XJustiz (for juridical documents) is employed to exchange information with the INPOL system used by the federal state polices.

Another example for data/document-driven interactions with other data centres is the generation of statistical data. Both the federal government and the federal state governments in Germany maintain statistical association to capture various information of public interest, e.g., demographic data, census data, or environmental data, etc.

An interesting case for improved interaction between citizens and government agencies has been described by the DZ1: Using a (hypothetical) Cloud storage service to archive and to manage electronic governmental documents could be used by citizens to make those documents available to public administrations.[7]

5.1.3 Services

End user services are either specific software services to support tasks for the public sector, or generic services such as email or provisioning of fat/thin clients. Since all data centres have several customers, strong emphasizes is put on the separation of services and resources assigned to each customer. This is done either by providing specific virtualized environments, or – if necessary for reasons related to data protection and security[8] – by operating separate physical servers isolated from other servers in the data centre.

Public sector software applications

A number of examples for those applications have been mentioned:

- Financial and budgeting management and accountancy
- INPOL police information system
- Enterprise resource management (with specialized configurations for each customer)
- Archiving
- Agricultural management
- Administrative software for schools and universities
- Software to manage social issues
- Electronic cadastral registers

These software applications are typically provided as three-tire applications with frontends allowing for network access (usually dedicated networks, in some cases VPNs over public Internet). The software is usually very proprietary: it has been customized for various customers (hence, for each customer a particular configuration of specific software solution is maintained). The problem of maintaining multiple configurations and versions is however well understood. DZ1 and DZ3 use SOA for integrations (e.g., for financial management, civil registration) to reduce the complexity of software management.

[7] We use this example as an inspiration for our usage scenario 2 (Section 5.2.3)
[8] For instance, this relates to the INPOL system maintained by DZ1.

Generic services

Examples are:

- IP telephony
- Office applications and email
- Networking and firewalls
- Client roll-out (mainly fat clients, with a trend to thin clients)
- Web based services such as CMS, portals.
- Consulting and software development. For instance, DZ1 has gained the status of a SAP competence center.

5.1.4 Foundational and Platform Services

Both DZ1 and DZ2 mention the use of ITIL as framework for service management. All data centres use standard methods for service management; ISO 27001 certification is either already in place of in preparation. Virtualization is generally employed (for instance, up to 85 % of the systems operated by the DZ1 are virtualized). Support services however are automated only to a certain degree: Monitoring on infrastructure level, data backup and restore, and test automation.

With the exception of the provisioning and management of infrastructure resources as a service provided between data centres, attempts to build up value chains comprising services provided by several data centres have yet not been made. In particular, there is no management approach (beyond ITIL) which supports federated service management (or even available).

5.1.5 Cooperation and Cloud Computing

DZ3 is already a merger of several public sector service providers – located in different federal states. It operates following the regulations of a state treaty between these states. In opposite to this, both DZ1 and DZ2 maintain multiple relations to other data centres and providers, mainly on service level by hosting or usage. Sharing of physical resource is usually not done. An exception is the DZ1, which provides storage and CPU power for statistical data processing and archiving. The main obstacles mentioned are legislative problems as well as economic issues – a proper business case is missing.

Employing Cloud technologies

Although private Clouds are recognized as promising first step, the positioning towards the use of Cloud Computing technologies appears to be ambivalent:

- When switching to a Cloud-technology based infrastructure, a major problem is the effort for maintaining two infrastructures (hardware, personal, management processes, etc.) during the transitional phase.
- Interoperability problems are apprehended for
  - Data and document formats,
  - Protocols between services,
  - Standards to mediate between Cloud services and Cloud infrastructure.
- The DZ1 has plans to use Cloud technologies for data and document exchange, leveraging the advantages of a homogenized technology to improve security processes, identity management and to increase the amount of automation in service management.
- A frequently found position is that Cloud Computing is what public sector data centres are already doing today (which mainly related to the Cloud aspects: Network based access, virtualization).

Community Clouds for IT Consolidation

Cloud Computing technologies can be used as an integrative platform to establish cooperation between several data centres and thus allow for consolidation, optimized usage of resources, concentration of know-how, and increased service levels.

The setup of those cooperation is however a political problem. Historically grown structures which are well established and well-functioning are very difficult to modify. Economic arguments do usually not apply, in particular if well-documented examples for a successful cooperation with massive cost savings are not (yet) available, and the transition of a cooperative model requires capital expenses, comprehensive system integration, redefinition of processes, adaptation of marketing strategies, and – last but not least – the establishment of a common way of thinking.

A concrete example is the current practice (and the underlying regulatory framework) for procurement of IT services, which is based on publishing a call for tenders. Such call for tenders are always related to a concrete budget of a particular administration: Publishing a shared call by administrations from different municipalities or federal states is not possible. Thus, the introduction of a Community Cloud as a means for IT cooperation between government agencies requires an administrative organizational framework which goes beyond the usual procurement procedures, such as the founding of an agency under public law, (e.g., a municipal special purpose organization).

Nevertheless, potentials for the creation of Community Clouds are recognized. A promising scenario is a collaboration of small and medium data centres (in particular on municipal level) to provide tailored solutions to their customers and to create a counter-weight to the competition of large data centres in the public sector market.

Public and Hybrid Clouds

Cooperation with private enterprises is assessed as very difficult: Major objections are on the strong data privacy regulations in Germany. If the processing of personal data is involved, a court of jurisdiction within the European Union is required for a service provider – some specific data protection laws on federal state level require the court of jurisdiction to be in Germany. In the most extreme case (the German federal state of Hessen), storage and processing of those data is *not allowed to take place in another federal state*.

Other restrictions have to be considered as well: As a general rule, German administrative organization cannot delegate the responsibility for the orderly and efficient execution of the core tasks they are meant to perform. This in particular means that they have to gain control over the processes of the provider to whom they outsource IT related tasks. From the current political and juridical discussions in Germany it is by no means clear whether SLAs are an appropriate instrument for that, as they only provide a result-oriented way of control. It is possible for the customer to react on the basis of the fulfilment of a contractual agreement on task execution (i.e., the “outcome”), but not proactively shape the processes which used for accomplishing those tasks (i.e., influence “the way things are done”).

Another objection relates to establishment of succession regulation and the avoidance of lock-in situations (which is not only a technical problem related to the availability of established standards): For instance, some data need to be guaranteed to be available for 120 years. Hence, the question arise how a private sector provider is able to guarantee to be available for this period of time. For public sector providers, the problem is bypassed by the fact that the German government is responsible to assume public guarantee obligation.

Open Standards and Software

The use of standards from the XÖV family has been already described in Section 5.1.2. Open source software is used, for instance Linux products for server configuration. However, those solutions have to be capable to provide appropriate service levels (which are contractual required). Hence, Open source is considered as an alternative to commercial solutions, but not esteemed as a dogma. The selection of appropriate software has to follow technical and business objectives.

5.1.6 Conclusions

We summarize the main findings of the interviews in a number of statements:

C 1. The employment of Cloud technologies is considered as important step towards the harmonization and modernisation of IT infrastructure. The main obstacles for such technological upgrades are however switching costs.

C 2. Community clouds are more difficult to achieve for a number of reasons related, e.g., to procurement regulations. In the federated political landscape of Germany a main problem is to archive a political consensus on cooperation, even if economic advantages are provable. Nevertheless, some examples (such as the maintenance of the INPOL system by the DZ1) illustrate that a model, in which provider appear as competence centres for certain specialized services, could be used to outline an implementation of a governmental community Cloud.

C 3. The use of hybrid or public Cloud infrastructure by German public administrations is challenging due to a number of arguments. It should however be noted that public-private partnerships based on concrete applications and projects is possible. A discussion of problems, restrictions and benefits based on concrete cases might help to solve many of the general problems for these cases.

C 4. Due to the switching cost argument, the migration of already implemented services into a Cloud infrastructure is unlikely to be a suitable first step. Much more promising is to establish new, innovative services to provide prove of concepts (in particular with respect to business cases and cost savings). Although, as already mentioned in bullet (C 3), many general problems and obstacles can be solved for concrete applications.

C 5. Interoperability problems are apprehended for

- Data and document formats,
- Protocols between services,
- Standards to mediate between Cloud services and Cloud infrastructure.

Standardized representation formats for data and documents (as used for input/output, exchange, or migration) are based on the XÖV standards family where appropriate.

5.2 Identification of Relevant Customer Scenarios and Use Cases

5.2.1 Overview

In this section, we are going to introduce three scenarios for using Cloud services in an eGovernment context. The scenarios aim at giving concrete examples for possible interactions between government agencies, Cloud providers, and citizens or enterprises. Table 12 provides an overview and indicates the deployment model, usage scenario categories, roles, and areas of interoperability.

Table 12: Scenario overview

Scenario	Deployment Models	Categories	Roles	Interop on	Justification from Interviews, etc.

1	**Open and Protected Data**	The scenario illustrates how data de-personalization can be used to enable private sector providers to host governmental processes.					
		Private / public	■ C2Cloud ■ G2Cloud	■ Citizen ■ Government agency ■ Governmental Cloud provider ■ Private sector provider	Data access	C 1, C 3, C 4, C 5; moreover, maintenance and publishing of open data do not belong to administrative core tasks. Therefore, control requirements are moderate.
2	**Citizen Support Service**	Electronic document safes are used as an example for Cloud services optimizing electronic workflows between administration, enterprises and citizens. The scenario can be implemented by deployment into private (governmental) Clouds, data encryption of personal information however makes is possible to use the scenario to discuss involvement of private Cloud providers as well. The scenario moreover addresses data/document interoperability.					
		Community / public	G2Cloud C2Cloud E2Cloud	■ Citizen ■ Enterprise ■ Government agency ■ Governmental public / private sector provider ■ Certification/key management provider ■ Administrative process provider	Data / documents Platform services	C2, C4, C 5. The scenario has been inspired by a similar idea explained by one of the interview partners. The optimization of electronic workflows has a high priority in Germany.
3	**Business Incubator for SMEs**	The scenario illustrates an integration of administration with business, in particular with SMEs that cannot afford to maintain an elaborated IT infrastructure by themselves.					
		Private / public	E2Cloud C2Cloud G2Cloud	■ Citizen / Cloud user ■ Enterprise ■ Government agency ■ Governmental public sector provider ■ Cloud broker ■ Cloud application developer	Processes, service composition and projection	C 1, C4, C 5. ENISA guideline on Clouds for the public sector (16), (17); goBerlin project.

The scenarios are not meant to provide examples of the employment of Cloud Computing that can be implemented already today. In fact, several elements are highly disputed in the current political discussion in Germany. As a large part of this discussion is effected by generic and general reasoning about, e.g., data privacy, and thus necessary tend to lead to negative answers, the goal is to give examples on how to analyze the obstacles, challenges, and benefits using concrete examples, and to come up with solutions for concrete problems.

Two of the scenarios will be used further in this Whitepaper:

- Scenario 1 provides the basis of the prototype implementation (see Section 6 and Appendix 8)
- Scenario 2 is used as a basis to the definition of templates for the description of use cases and usage scenarios. A prototypical methodology and a first template definition are described in Appendix 10.

5.2.2 Scenario 1: Open and Protected Data

Alice has noticed a pothole in the road right in front of her home. Remembering that the district administration has contracted a service provider (the *complaint management service provider*, CMSP) to establish a special service to register citizen complaints, she uses a special app running on her mobile to take a photo of the pothole, and – after adding some additional information (category of the problem, e.g., obstruction of traffic, GPS coordinates, some explanation) – issues a complaint. In the evening she checks at a special Web site that her complaint has been registered and transferred to the *responsible public authority (RPA)*, e.g., the road maintenance office. This Web site displays a *mashup* comprising a map augmented with various information provided by administrations, such as status information on registered complaints, planned road construction work, etc.

The administration responsible to process complaints (in our case: the road maintenance office) may use an additional IT service provider to obtain public sector software applications such as software for resource planning, logistics planning, accounting, etc.

However, after a couple of weeks, the pothole is still not fixed. Before re-issuing the complaint, she registers at the CMSP Web site with her name, email and phone number to receive status updates on the processing of her complaint (via SMS or email).

Remark

The complaint management scenario is specified in detail in Appendix 10 and implemented as a prototype showing how open data and services can be deployed and operated in a public cloud.

5.2.2.1 Related Services and Projects

- **FreedomSpeaks**[9] is a US social network which allows its member to compose letters to the officials representing them. FeedomSpeak is not maintained by a government agency, but by a private sector company.
- **Märker Brandenburg**[10] provides a complaint management for some municipalities in the federal state of Brandenburg. It is quite similar to the service described in this section. Complaints are submitted by means of a Web site. An email address can be submitted to receive information on status changes of submitted complaints.
- **Unortkataster Köln**[11]. The city of Köln maintains a complaint management service as well. Citizens are able to mark spots in the town scape as "no locations" (German: *Unorte*). Submissions are done using an interactive map. Functions for complaint tracking of receiving of notifications are not provided.
- **Wer denkt was**[12] provides a German wide complaint management service. Complaints can be submitted via an interactive map or a mobile phone application. Registration is required to issue a complaint. Notifications on status changes are provided.
- **AbgeordnetenWatch**[13] is a German service similar to FreedomSpeaks (see above). It allows citizen to contact official representatives via a Web portal. AbgeordnetenWatch enables citizens to question their members of parliament in a public environment, find out about the voting record of their members of parliament, follow up on promises made , and learn all about the extra earnings of members of parliament

[9] http://www.freedomspeaks.com/default.aspx
[10] http://maerker.brandenburg.de/lis/list.php?page=maerker
[11] http://www.unortkataster.de/
[12] http://www.mängelmelder.de/
[13] http://www.abgeordnetenwatch.de/, see http://www.abgeordnetenwatch.de/wir_ueber_uns-150-0.html#about_usb for an English reference.

These examples show that complaint management services can be provided by enterprises from the private sector as well.

5.2.2.2 Analysis

Differentiating between open and protected data

An important aspect of the scenario described above (and the related services) is that data appears in several contexts:

- Complaints of registered users contain personal data (name, email, phone number) to enable complaint tracking by these users
- In opposite to that, anonymous complaints contain no personal data.
- Complaints are transferred from the CMSP to the responsible agency (e.g., road maintenance office). This agency does not need to know the identity of the issuer of those complaints to perform its core tasks.

Hence, data protection regulations apply only if a registered user submits a complaint.

Actors and Roles

A number of roles (compare Section 4.1.3) can be identified:

- **Citizen:** The user who submits complaints (either anonymous or registered)
- **Government agency:** CMSP itself or the responsible public authority (RPA) processing of citizen complaints (i.e., the district administration). At this side, two additional roles can be identified:
  - ***Governmental service administrators*** are responsible to perform administrative tasks on the provided services such as creating new accounts for public servants, perform maintenance tasks on data bases, etc.
  - ***Public servants*** are responsible to maintain the set of stored complaints: i.e., removal of malformed or bogus complaints, maintenance of statistics, etc.
- **Governmental Cloud provider (CMSP).** The CMSP provides services to the citizen and to the RPA. Since personal citizen data are stored in relation to submitted complaints, the governmental Cloud provider is either a public sector provider based in Germany or a private sector provider with court of jurisdiction located in Europe. In any case, compliance with German privacy regulations has to be ensured.
- **Cloud provider (CMSP).** The complaints can be stored as open data in a public cloud. In the scenario they are accessed via the open OData protocol.
- **Governmental Cloud provider (RPA).** The IT provider which supports administrative procedures for the RPA. Because personal data of citizens are not processed at this site, hence, privacy regulations do apply only in relation to staff data.

Possible architecture

Figure 17 demonstrates a possible architecture of the complaint management system CMS. It comprises three “layers”: The citizen service layer consists of the interfaces available for citizens, namely the front end for registered users, the complaint management display mashup[14], a notification “lockbox”, and the mobile application for submitting complaints. The administrative service layer comprises both management and user frontend for service administrators and public servants. The backend layer utilizes Cloud technologies for providing SaaS and PaaS (for data base access). The CMS has to be part of a private Cloud (or a Community

[14] Third party providers may contribute to this mashup; this aspect is not shown here. Compare Section 5.2.4 for a scenario focusing on public private partnership based on Cloud Computing

Cloud) ensuring compliance with German data privacy regulations. In opposite to that, some services used by the RPA can run in a private or public Cloud. Open data can be hosted in a public Cloud.

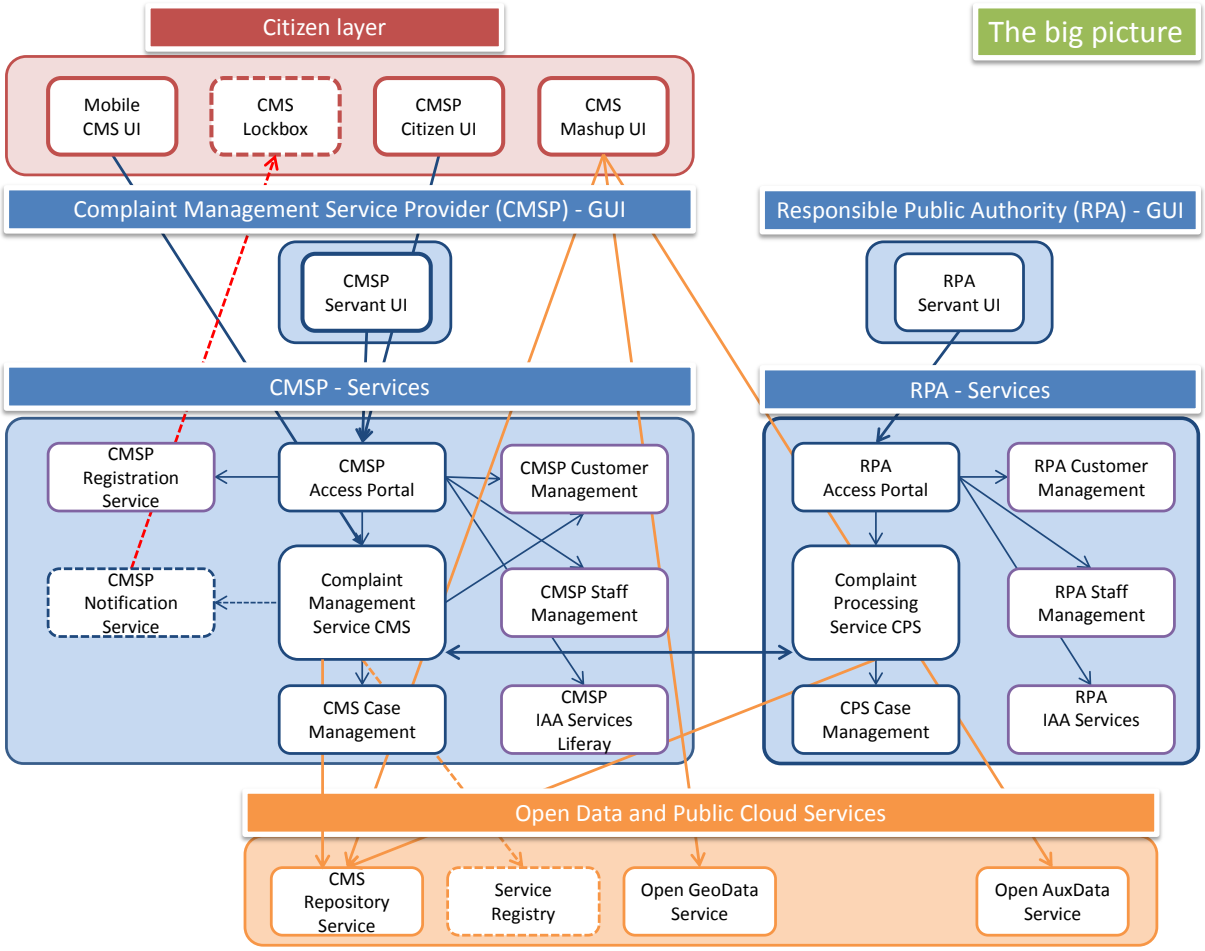


Figure 17: Complaint management system architecture.

The architecture outline emphasizes among others the need for interoperable data exchange. Both, the user front end at citizen level and the CMS mashup user interface are likely to be implemented as thin Web based clients; the mobile application uses standard communication mechanism available on the mobile phone. Hence, a protocol and format standard for data access and representation is required to ensure interoperability on service (and platform) level.

In particular, in opposite to the “write access” required to insert data into the complaint data base and the processes of the administration responsible to resolve the cause of a complaint, the display of complaint data and their statuses (and other information provided by the RPA) is qualified as open data. Therefore, protocols and access mechanisms to those data should follow established standards. For instance, a Web Service or REST based protocol like OData would be appropriate to realize the open data access as illustrated in Figure 17.

Regulatory requirements

The regulatory requirements for both governmental Cloud providers are defined by the IT Baseline Protection Catalogs of the German BSI (12) which is mandatory for data centers providing services to public administrations in Germany.

- ISO 27001 certificate or similar
- Logging of system level events

- Logging of user and administrator level
- System and software catalogs.
- Planning for discontinued operation to avoid lock-in situations (standardized data formats, frequent data base backups by third parties)

Special requirements for the Governmental Cloud provider (CMSP)

Of particular interest are regulatory requirements concerned with data privacy and protection. Since citizen register at the complaint management service provider's Web site, it can be assumed that citizens agree in processing of their personal data for the purposes described above, hence storing and processing of those data is permitted by law. However, it has to be made explicit:

- That personal data are deleted once they are no longer needed (i.e., if a complaint is processed completely).
- Personal data are not allowed to be used for purpose different to the one described in the scenario. In particular, the responsible administration is not allowed to obtain information of the person who issued a complaint. It is however possible to deliver de-personalized information (e.g., statistics) to other administrations (e.g. Federal State Offices for Statistics).
- Citizens have the possibility to receive information on personal data which are stored. Additionally, functions to correct or delete those data have to be provided (in the described scenario, these functions are provided by given citizens the means to maintain their own user accounts and associated profiles).
- Clearly, the systems used for storing and processing of personal data have to be protected against unauthorized access and secured against technical problems (e.g., backup solutions are mandatory).
- For auditing purposes, the federal state date protection official require recording of extensive information on the type of personal data which are stored and processed, on the systems used for this, on the implemented management procedures, etc.

5.2.3 Scenario 2: Citizen Support Services

Bob and Clair, proud parents for the first time, face the next challenge in their life, namely to manage applying for *parenting benefit*. In Germany, this is a fairly complex procedure citizens have to cope with; a complete description is beyond the scope of this report. For the purposes of this section it is enough to understand that a number of documents are necessary to complete the application comprising at least the following:

- Birth certificate of the child (issued by *the civil registry office*)
- Certificates of salary (prior the data of birth of the child, issued by the employer)
- Certificate of the *health insurance* on maternity benefit
- Certificate of the *employer's* contribution to the maternity benefit
- Declaration of planned working hours during acquisition of the parenting benefit (by the *parents*)
- Certificate on planned working hours (issued by the *employer*)

Fortunately, Bob and Clair own electronic document safes (EDS) to store and administrate their documents. Basically, an EDS is a secure storage for official documents. Government agencies or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedure. Access has to be granted by the owner to comply with German data protection regulation.

EDS owners access the safe using a special application providing secure encrypted communication and authentication (e.g., U-Prove based and with the German electronic identity card). Additionally, government agencies, enterprises, insurance agencies, etc. can use open interfaces to enter documents into EDS, and to

access its contents (these activities require an explicit authorization by the EDS owner). Recently, a new version of the EDS has been made available with offers additional process support: EDS owners can deploy process descriptions of administrative procedure into the EDS which steer the execution of this procedure. For instance, Clair uses a parental benefit application template to identify and request the necessary documents and to assign dedicated permissions to the district administration (which in Germany is responsible to process parental benefit applications) to access these documents. Process description can be downloaded as trustworthy, certificated objects from a process provider Web site.

Clair did a bit of background checking to learn about the EDS provider, and to understand the security issues related to electronic storage of documents. It turns out that the EDS provider is organized as a collaboration of several small data centers on municipal level with dedicated resources. They use Cloud Computing technology to manage those resources, i.e., they maintain a community cloud. Hence, as particular data stored in the EDS are encrypted, the EDS provider does not know what data actually are stored in a particular EDS.

Remark

The EDS scenario has been selected as an example on how to apply the templates for usage scenarios and use case descriptions proposed in Appendix 10.

5.2.3.1 Related Services and Projects

- **BSI recommendation TR-ESOR (TR-03125)** (19). The TR-ESOR recommendation of the BSI addresses the long-term storage of electronically signed documents. It described how this can be achieved in a trustworthy, regulatory compliant way. It defines a functional middleware to ensure accessibility and readability, integrity, authenticity, protection and security of those documents. It moreover provides references to national and international standards for document representation and organization, such as XÖV (see below), SAGA, OASIS, etc.
- **XÖV** refers to a family of national standards for the exchange of electronic documents between administrations, for example XDomea. Its purpose is to enable integrated business processes in the German public sector.
- **Fraunhofer eSafe** (20). The Fraunhofer institute FOKUS has developed a version of the EDC called eSafe. This concept shares with the EDC as describe above the idea that documents can be stored in a trustworthy, secure way within a Cloud infrastructure. It moreover describes a mechanism to fragment and distribute such documents among several storage providers, making it very difficult for an unauthorized person to retrieve the original document. The eSafe however does not address document exchange between administrations and the associated process management described in the scenario.
- **Fresco project**. The German Federal Ministry of the Interior has initiated a high priority program for the optimization of electronic processes between enterprises and public authorities[15]. Fraunhofer FOKUS has published an associated concept study in late 2009 (17) together with partners from industry and research organizations. An implementation and pilot project has started in 2010. The core component of the architecture is the “flexible, rule-based, easy, and secure communication processor” FRESKO that provides trusted storage for confidential data of the enterprise and its employees. FRESKO executes workflows that automatically aggregate and distribute these data considering the enterprise’s legal obligations. The FRESKO-concept will be extended towards the optimization of processes between public authorities in the future.

[15] Bundesministerium für Wirtschaft und Technologie; Fünfter Nationaler IT-Gipfel: Programm – Personen – Projekte; Dresden, Dezember 2010

- **De-Mail** refers to the exchange of documents via the Internet between citizens, enterprises, and administrations based on mutual authentication and end-to-end encryption. De-Mail is realized as a centralized service. Providers have to be accredited by the BSI.

5.2.3.2 Analysis

Secure long-term storage of electronic documents

In principle, a private sector company could adopt the role of an EDC provider as well: Since data in the EDS are encrypted and thus not visible to the provider, the "data protection barrier" can be considered as comparable to "low": In fact, there is a vivid discussion ongoing between German legal experts whether data encryption is as qualified as data anonymization. Hence, this white paper discusses the hypothetical scenario of an EDS services to analyze the requirements of storing personal data in public cloud infrastructures, and using those data to interact with public sector authorities. Significantly, when owning an EDS, citizens can approve that personal data are stored and processed electronically. Hence, data privacy applies only insofar as citizens have to trust the EDS provider.

On the other hand, if an EDS is interpreted as a technical mean to support administrative processes, governmental public guarantee obligations apply: Government agencies are responsible to ensure the continuous availability of this service (up to 120 years for certain types of documents). Hence, the question arise how a private sector provider is capable to give sufficient guarantees on its own continued existence, future business orientation, etc. A possible solution is to maintain a governmental Cloud provider as "fall back", while allowing public sector providers to participate on the emerging market of electronic document storage. Of course, interoperability to operate EDS like system is mandatory between private and public sector platforms.

The usage scenario provides an example of a citizen support service offered by a public sector Cloud provider. Other usage scenarios (beyond the "German" border) are possible, for instance: moving from one EU member state to another. Since documents in the EDS are still controlled by its owner, the integration into administrative procedures does not depend on data transfers between administrations of different member states but is based on the establishment of appropriate process description within the EDS. Other examples comprise the registration of a business within the European economic region.

Roles

The following roles can be identified:

- **Citizen**. The person who "owns" the documents in the EDS. Since the EDS is intended to provide trustworthy long-term storage of personal documents, sufficient data security and data protection is crucial.
- **Enterprise**. An enterprise who owns an EDS. This EDS may contain sensitive data as well as personal data (e.g., of customers or employees), hence data protection issues need to be taken into account.
- **Government agency**. An administration which requires access to an EDS either for accessing or delivering a document. Both operations require the explicit authorization of the safe owner.
  As before, we can distinguish between governmental users (officials in charge) and administrators**.**
- **Governmental Cloud provider.** The provider of a governmental EDS service. This Cloud is organized as private or community Cloud.
- **Public sector provider.** The provider of a public sector EDS service. This Cloud is organized as private or public Cloud.

A number of additional roles can be identified which are specific to the EDS usage scenario:

- **Certification and key management providers.** More complex role structures can be designed if the trust relationship between document owner and EDS provider (and other parties such administrations) is analyzed in more detail. For instance, by employing a third party for the management of encryption keys for encrypting personal documents the assumption that the owner trusts the EDS provider can be dropped.
- **Administration process provider.** As discussed above, the EDS also provides process support, i.e., it actively requests documents from administration on behalf of its owner and delivers them in a certain, process specific order. The descriptions of such processes (e.g., as data objects or software modules) are maintained by a hypothetical administration process provider.

Architecture

Figure 18 illustrates a possible architecture for the EDS. Its main component is the EDS storage, i.e., a Cloud based infrastructure providing storage, access, and management functions for EDS. Each EDS comprises a tenant storage containing the documents of the EDS user, and several components to handle access, authorization, and usage of the EDS.

- Input (I) and output (O) provide storage for documents which require owner authorization to enter/leave the EDS.
- A process engine (P) coordinates the actual usage of documents in the EDS. The process engine therefore implements an administration process driven by a citizen (or enterprise). It describes which administration has to deliver or access which document in the EDS, and in which order, to realize a certain administration workflow.

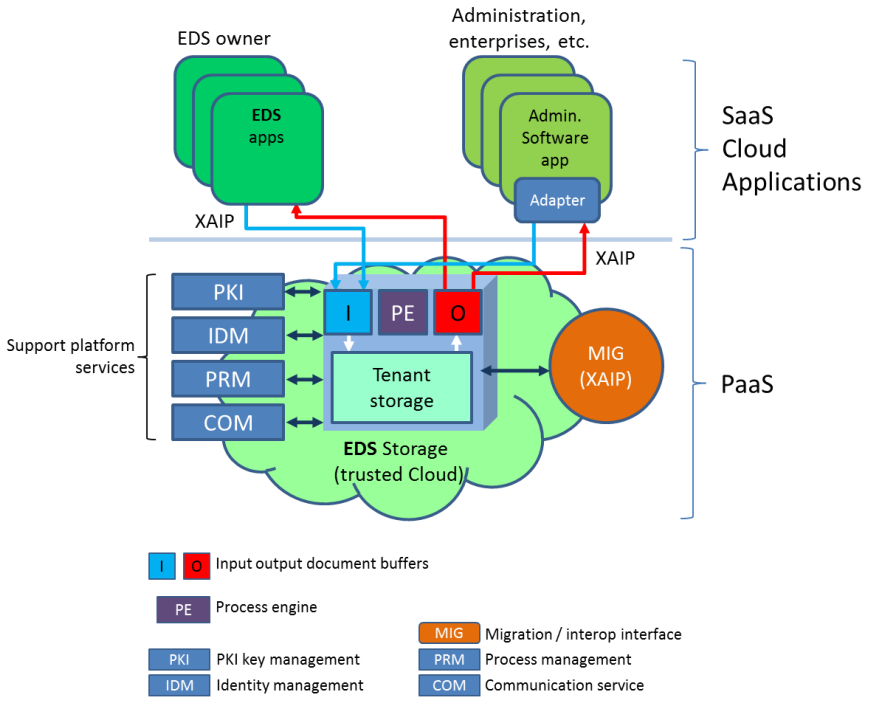


Figure 18: EDS principle architecture

A number of additional components are required:

- Key management for encryption of documents and communication channels.
- Identity management for access, authentication and authorization.
- A process management to embed the EDS as a software service in a Cloud infrastructure.
- A communication service providing secure and reliable transfer of electronic documents.

Access to the EDS is provided by two mechanisms:

- An EDS app allows the EDS owner to access the contents of his/her safe, to organize it, and to delete if required. In a simple form, such an app provides simple browser, file management and access right management functionalities.
- Enterprises and administration which generate documents and access them via specific software applications access the EDS by means of a specific adapter layer.
- In the German context, a possible document representation format would be the XAIP format[16] which is described in the technical guideline TR-03125 (19) of the BSI.

Finally, in order to design a case for public private partnership, it becomes crucial that means are available to transfer documents in the tenant storage between providers: EDS owners cannot rely on the continued availability and sufficient service level of a private enterprise; therefore, a migration interface (MIG) have to be available to transfer the contents of the EDS from one provider (and EDS implementation) to another: of course, the transfer syntax need to follow accepted and established data representation standards. A prototypical protocol (based on the technical guideline TR-03125 of the BSI) is outlined in Appendix 10.3.2.3).

Regulatory requirements

Since citizens agree on the storage of personal data in the EDS, data privacy regulations do not directly apply in this case. However, an EDS provider has to be trustworthy. Therefore, following German regulations concerning data security and privacy (e.g., by implementing the measures proposed by the BSI basic data protection guidelines and obtaining an ISO 27001 certification) have to be considered as necessary steps to gain market acceptance.

Since documents stored in the EDS provide evidence about the citizen, electronic signatures and certification is required. Hence, a number of additional regulations have to be taken into account. The most important ones are:

- German Signature Law
- European Signature Directive

5.2.4 Scenario 3: Business Incubator for SMEs

Donald owns a movers company in the Berlin area. Ellen heads a construction firm. Fred works as free-lancing paver. Grit is an accommodation broker. All these small enterprises cater a common market, namely supporting people moving house from one place to another. Administrative procedures are part of the picture as well: German citizens need to register their address of residence at the registration office.

An open market place aims at integrating administrative procedures and services offered by private sector companies, in particular SMEs without the capability to maintain an elaborated IT infrastructure. By participating in the market place, these companies can provide appropriate offers to concrete situations and specific types of customers. On the other hand, activities such as moving, building a house, finding a suitable playschool in the new environment, etc., can be comprehensively managed.

5.2.4.1 Related services and projects

- The **goBerlin** project has recently been accepted for founding by the German government as part of the Trusted Cloud initiative. It aims at providing a Cloud based business/public sector process integration platform as described in the scenario.

[16] Compare http://www.cdc.informatik.tu-darmstadt.de/~wiesmaie/publications/HKLW09_TRarch_extended.pdf

- The **ENISA guideline** "Security & Resilience in Governmental Clouds"[17] describes a scenario based on the **J-SaaS model**[18]. J-SaaS is a Web based SaaS infrastructure which aims at providing software services at low cost to SMEs. However, the scenario does not involve the integration with administration services.
- The advertisement and integration of business offers is the main focus of the **THESEUS/TEXO**[19] project. TEXO aims at the development of a Web service based market place which allows in particular SMEs the participation in a world-wide market, thus creating a new, Internet based economy.
- The **Logistics Mall**[20] is a project of the Fraunhofer-Innovationscluster „Cloud Computing für die Logistik". The idea is to provide a Cloud based platform to compose and orchestrate logistic processes, including software as well as physical resources (warehouses, transport, etc.).
- **PEPPOL** (Pan-European Public Procurement Online)[21] aims at implementing common standards to enable EU-wide public eProcurement. Existing national systems of electronic public procurement will be linked so that all participants can enjoy the full benefits of a single European market. PEPPOL is operated under the European Commission's Competitiveness and Innovation Framework Programme's ICT Policy Support Programme.

5.2.4.2 Analysis

The business incubator scenario is an example for integrating administrative procedures and associated businesses. Therefore, two levels need to be considered:

- Administrative processes deal with personal data. Hence, a private or community Cloud maintained by public sector providers is an appropriate model.
- Business integration requires no special consideration of data privacy regulations; in fact providing a portal for business registration with associated integration services is a valid business case for a public Cloud provider.

That's why we concentrate on a hybrid Cloud deployment model when discussing this usage scenario.

Roles

The roles that can be identified for this scenario are as follows:

- **Citizen / Cloud user**. The citizen role appears in two flavors: As an end user of governmental services and as user of services provided by public sector third party providers.
- **Enterprise**. A commercial organization (e.g., an SME) which uses the market place to integrate its business processes into appropriate governmental processes.
- **Government agency**. The administration executing the public sector processes in question and providing information and integration of the business processes of enterprises.
- **Governmental Cloud provider (public sector)**. As already explained, the core governmental processes (such as citizen registration) cannot be outsourced into private sector Cloud infrastructures. The usage of private or community Cloud models however is possible.
- **Cloud broker.** The provider of the market place infrastructure appears in the role of a Cloud service broker, since it does not provide only an infrastructure, but negotiates access to public sector Cloud resources (i.e., access and integration to governmental services) as well. It should be noted that the Cloud broker needs to

[17] http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport
[18] http://www.fujitsu.com/global/news/pr/archives/month/2010/20100601-01.html
[19] http://www.theseus-programm.de/en-us/theseus-application-scenarios/texo/default.aspx
[20] https://mmp.logistics-mall.com/web/guest/purchase
[21] http://www.peppol.eu/

maintain a tight interworking with the government agency. Since governmental processes are involved, government agencies are obliged to ensure a certain level of security, data protection and privacy, and availability.

- **Cloud application developer**. Finally, an actor who has not been discussed so far is the Cloud application developer who provides specific user applications which allow citizens to access and employ the combined governmental/business processes.

Architecture

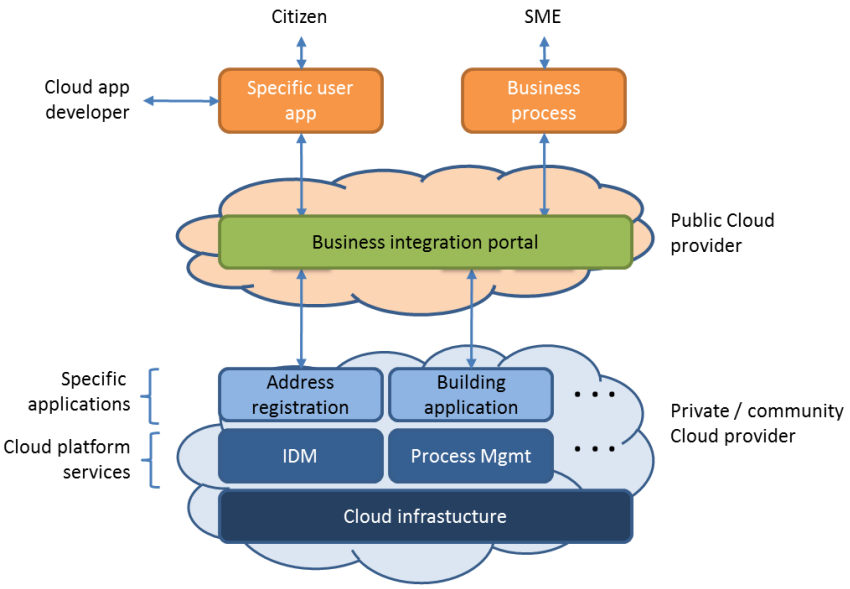


Figure 19: Business incubator set-up as a hybrid Cloud

Interoperability

Of particular interest in this scenario is the interworking between business processes of SMEs, public sector services, and end user (citizen) services. We concentrate on the analysis of the live cycle (using the DMTF model as explained in Section 2.2). We find that the emergence of citizen (end user) services can be explained by the combination of three live cycle chains as outlined in Figure 20. The left hand side chain describes the states that the governmental service assumes (the first three stages of the model are compressed into one stage for the sake of simplicity). Business processes of the SMEs who used the integration service provided by the market place are depicted in the middle block, while the actual end user (citizen) service is shown at the right hand side.

The integration of governmental services and SME business processes (functional description, service level parameters, accounting and billing parameters) rests upon the composition of several processes. On the other hand, the definition of the end user service requires to identify and to expose certain aspects of the composed process to the end user – we refer to this step as “projection”.

Obviously, the adoption of SOA principles is a key requisite to implement the open market place scenario. A detailed modeling of the required components, description and integration mechanisms is beyond the scope of this white paper.

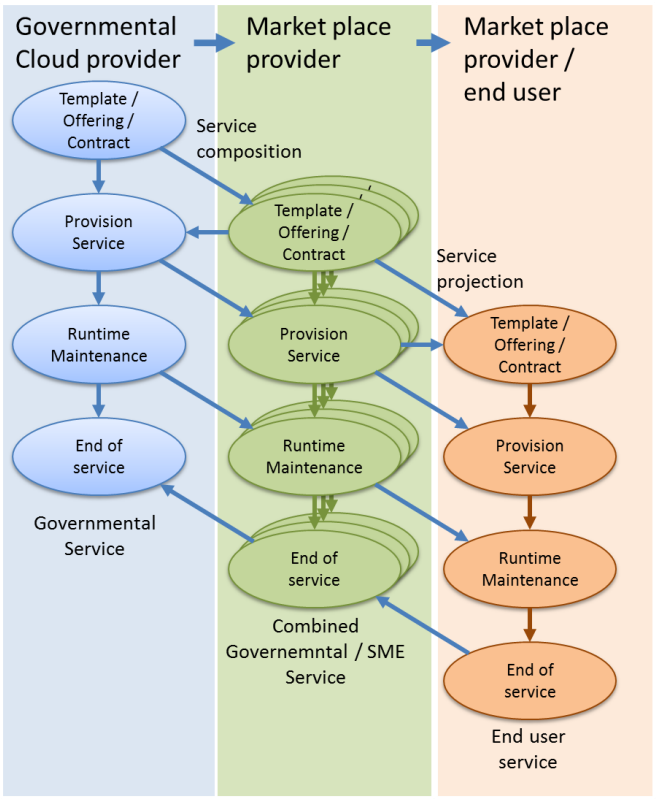


Figure 20: Superposition of service life cycles

5.2.5 Conclusions

In this section, three usage scenarios for Cloud Computing in the German public sector have been described and analyzed. The choice and concrete definition of the scenarios has been inspired and steered by a number of sources, in particular three interviews performed with members of governmental data centers in Germany.

- Scenario 1 illustrates how data privacy issues can be resolved by separating between personal and non-personal (open) data. Governmental processes which do not rely on personal data can be hosted in public Cloud infrastructures.
- Scenario 2 shows how a Cloud service providing a secure document storage can simplify the interaction between administrations, enterprises, and citizens, optimize governmental processes by delivering documents in a timely manner, and enable cross-administration processes by the electronic exchange of documents.
- Scenario 3 outlines the idea of interconnecting governmental processes and enterprise business processes (e.g., SMEs) to provide a business incubator for those enterprises. The scenario imposes interesting questions on a collaborative lifecycle management between the several actors.

The main conclusions of this work are:

C 1. When discussing the involvement of Cloud Computing in the German public sector, concrete scenarios are necessary to avoid generic “killer arguments” and to analyze problems in a given context, where a solution becomes possible. Therefore, the examples described in this section are not undisputable and they do not intend to be.

C 2. The obvious next step is to turn (at least) one of these scenarios into a living pilot. In the context of this project, a prototype implementation of the first scenario is under development. Compare Section 6 for an overview and Appendix 9 for a more detailed specification.

C 3. The usage scenarios provide a context for the discussion of concrete use cases, which in turn lead to the identification of standardization requirements. How this can be done in a formalized way is illustrated in the Appendix 10.

6 Overview on the Demonstration Scenario

6.1 Objectives

The prototype implementation aims on demonstrating a number of objectives including the following:

1. The scenario demonstrates interoperability between
    - Legacy systems and services in the cloud
    - Services operated by different Cloud providers
2. User management compliant to German data privacy regulations
3. Migration of Cloud services between different Clouds
4. Storage of open data in a public Cloud and access via open protocols
5. Usage of Hybrid Clouds (open data and confidential data) in the public sector.

The selected demonstration scenario has been shown at the German fair CeBIT in early March 2011. It will be expanded towards a demonstration on Cloud interoperability between different public sector agencies. Its main goal is to show the usage of cloud services between public administrations, to justify privacy protection by using a private Cloud, and to demonstrate the seamless usage of a public Cloud. Furthermore, another aspect will be considered, that is the interoperability between different technologies. The expanded scenario is an instantiation of the Cloud usage scenario 1: Open and Protected Data (Section 5.2.2).

6.2 Overview

The Government service scenario which is going to be realized is depicted in Figure 21.

In the scenario, citizens can report any problem in their environment using location aware mobile devices. A Citizen takes a photo of a significant problem, selects a category for the problem (e.g., road construction or garbage collection) and optionally adds a more detailed description. The application running on the mobile device adds geographic information and sends the complaint composed from these data to a complaint management service.

The complaints are collected within a private Cloud maintained by the complaint management service provider (CMSP). In the demonstration scenario, the architecture comprises in particular components for a case management and a user management, which need to be kept in a closed infrastructure due to German data privacy regulations. Additional information (e.g. photos, complaint descriptions, etc.) count as non-personal information and can be stored in a public Cloud. Moreover, processes related to the public administration that is responsible to deal with the reported problem (called the responsible public authority – RPA) can use the public cloud infrastructures to get the details on the reported problems or complaints as there is no personal data involved in that process.

The CMSP provides an open interface which allows accessing the non-personal aspects of complaint reports. They are visualized together with pictures and statistics about similar or other problems in the same region.

From a “Mashup point of view” open data, provided by public authorities and information from several open APIs such as Google Map, Charts, and Geocoding are merged together to provide a graphic representation of the existing “concerns”.

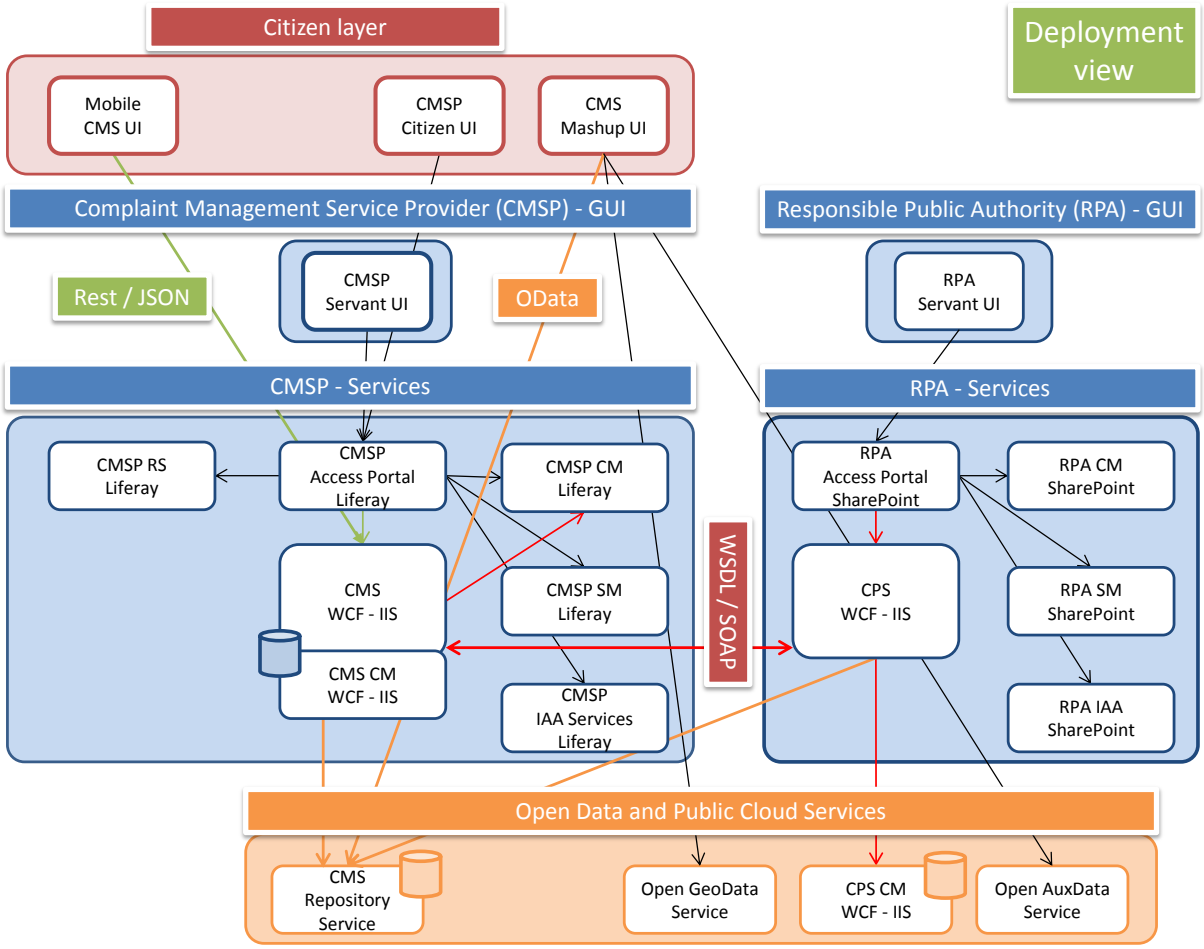


Figure 21: Complaint Management deployment architecture

Restricted access to the Complaint Processing Service CPS of other public authorities is possible and governed by access control and authorization rules.

From a "Cloud point of view" different public authorities may use either a local case management (CM) to administer the complaints or they may use a CM service in the private Cloud or they may use a multitenant CM service.

Appendix 9 of this document contains a details specification of the software architecture. It also explains how this architecture is related to components and services already available in the German public sector.

6.3 Roles and Functions

The following Table 13 summarizes the functions provided by the several user interfaces which appear as components in the scenario, and the roles of human actors associated with them.

Table 13: Roles and associated functions for the complaint management service scenario

Layer	Interface	Role	Function
Citizen layer	Citizen UI	Registered citizen	■ Register ■ Login ■ Edit profile ○ Select notification mode ■ Display/filter complaints ■ Issue complaint
	Mashup UI	Registered or anonymous citizen	■ Display/filter complaints
	Mobile UI	Anonymous citizen	■ Issue complaint
		Registered citizen	■ Issue complaint
Government servant layer	CMSP GUI	Administrator	■ Login ■ Add/remove CMP staff accounts
		Servant	■ Login ■ Remove citizen account ■ Display/filter complaints ■ Edit complaint ■ Forward complaint ■ Remove complaint
	RPA GUI	Administrator	■ Login ■ Add/remove RPA staff accounts
		Servant	■ Login ■ Change complaint status ■ Display/filter complaints

7 Summary, Conclusions, and Further Work

7.1 Summary

7.1.1 Use Case Analysis

The first part of the compendium concentrates on Cloud Computing definitions and technical use cases, such as those provided by the *National Institute of Standards and Technology* (NIST) and the additions by *Microsoft*, the *Distributed Management Taskforce* (DMTF) and the *Cloud Computing Use Case Discussion Group* (CCUCDG).

The NIST definitions of Cloud Computing are the most agreed and cited definitions that currently exist. They present the most common agreement for the term "Cloud Computing" and are used as a *starting* point for most discussions. Following NIST, Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort. It aims for automatic adaptation of the Cloud infrastructure to the dynamic requirements of hosted software components. The NIST Cloud model introduces five essential *characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service)*, three *service models (infrastructure, platform, and software as a service)*, and four *deployment models (private, public, community, and hybrid Cloud)*.

The *Open Cloud Standards Incubator* of the DMTF has published three White Papers about Cloud Computing focussing on *Cloud Interoperability*, *Cloud Architecture and Management*, and *Use Cases for Cloud Management,* respectively. These use cases are defined alongside the lifecycle of Cloud services. DMTF introduces six states for the lifecycle of a typical Cloud service together with those use cases that are most relevant to each state. Moreover, these white papers distinguish in the description of their use cases between business and operations related actors, i.e. Cloud service providers and Cloud service customers. For this reason it is straight forward to map these use cases to eGovernment scenarios between data centres supporting different public authorities and use cases between public authorities, enterprises and citizens.

NIST itself has introduced twenty-four use cases that are categorized into four different groups: management use cases, interoperability use cases, security use cases and future use cases. Management use cases focus on business relationships between Cloud service providers and customers, and on the management of data and virtual machines. Interoperability use cases focus on Cloud burst scenarios considering the migration of data, applications and VMs between different Cloud providers. Security scenarios tackle issues such as federated identities, authentication, authorization, monitoring, and shared access.

Of special importance for the German public sector are interoperability and security related use cases considering data protection and access related issues. As for the DMTF use cases, the NIST actors, *Cloud service provider*, *customer*, and *user* can be easily mapped to corresponding eGovernment actors. Using this mapping we have introduced additional supporting actors such as *data protection authorities* and *eIdentity providers* that are relevant in the German context.

Finally, the *Cloud Computing Use Case Discussion Group* (CCUCDG) discusses a set of usage and customer scenarios. Usage scenarios describe different configurations of deployment models such as *End User to Cloud*, *Enterprise to Cloud to End User*, *Enterprise to Cloud*, *Enterprise to Cloud to Enterprise*, *Private Cloud*, *Changing Cloud Vendors*, and *Hybrid Cloud*. Customer scenarios are real life examples like *Payroll Processing*, *Logistics & Project Management*, *Central Government Service in the Cloud*, *Local Government Services in a hybrid Cloud*, and *Astronomic Data Processing*. These scenarios can be compared with the example scenarios introduced by

the *European Network and Information Security Agency (ENISA)*: *Healthcare Cloud*, *Cloud Infrastructure for Local and Regional Authorities*, and *Governmental Cloud as a Business Incubator*.

The definition of a *Cloud taxonomy* helps to obtain a common understanding of Clouds and to motivate the selection of important use cases and scenarios. Our taxonomy extends the definition provided by OpenCrowd that focuses mainly on a categorization of Cloud services.

Hence, the use cases considered can be divided into *usage scenarios* and technical *use cases*. Abstract *usage scenarios* can be instantiated by real life *customer scenarios* such as those introduced by CCUCDG or ENISA. *Technical use cases* can be subdivided in *life-cycle* related use cases as introduced by DMTF and *management*, *security* and *interoperability* related use cases as introduced by NIST. Customer scenarios and technical use cases can be considered as orthogonal. The implementation of any customer scenario requires the consideration of a subset of corresponding technical use cases. To identify the technical use cases and associated customer scenarios that are relevant to the German public sector additional aspects have to be considered in the taxonomy:

- The *deployment model* (private, public, hybrid, community) might be restricted depending on the public sector usage scenario.
- The *role model, as a* result of the analysed use cases, has to be extended to capture the specific relations between administrations, enterprises, and citizens.
- The traditional *service models* (IaaS, PaaS, SaaS) need to be aligned with future service models, such as Data-aaS, Process-aaS, and Knowledge-aaS, to help categorizing usage scenarios as well as technical use cases.
- Specific *business models* such as G2Cloud, G2Cloud2C, G2Cloud2G, G2Cloud2E (G: government, C: citizen, E: enterprise) can be used to refine the usage scenarios considering the eGovernment specific actors.
- The roles of the external *supporting actors,* such as eIdentity providers that can be derived from the technical use cases have to be considered.
- Additional *non-functional properties* of Cloud services such as availability, performance, resilience, accounting and billing, together with SLA/SLO policies have to be well thought-out.

7.1.2 Interviews

To evaluate the applicability of Cloud Computing in the German public sector and to suggest a roadmap for the introduction of Cloud Computing, a number of interviews have been conducted with leading personal of governmental data centres at both municipal and federal state level. During the evaluation of the interviews it became clear that scenarios for the introduction of Cloud Computing for the German public sector have to follow the subsequent statements:

- The employment of Cloud technologies is considered as an important step towards the harmonization and modernisation of the IT infrastructure.
- Community clouds are more difficult to achieve for a number of reasons related, e.g., to procurement regulations, and will require the establishment of an accompanied governmental organization, e.g., an agency under public law or a municipal special purpose association. Nevertheless, some examples illustrate that a model, in which providers appear as competence centres for certain specialized services, could be used to outline an implementation of a governmental Cloud composed of community Clouds.
- The use of hybrid or public Cloud infrastructure by German public administrations is more challenging due to a number of arguments. A discussion of problems, restrictions and benefits based on concrete cases might help to solve many of the general problems for these cases.
- A main objection against modernisation relates the investments required for the transition to new technologies. Hence, instead of migrating established systems and services into the Cloud, a more

promising migration path leading to the introduction of Cloud Computing to the German public sector consists of the definition new, innovative services to provide prove of concepts.

- Standardized representation format for data and documents (as used for input/output, exchange, or migration) are based on the XÖV standards family.

7.1.3 Scenario Synthesis

When discussing the introduction of Cloud Computing in the German public sector using concrete scenarios are a suitable means to avoid generic "killer arguments". It further helps to analyze problems in a given context and to provide possibilities for suitable solutions. The examples described herein are arbitrary and do not claim for completeness.

The following three categories of customer scenarios have been identified as typical scenarios for the German public sector. A prototypical implementation of the first scenario utilizing *Microsoft System Centre 2012* (11) for the implementation of a private Cloud and Microsoft Azure as a public Cloud is under development. Supplementing scenarios have been identified in the *Trusted Cloud Initiative* that has been initiated by the German Ministry of Economics and Technology. The corresponding projects will start in the second half of this year (2011).

7.1.3.1 Open and Protected Data

Applications like the US 311 service, the German complaint management services "Mängelmelder", and "Märker Brandenburg" allow citizens to submit complaints about issues like broken traffic lights, road damages or others in municipalities by electronic means. The complaints are assembled and forwarded to the responsible public authority. A corresponding customer scenario consists of public data about complaints, private/protected data about the issuer, and the status of the associated complaint. An important aspect of this scenario is that data appears in several contexts:

- Complaints of registered users contain personal data such as name, email, and phone number to enable personalized complaint tracking and notifications;
- Anonymous complaints that do not contain personal data;
- Complaints that are transferred to the responsible public authorities. This administration does not need to know the personal data of the issuer to perform its core tasks.

Hence, data protection regulations apply only if a registered user submits a complaint. The architecture emphasizes the need for interoperable data exchange. Both, the user front end for citizen and the public complaint display are likely to be implemented as thin Web based clients; mobile applications used to submit the complaints use standard communication mechanism available on the mobile phone. Consequently, an open protocol and format standard for data access and representation ensures interoperability at service and platform level. The prototype uses the *Open Data Protocol* Odata for this purpose.

The regulatory requirements for the public authorities involved in this scenario are defined by the *IT Baseline Protection Catalogues* of the German BSI. They comprise aspects like ISO 27001 certificates or similar, logging of system level events, logging of user and administrator level, system and software catalogues, and planning for discontinued operation to avoid lock-in situations.

The scenario comprises several public authorities providing complaint related services as SaaS. The complaint storage service is implemented in a public Cloud accessible via OData, most administrative service are implemented as SaaS in private governmental Clouds with the exception of a case management services deployed as SaaS in a public Cloud.

7.1.3.2 Citizen/Enterprise Support Services

Citizen and enterprise support services can be built around the concepts of an intelligent *electronic locker* or *data safe* that is on a first view a secure storage for sensitive documents. Public authorities or other parties such as employers can access the safe to enter documents such as official notifications, salary certificates, rental contracts, and insurance policies for the owner. They can access those documents if necessary to perform an administrative procedure. Access has to be granted by the owner to comply with German data protection regulation.

An owner can access the safe using a special application interface providing secure encrypted communication and save authentication. Moreover, a safe may support mechanisms to actively request documents, e.g. via administrative workflows that can be stored and executed in the safe itself. Workflow descriptions can be downloaded as trustworthy, certificated objects from a process provider Web site. Similar concepts between enterprises, citizens and public authorities are currently under development in Germany but without considering the utilization of Cloud technology.

This usage scenario provides an example of a citizen support service offered by a public sector Cloud provider that operates the safe. Other usage scenarios (beyond the “German” border) are possible, for instance: moving from one EU member state to another. Since documents in the safe are still controlled by its owner, the integration into administrative procedures does not depend on data transfers between administrations of different member states but is based on the establishment of appropriate process descriptions within the safe.

7.1.3.3 Business Incubator for SMEs

An open market place aims at integrating administrative procedures and services offered by private sector companies, in particular small and medium enterprises (SMEs) without the capability to maintain an elaborated IT infrastructure. By participating in the market place, these companies can formulate offers more appropriate to concrete situations, and specific types of customers. On the other hand, activities such as moving, building a house, finding the right playschool, etc., can be comprehensively managed utilizing the provided services. The business incubator scenario is an example for integrating administrative procedures and associated businesses. Therefore, two levels need to be considered:

- Administrative processes deal with personal data. Hence, a private or community Cloud maintained by public sector providers is an appropriate model.
- Business integration requires no special consideration of data privacy regulations; in fact providing a portal for business registration with associated integration services is a valid business case for a public Cloud provider.

7.2 Conclusion

The definition and analysis of use cases and scenarios provides a suitable methodology to understand the opportunities and challenges of the introduction of new technologies accompanied business models. They do not only enable capture technical requirements and to identify promising application domains, but also are useful to determine legal and organisational limitations. This is of major importance if Cloud Computing is concerned: Cloud Computing is a global technology in the sense that the storage and processing of customer data cannot necessarily be localized within a pre-determined data centre. Hence, a possibly large variety of legal, political, societal, and organisational constraints and particularities need to be taken into account, which can only be understood on the bases of dedicated cases and scenarios.

The benefits of a use cased based methodology has been acknowledged also within standardisation bodies such as the JTC 1 / SC 38 of ISO. The Study Group on Cloud Computing (SGCC) has adopted such an approach to identify work items for a possible working group on Cloud Computing. Parts of this document will be provided as material supporting these activities (Appendix 10 has already been submitted as expert input to the SGCC).

The use cases analysed in the first part of this compendium concentrate on technical aspects of Cloud Computing, and are therefore suitable to understand technical standardization requirements. One conclusion which can be drawn from the interviews with public sector IT service providers is that decisions on the introduction of new technologies in the public sector are always taken against the background of the legal and political context. Control requirements, data privacy and protection guarantees, and administrative principles such as the existence of a concrete purpose for data collection are more important than efficiency and cost reductions. Hence, use cases need to be accompanied by usage scenarios which do not only identify meaningful application areas but provide necessary contexts by means of concrete examples.

However, administrations not only in Germany are facing reduced IT budgets and a lack of qualified personal. Therefore, after all, cost reductions, efficient work organisation, consolidation of technical and personal resources, etc. need to be considered. Cloud Computing is currently understood as one possible way to cope with these problems. The public sector requires suitable migration strategies to employ Cloud Computing as means for data centre modernisation and consolidation. Moreover, private sector companies possess resources and capabilities which provide enormous potentials for the public sector as well. Therefore, migration strategies towards Cloud based IT cooperation between public sector entities and between public and private sector need to be defined.

This document provides a number of examples of the prototypical application of Cloud Computing concepts to achieve such cooperation. Following a similar agenda, the German government has founded a number of projects within the so-called “Trusted Cloud” initiative[22] to explore the applicability of Cloud Computing as a technological platform to provide secure and trusted IT resources and services to administrations as well as to small and medium businesses (which are usually seen as one of the backbones of the German economic structure).

Hence, the following recommendations for future activities can be derived:

- Standardization of technical aspects employing a use case based methodology, which need to be accompanied to the analysis of legal and organizational aspects. Usage scenarios are a suitable means to provide this context.
- The suitability and feasibility of a certain migration path towards a specific application of Cloud Computing has to be motivated by means of concrete demonstrators using existing technologies, providing and immediate experience of the underlying concepts.
- Finally, instead of migrating existing (and functionally sound) applications into the Cloud, a more promising way to demonstrate the benefits of Cloud Computing is to start with novel, innovative applications to demonstrate that certain services can be provided using Cloud Computing in a better, secure, and cost efficient way.

7.3 Future Work

The work presented in this paper provides a solid ground for future activities. A paper providing a summary of this white paper has already been accepted for the eChallenge 2011 conference

[22] http://www.bmwi.de/BMWi/Navigation/Ministerium/Projekte-und-Wettbewerbe/trusted-cloud.html

(http://www.echallenges.org/e2011/default.asp). It is planned to present the results of this work on several workshops to the public. Negotiations to arrange such workshop are on the way.

In several standardization organisations, in particular the SC 38/JTC 1 of the ISO, a vivid discussion on use cases is on-going. We already provided the usage scenario and use case templates as expert input to the Study Group on Cloud Computing (SGCC).

8 Appendix: Questionnaire

The questionnaire has been developed to structure proposed interviews with providers of government services. The interview partners got only the questions, but not the text describing the underlying assumptions and goals at the beginning of each section of the questionnaire. The questionnaire has been iteratively refined during the interview phase. We present here its latest stage.

The following core assumptions have been made:

1. Electronic interaction and communication between government agencies is achieved by the exchange of **data** in the **format of documents**. At least in Germany, several (XML-based) standards exist which would allow shifting to an electronic exchange; these standards are based on legal requirements.
2. Processes are either provided to "end-users" (i.e., actual eGovernment applications, networks, platforms, etc., used by administrations or citizens), or can support the internal operation of a data centre (e.g., backup & restore, event management, etc.). We refer to this class of services as "foundational". Many of these functions are generic in nature and thus can be capsulated and provided e.g. as Cloud services. Thus "stitching" together a virtual data centre out of the Cloud is possible and provides a "Cloud broker" business case and scenario.
3. A main problem is that data centres usually do not share resources, thus we cannot ask directly for process or data interoperability.

8.1 General Questions

***Assumptions and goals**: These questions have the purpose to warm-up the discussion.*

- Please describe your company: How many employees, main business areas, founded when, organized how, etc.
- Who are your customers?
- What kinds of services and applications do you provide?

8.2 Document Interoperability

***Assumptions and goals**: The current state is that government processes are defined by the exchange of documents such as applications, forms, certificates and notifications that are printed on paper or available as PDF or similar formats. There are, however, quite a few standards for electronic document representation which can be used to drive cooperation between administrations.*

- Do you provide services to process data of citizens?
- On which data (documents, etc.) do these services act? Who issues those documents? What documents are produced by the service software you provide?
- Are there standards for the electronic representation of documents? Are those used by your software services?
- Do you use specific software to file and process the documents?
- How important is data and document portability? What role does that play to prevent lock-in situations?

8.3 End-user Services

***Assumptions and goals**: Many services are provided using very specific software. Considered cooperation, this is worse as the underlying processes make sense only in the very specific context of the respective administration. Thesis is that a lot of those applications can be made more general by using SOA principles, extended configurability, etc. Standardized software can be provided to several administrations (and thus are candidates for SaaS).*

- Do you provide customized services to your customers? If so, is the customization done by configuration or do you use adapted software?
- Are there specific parts (e.g. software components) of your system landscape which are used by more than one of your customers?
- Do you use a "SOA"-approach for your services?
- Do you use standardized data formats?
- Do you have "interfaces" to other data centres?

8.4 Foundational (Platform) Services

***Assumptions and goals**: Service management can be standardized (e.g., ITIL). Once we have a proper standards for processes and interfaces, service management can be provides as a cloud service. Current state however is that in particular small data centres use proprietary solutions, a lot of handiwork, and experience of admin staff.*

Please describe the way you perform service management, e.g.,

- Change & configuration management
- Failure management
- Incident management
- System monitoring & event tracking
- Backup approach
- Virtualisation approach

In particular, describe to what degree these aspects are automated. Do you use generic approaches or do you have special solutions? Do you use standardized methods, or proprietary solutions?

- Do you have any suggestion for additional foundational services?

8.5 IT-Cooperation and Cloud Computing

***Assumptions and goals**: The goal of these questions is to determine if there are already examples of IT-cooperation between data centres, and to what degree these can be used as a source for use cases and scenarios. A second purpose is to determine the current state of the introduction of Cloud Computing, in particular with respect to interoperability and standardisation issues.*

Cooperation

- Do you share services or resources with other data centres? Where do you see the main benefits and problems in cooperating with other data centres?
- Do you cooperate with other data centres on administrative processes? If not, could you imagine doing so? Under which conditions this would be beneficial?

Introduction of Cloud Computing

- Do you already use Cloud Computing technologies or do you have plans to introduce them?
- Which services do you consider as main candidates for a migration into a Cloud. Examples: Administrative processes within a particular administration, citizen services, enterprise services, shared processes between several administrations?
- Do you consider the introduction of Cloud Computing as a chance for the definition of new eGovernment related services and application?
- Do you believe that the introduction of Cloud Computing will create potentials for cost reduction for your customers?
- Do you see legal or regulatory problems when cooperating with other data centres? Do you see the need for additional regulation from the German government?
- Are you worried about lock-in to a specific technology or to a specific service provider?
- Are you familiar with the idea of "switching costs" in the cloud? What role does that play to prevent or contribute to lock-in in the cloud?

Interoperability

- Do you see problem in migrating legacy system into the Cloud? What are the benefits of such a migration?
- Do you see any problems concerning the interworking between legacy services and virtualized cloud services?
- Where do you see interoperability problems caused by the introduction and usage of Cloud services?
- Can you imagine to use Cloud resources (either permanently or temporarily) of providers from the private sector? What are the main benefits?

Open Standards and Software

- Do you already use open standards, or are they open standards which are of particular interest for you?
- Do you believe that governmental regulations concerning those standards would be appropriate?
- What is your opinion concerning the use of open source software? Do you believe that governmental regulations concerning open source software would be appropriate?

9 Appendix: Specification of the Demonstrator

The reference architecture for the implementation of the European Services Directive (14) that has been developed by Fraunhofer FOKUS can be used as a blueprint for the architecture of *Public Sector Services* (PSS) provided by collaborating public authorities in Germany. Before elaborating the architecture of the prototype demonstrator for the complaint management service, we explain the components of the PSS architecture in the following Section 9.1. Then, Section 9.2 aligns this generic architecture to the concrete service in question.

9.1 Service Architecture for Public Sector Services

The architecture defines a SOA-framework for the design, implementation and deployment of the sample customer scenarios that are identified in this White Paper. The specification of the *Complaint Management Service* (CMS) demonstrates how this framework can be customized in a Cloud environment.

9.1.1 Components and Execution Environments

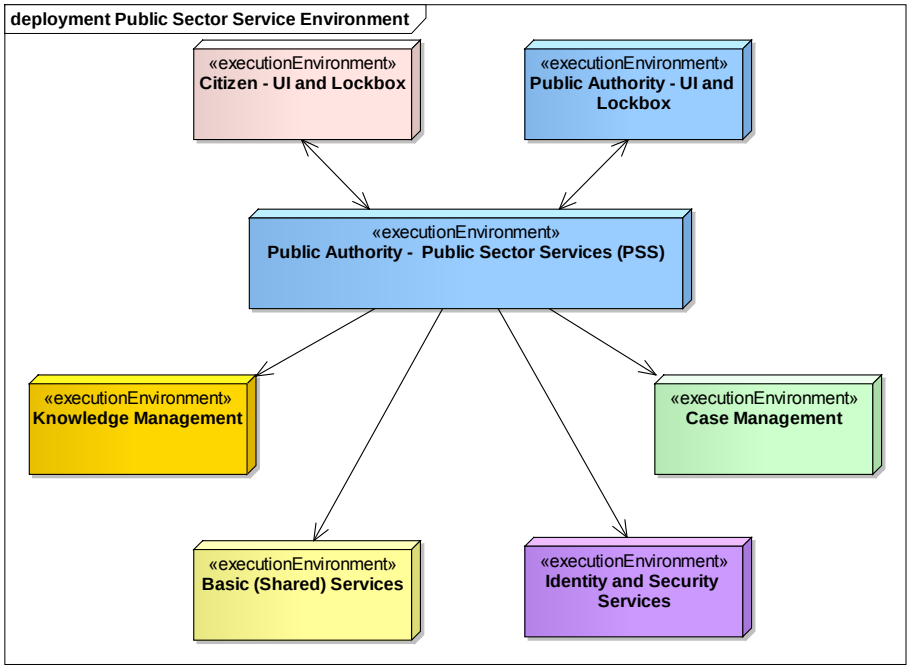


Figure 22: Execution environments for public sector services

Figure 22 defines the most important high level services as *execution environments* . The arrows denote the relations between the components running in the execution environments. Figure 23 provides a more detailed view of these components that are used for the implementation for *Public Sector Services*.

The execution environment of a *citizen* consists of a thin or thick client for the *User Interface* (UI) and a *Lockbox*. The citizen will access the service using its browser and connect to the *PA Portal* of the public authority or, more generally, to an access portal providing a couple of public sector services. For specific services like tax declaration applications a citizen may use a thick client running on the user's PC. In case a public authority returns official notifications to the citizen or has some requests, the citizen has to provide a kind of electronic mailbox called lockbox.

A citizen may use inquiry services in an anonymous way or personalized, trusted services as a registered user or customer. In case the concept is extended to support electronic communication between enterprises and

public authorities the business relationship between the actors involved in a transaction becomes more complex. The enterprise probably will have a *customer relationship* to the public authority and authorizes employees in dedicated roles to act on behalf of the enterprise as a user of associated public sector services.

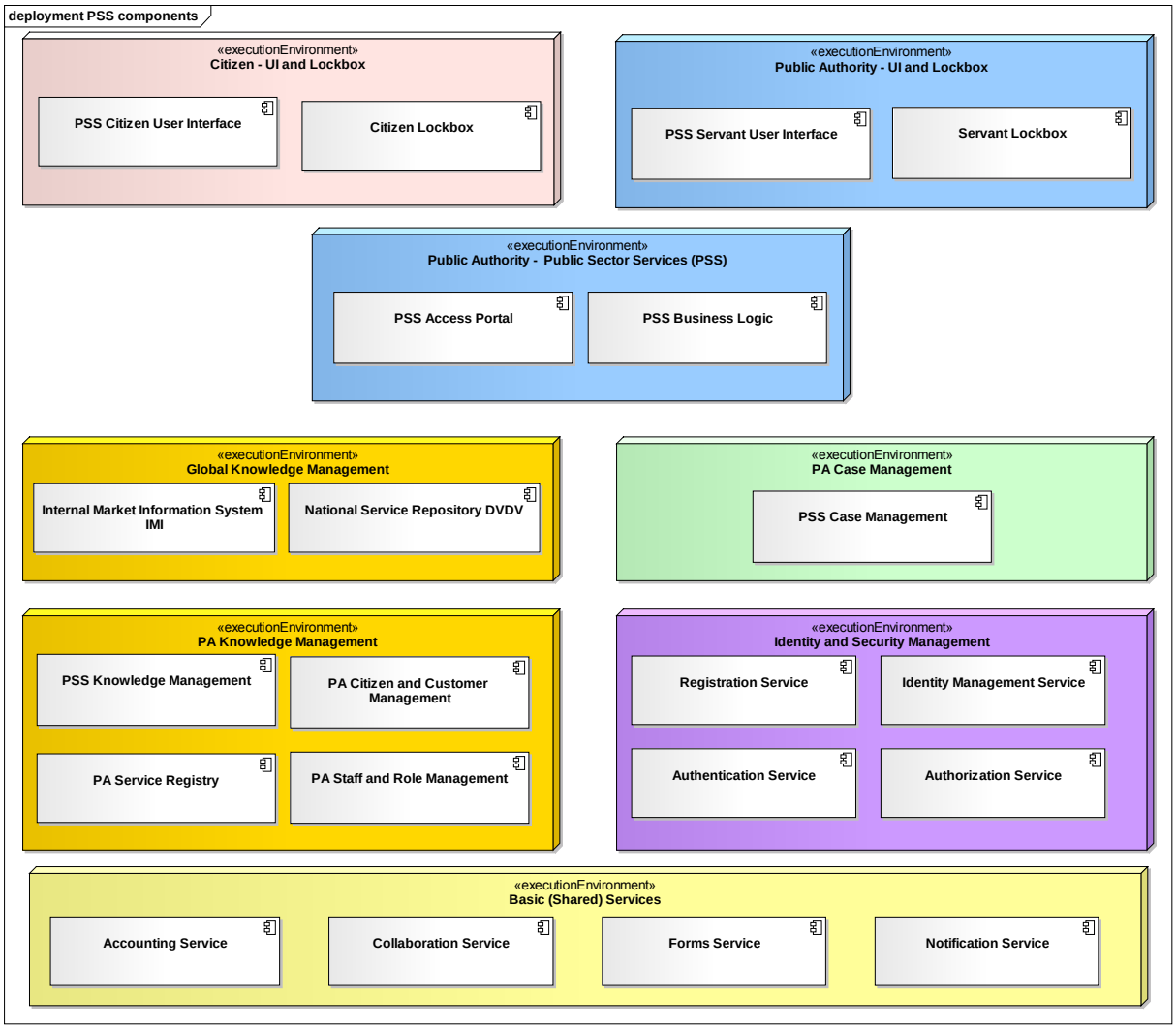


Figure 23: Detailed component architecture for public sector services

9.1.2 PA Services and Repositories

The business logic of the *Public Sector Service* (PSS) runs in the execution environment of the public authority. It can be accessed via dedicated interfaces that in most cases are invoked by the *PA Access Portal* of the public authority. The portal itself can be accessed by a *citizen* respectively by a *servant* via role specific, dedicated user interfaces.

The implementations of *PA Access Portal* and *PSS Business Logic* may invoke a set of supporting services. Depending on the implemented access (identification, authentication, authorization) and session concepts related security services can either be invoked by the portal or by the PSS.

Following the model-view-controller pattern[23] the *PA Portal* implements the view and the *PSS Business Logic* implements the controller part of a PSS. The model is split into two different sub-components:

- Status and history of the PSS *workflow* (application received, processing, pending request, notification sent, objection, closed, …) are managed by the *PSS Case Management* service.
- The data and documents necessary to execute the PSS are managed by associated PSS *Knowledge Management* services. There is an ongoing discussion in Germany if (electronic copies of) user documents and personal data should be *attached* to electronic applications and stored and managed in the knowledge management system of public authorities or if user documents and personal data should be stored under the control of their owner (user, citizen, enterprise) who *authorizes* a public authority to access dedicated documents during the execution of a PSS. The reference architecture supports both solutions.

The PSS is a public service used by citizens or enterprises as well as by PA servants. To distinguish the different users and their roles, additional services supporting the *management of citizens and customers* (enterprises) and the *management of staff and their roles* within the public authority are running in the public authority's execution environment as part of the *PA Knowledge Management*. Access to these internal services is only granted to authorize servants via dedicated user interfaces supported by the *PA Access Portal*.

Citizens, servants and probably other services access a PSS with different roles and access rights. The *Identity and Security Management* provides a set of services used by anonymous and registered citizen and by registered public servants. These services are responsible for the registration of citizens and the identification, authentication and authorization of citizens, servants and administrators.

In addition to the *PSS Knowledge Management* service several other registries and information resources are necessary to implement collaborating PSSs. The *PA Service Registry* (SR) is needed to locate supporting public sector services, security services and basic services, which are all registered in the SR. In Germany the national registry for public services (DVDV) (30) can be used as a global accessible service registry. In a European environment the Internal Market Information System IMI (16) will be part of the knowledge management. IMI provides information about the posting of workers within the EU.

Basic *shared services* contain PSS independent services supporting functionalities such as accounting, collaboration, forms and notifications. Not all services are used in the scenarios considered in this paper even though some are typical candidates to be outsourced in a shared, public cloud SaaS environment.

9.2 Complaint Management and Complaint Processing Services

The demonstrator described in this section is an instantiation of the complaint management and complaint processing services introduced in Section 5.2.2 and further described in Section 6. While the previous sections concentrate on analysis and the definition of functional requirements from a user perspective, respectively, in this section we are going to perform a detailed modeling of the software architecture.

9.2.1 Functionality

The *Complaint Management Service* CMS offers the following general functions:

- Citizens can issue complaints using, e.g., a mobile phone. It is possible to send a complaint description including location information and a picture either anonymous or identifiable, i.e., associated with a

[23] This software design pattern distinguishes the implementation of business logic (controller), data access and storage (model), and user interface (view).

registered citizen account. Issuing an identifiable complaint requires prior registration. In the latter case, automatic notification via SMS on changes of the status of the complaint can be requested.

- A registered citizen can use his account to review the statuses of his complaints ("myComplaints" interface). Automatic notifications on status changes can be turned on and off.
- There is a public Web interface ("allComplaints") displaying all complaints in a selected area (without citizen ids). Some filtering functions such as type of complaint are desirable.
- The CMS routes complaints to *Responsible Public Authorities* (RPA) such as road maintenance and waste management where the complaint is processed in associated *Complaint Processing Services* (CPS). During this process, personal information (citizen ids) is removed and only general information about the complaint such as category, time, date, location and reference to the taken picture is forwarded.
- Complaints will be administered in two public authorities:
  - The *CMS Provider* (CMSP) provides functions to administer the associated cases including personal information. The anonymous complaint descriptions are stored (read/write/delete) within the *CMS repository*. The associated cases are managed in the *CMS Case Management*.
  - The *Responsible PA* (RPA) handles the processing of anonymous complaints in the *CPS Case Management* and forwards status changes to the CMS. The RPA can access (read) the complaint descriptions administered by the CMSP.

9.2.2 Roles and Actors

The following list explains the different roles of system users, their rights and responsibilities.

9.2.2.1 Complaint provider

Citizens are the provider of complaints. They can access the system with two different roles:

- *Anonymous citizen* issue an anonymous complaint, access public complaint display via the "allComplaints" interface.
- *Registered citizen* issue an identifiable complaint, access "myComplaints" interface, access/edit user profile, turn automatic notifications via SMS on/off

9.2.2.2 CMSP Administration

- *CMSP administrators* add/remove/edit citizen and servant accounts and roles
- *CMSP servants* are processing the complaints (edit complaint status, issue re-routing)
- *Citizens* register and edit account and profile information

9.2.2.3 Responsible Public Administration

- RPA administrators add/remove/edit customer (other Pas) and servant accounts and roles
- RPA servants are processing the complaints (edit complaint status)

9.2.3 Components and System Architecture

Figure 24 describes the general system components of the *CMS demonstration scenario*. The components on the left are used to implement the CMS itself; the components on the right are used to implement the associated public sector services running in the RPAs. Both families of components refine the general component architecture depicted in Figure 23 by refining necessary components and removing unnecessary components. It can be concluded that the component architecture of the complaint management scenario fits well into the generic framework for German public services.

Both CM and RPA services are implemented using access portals. These portals govern access to the provided services considering the authorization of staff members and citizens. While citizen are only allowed to use the *Registration Service* and the *CMS*, servants are allowed to use associated interfaces of CMS and RPAs and administrative services depending on their role and authorization.

The knowledge management contains the CMS-specific *CMS repository* – CRS. This repository provides access to descriptions of complaints including public available information such as pictures, category, time and date, and location. The service is accessible utilizing the Open Data Protocol OData (30). It has to be ensured that read access (all users) and read/write/delete access (CMSP) are distinguished.

The *CMS Case Management* uses personal data of the citizens and manages the status of complaints that have been reported by them. The *RPA's Case Management* systems running in the responsible PAs use anonymous identifications to identify complaints. They don't depend on private data.

The CMSP administrative security services manage access information for staff members and citizens. The corresponding PA services manage access information for staff members and possibly for the CMSP and other collaborating public authorities.

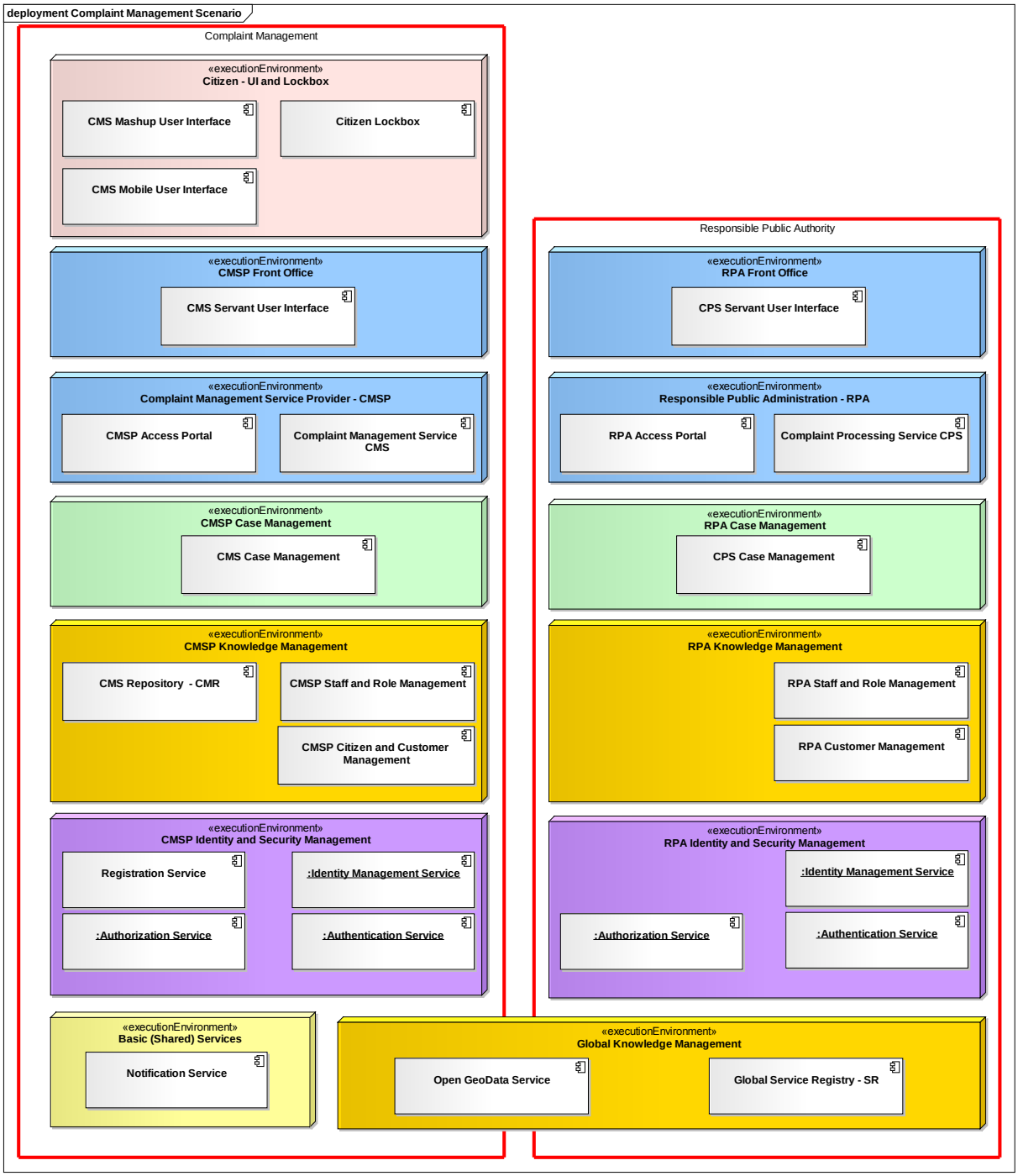


Figure 24: System component architecture

Only the CMSP provides a registration service for citizens. The addresses of the CMS and the RPASs respectively their interfaces are stored in the global *Service Registry* (SR). An *Open GeoData Service* allows access to geographical maps in the complaint Mashup shown to the end users.

9.2.3.1 Deployment Architecture

Figure 21 on page 53 shows which components are deployed in the environment of a citizen, the CMSP and responsible PAs. The CMSP is implemented in a Liferay environment implementing several administrative function using Liferay internal REST/JSON interfaces. The CPS is implemented in a SharePoint environment.

The arrows depict the most important invocations between the components showing the communication protocols used in the scenario.

- The citizen layer components and the servant UI components invoke the CMS and CPS services using REST/JSON.
- The complaint repository service is accessed using OData that is a REST/JSON based protocol, too. Write access to the *repository* is only possible for authorized users via the *CMSP Access Portal* and the *CMS*. Read access to the *CMR* is possible for anonymous users via the OData-API.
- Between CMS and CPS Web services are used.

The main components of the scenario are deployed in a private cloud utilizing Microsoft System Center 2012. The open data and public services are deployed in a public cloud utilizing Microsoft Azure. The public authorities CMSP and RPA have access to all restricted information in the private cloud. All personalized data is stored in a private cloud. Public information about the complaints is stored in the public cloud to demonstrate access to data stored in the cloud. For this reason the CMS repository service is deployed in a public cloud and can be accessed from external clients (read-only) and the CMS (r/w/d).

As mentioned before, the *Case Management Services* in the responsible PAs operate on non-personal data. For this reason the services can be deployed in a public cloud. They act as an example for a service that can be outsourced to a public infrastructure. Of course it has to be guaranteed that this service can only be accessed by authorized servants utilizing appropriate means.

9.2.4 Component Interactions

This section describes some simplified sequence diagrams (MSC) of the CMSP services. The MSCs are used to specify the possible interactions in the CMS scenario in some more detail. A bold arrow indicates a synchronous invocation; the request has a return value. Thin arrows indicate notifications.

Some communication protocols in the MSCs are grouped to UML fragments. These fragments indicate control structures such as loops or alternatives (case).

9.2.4.1 Registration

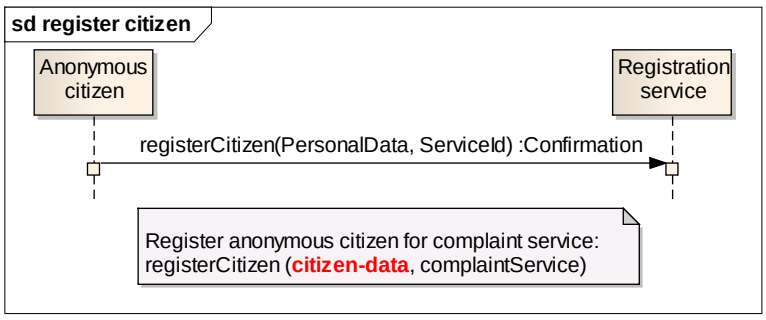


Figure 25: Registration of a citizen for a PSS

A citizen registers himself for a specific service providing the required personal data. Similar functions to cancel the registration and to inquire information about existing registrations have to be provided.

9.2.4.2 Complaint Processing

Figure 26 depicts how a registered citizen provides information about a new complaint and inquires information about his existing complaints. Figure 27 shows how an anonymous citizen provides information about a new complaint and inquires public available information about complaints.

Both diagrams focus on the interworking between citizens, CMS and RPAS and abstract from further services and implementation details. The protocol between citizen, access portal and public sector service is not considered, too.

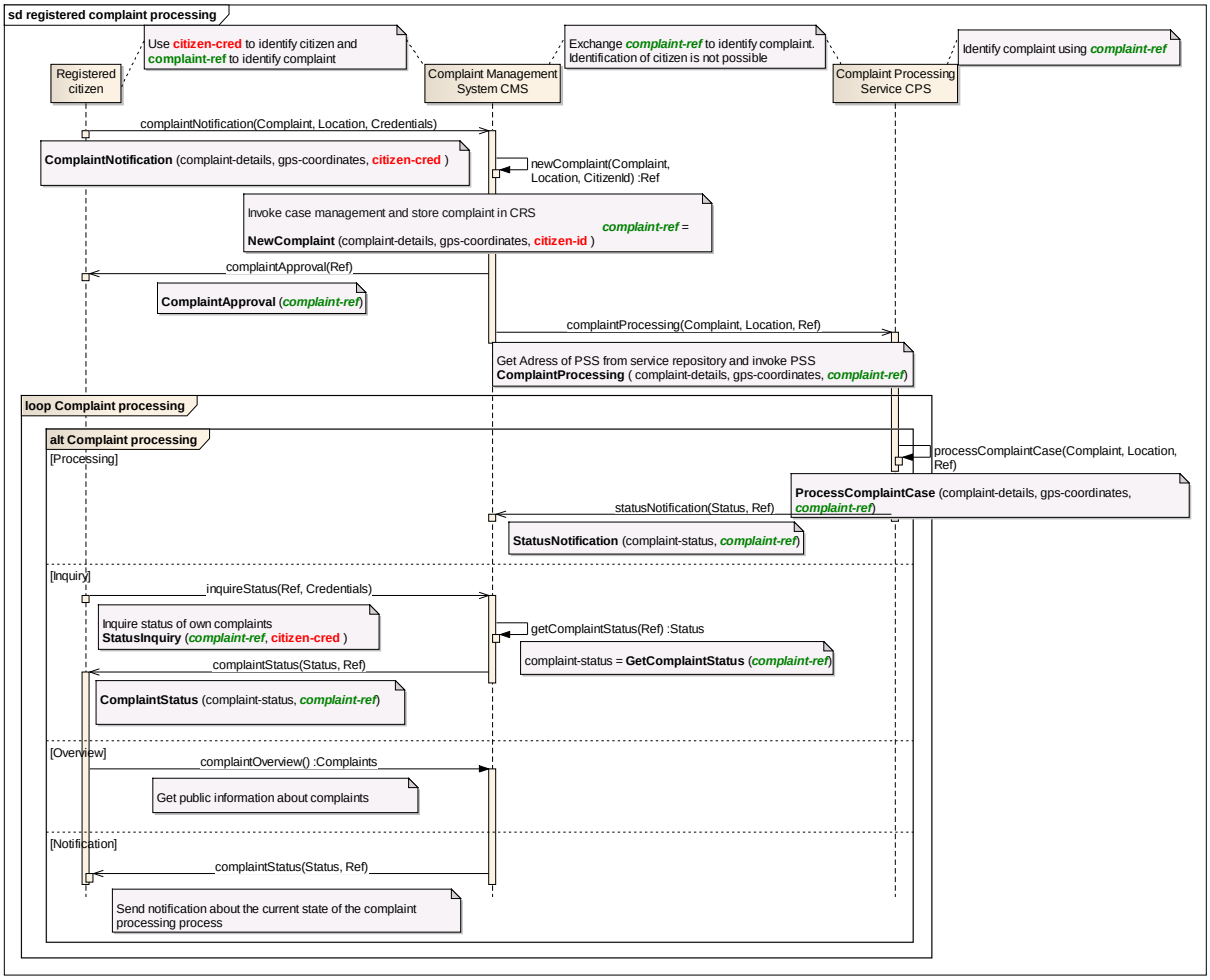


Figure 26: Complaint processing for registered citizens

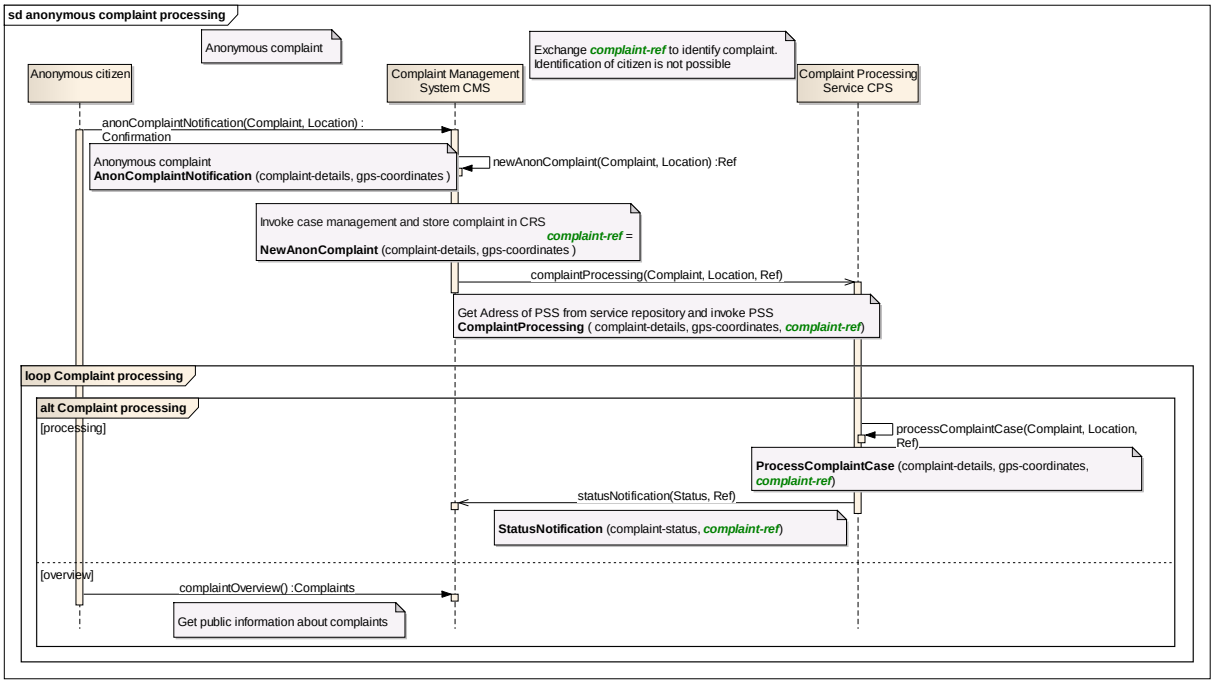


Figure 27: Complaint processing for anonymous citizens

9.2.5 Interfaces and Data Types

This section provides a first version of the specifications of components, interfaces and data types. The specifications have to be refined during the design and implementation process.

The MSCs are using the following specifications of the components and interfaces involved in the CMS scenario. The specifications, especially of the “core-interfaces” to the servants, have to be refined during the next design steps of the scenario.

A complaint (as a data type) has at least the following attributes:

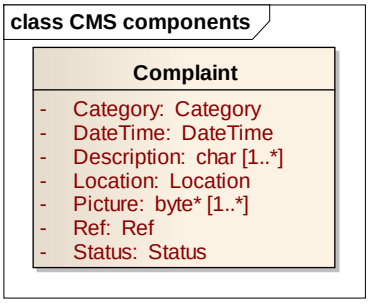


Figure 28: Complaint data type

9.2.5.1 Constraint Management System CMS

The CMS provides one interface to the servants, two interfaces to the anonymous and registered citizens, and one callback interface to the RPAs.

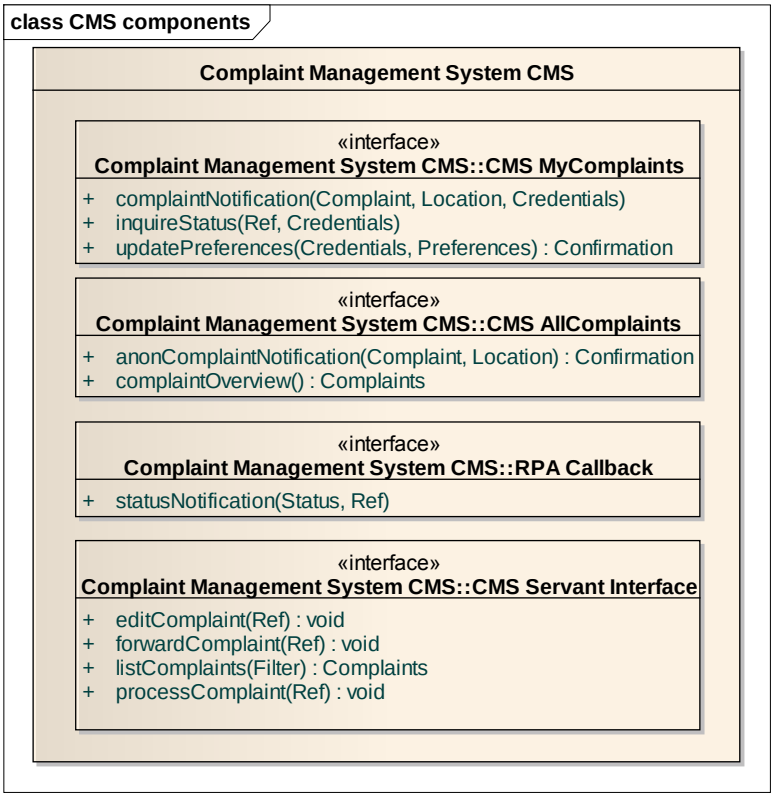


Figure 29: CMS interfaces

9.2.5.1.1 CMS Case Management

The CMS Case Management provides operations to create new cases, to set and get status information and to get references to all complaints of a given citizen.

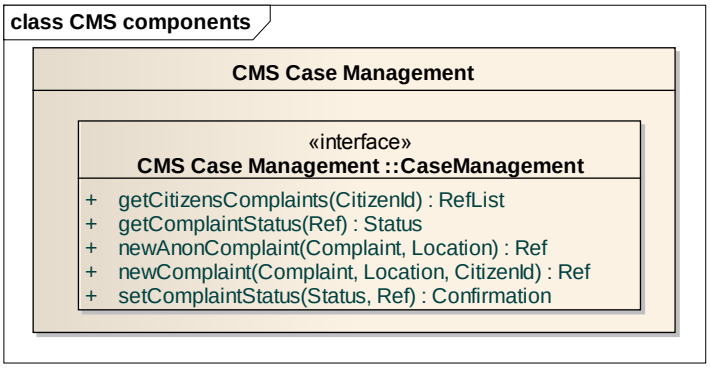


Figure 30: CMS Case Management

9.2.5.2 Registration Service

The registration service supports the registration and deregistration of citizens, the subscription and un-subscription of public services, and information about all subscriptions of a given citizen.

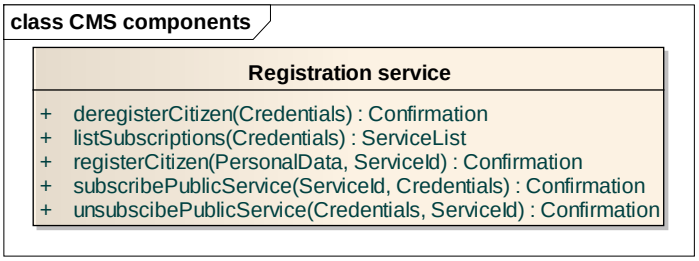


Figure 31: Registration service

9.2.5.3 Complaint Processing Service at Responsible Authority

The *Constraint Processing Service* CPS provides one interface to the CMS and one interface to the servants.

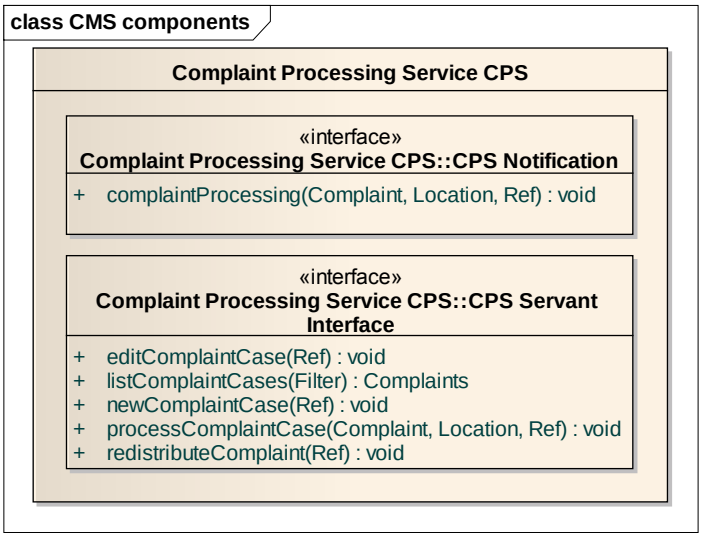


Figure 32: CPS interfaces

CPS Case Management

The case management for the CPS is a little bit simpler than for the CMS.

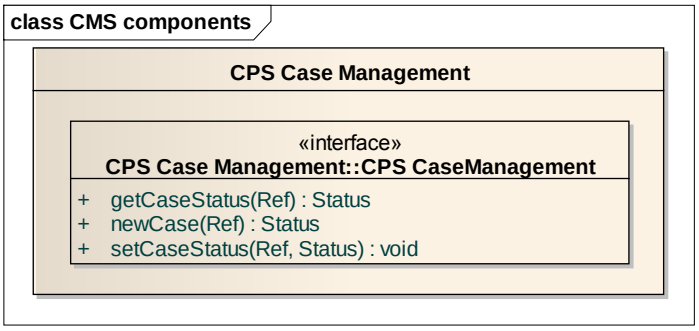


Figure 33: RPA Case Management

9.3 Analysis and Discussion

The scenario illustrates several interoperability issues identified in the interviews:

- Interoperability problems are apprehended for
  - *Data and document formats:* Addressed by “standardized” description of complaints
  - *Protocols between services:* Addressed by utilization of OData and inter PA protocols
  - *Standards to mediate between Cloud services and Cloud infrastructure*
- The scenario demonstrates an innovative service that is currently not (or prototypical) available in Germany but that can be designed and implemented utilizing the framework developed for collaborating public sector services. Such innovative services are typical candidates to evaluate the usability of cloud computing.
- The scenario demonstrates how SOA concepts (reusable services, dynamic binding) can be used in combination with cloud technology.
- Collaboration of public sector services, hosted in different data centers, can be demonstrated.
- Storage and secure access of data stored in a public cloud (*integrative platform*) can be demonstrated. The whole scenario is implemented in a hybrid cloud.
- Integration of public cloud SaaS concepts (case management) into public sector service can be demonstrated.

10 Appendix: Templates for Usage Scenario and Use Case Descriptions

10.1 Introduction

This document proposes the employment of usage scenarios and use cases as an analysis tool to identify specific characteristics and requirements of Cloud Computing. By a usage scenario we mean a concrete (however potential) implementation of a Cloud based system or service. A use case describes the activities of the actors (or components) of such a system or service while using such a system or service in a particular way: A usage scenario therefore serves as a concrete "story" with the purpose to demonstrate a certain concept or idea. It may comprise several use cases.

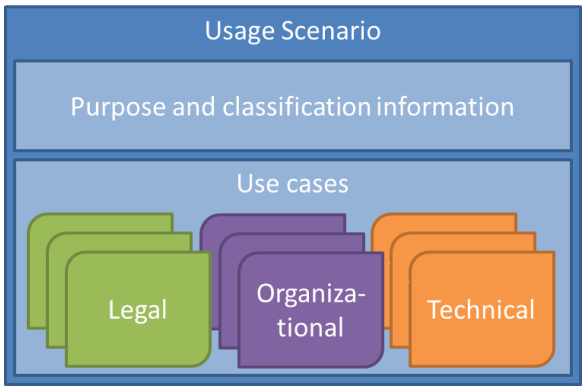


Figure 34: Usage scenarios and use cases

Figure 34 illustrates the relation between usage scenarios and use cases. A usage scenario comprises consists of a description of its purpose (combined with an outline of the concrete system or service), and a number of use cases. Currently, three relevant categories of use case have been identified: Legal, organizational, and technical use cases.

The document is structures as follows. Section 10.2 introduces the templates proposed to describe usage scenarios (Section 10.2.1) and use cases (Section 10.2.2). In Section 10.3, an extensive example of a usage scenario and (Section 10.3.1) associated use cases (Section 10.3.2) is discussed. The usage scenario describes a Cloud service (involving PaaS and SaaS) objects, namely an electronic document safe (EDS). The EDS is understood as a means to enable the exchange of electronic documents between citizens, enterprises, and administrations. It is designed in particular to identify issues in using Cloud Computing in the context of public administrations.

In the Sections 10.3.2.1 – 10.3.2.3, a number of use cases are defined which illustrate certain points. Since requirements on the use of Cloud Computing (or any technology) in the public sector (and therefore, requirements on standardization) cannot be identified and analyzed without a legal, societal, or political context, strong emphasize have been laid on viewing on these use cases from a "German" perspective. The intention is not to restrict to the legal and regulatory framework valid for Germany, but to illustrate how use cases can be used to take the national specifics of different countries into account: If we succeed to develop a method to answer question concerning, e.g., data privacy, and illustrate how to apply it to Germany, a similar approach will work for other countries as well.

10.2 Templates

10.2.1 Usage Scenario

A usage scenario is therefore described by the following items:

- **Description**: A general description of the US, e.g., by means of a little story illustrating its main points and purposes.
- **Category**: The main focus of the US, **technical**, **organizational**, **legal, business**, etc. (not exclusive) The categories determines the template(s) used for use case descriptions.
- **Domain:** The application domain of the US, e.g., Identity, Data privacy, Public sector services, Security, Environment, Quality of service, Management, Transport, etc.
- **Goals and purposes:** A description of the main concepts and ideas to be illustrated by the US. What are the main points to be conveyed? What is the rationale behind the usage scenario
- **Actors and Roles:** Actors playing specific roles in the usage scenario. This may include domain specific entries (e.g., additional service providers).
- **Software layers:** IaaS, PaaS, SaaS, etc.
- **Deployment model:** Private, public, community, hybrid, etc.
- **Components and services**: Some architectural description of the system described in the US.
- **Existing specifications to rely on**: Are there already standards or specs available?
- **New specifications required**: What is not yet available?
- **Related use cases**: List of Ucs related to the US.

Usage scenario template

ID	Title
Description	Main “storyline” for the use case
Category	**Technical**, **organizational**, **legal**, …
Domain	E.g., public sector services
Goals and purpose	What is demonstrated by the US?
Actors and Roles	Actors and their roles participating in the scenario, e.g., described using a table as follows:

Actor	**Roles**
Actor 1	Role 1 for actor 1 Role 2 for actor 1 . . .
Actor 2	Role 1 for actor 2 Role 2 for actor 2 . . .

Software layers	IaaS/VM layer, PaaS layer, etc.
Deployment model	Private, public, community, hybrid, …
Components and services required for execution, and proposed architecture	Relate of a reference model and deployment model, provide some architectural description
New specifications required between the actors	Identification of specification (and standardization) requirements (derived from the corresponding entry in the use case descriptions)
Related use cases	**List of use cases related to this scenario**

10.2.2 Use Cases

Use cases describe certain aspects related to a usage scenario, for instance a detailed interaction between user and provider. We distinguish between technical, organizational, and legal use cases, organized into the following hierarchy:

Hence, depending on the level of granularity, a legal use case may determine several organizational use cases illustrating how the legal requirements are implemented, which in turn are related to several technical use cases. For instance, the German legal requirement that security events need to be reported to the responsible data privacy authority implies that there are procedures in place to do so. Which parts of the hierarchy need to be present depends on the purpose of the corresponding usage scenario. If the objective is to understand some technical issues, then use cases on the technical level are sufficient. On the other hand, if the objective is to analyze how a specific legal regulation is implemented by organizational and technical means, then use cases from all three categories have to be present.

10.2.2.1 Legal

Legal use cases may relate to a certain area, e.g., Europe, US, China, etc. Since Clouds are globally distributed amongst a number of countries, different legal frameworks need to be considered.

Legal use case template

ID	**Title**
Description	Short summary of the use case
Actors and Roles	Actors and their roles participating in the scenario, e.g., described using a table as follows: **Actor** / **Roles** **Actor 1**: Role 1 for actor 1; Role 2 for actor 1; . . . **Actor 2**: Role 1 for actor 2; Role 2 for actor 2; . . .
Goals and aspirations for the UC	Background and main message of the use case
Legal domain	Data privacy regulations, licensing, contracting, etc.
Area	E.g., Europa, US, . . .
Legal frameworks, laws, etc., to be taken into account	Laws, policies, etc. which are of relevance
Required preconditions	Any preconditions necessary to understand the use case
Compliance criteria	Explanation why the use case is an illustration on how legal requirement can be implemented
Description of procedures to ensure legal compliance	Explanation how the use case shows the implementation of legal requirements
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case
New specifications required between the actors	**Specifications and standards needed to establish the goals of the use case**

10.2.2.2 Organizational

Describes organizational measures, e.g., service management procedures to be implemented, permissions, obligations, etc.

Organizational use case template

ID	Title
Description	Short summary of the use case
Actors and Roles	Actors and their roles participating in the scenario, e.g., described using a table as follows: **Actor** / **Roles** **Actor 1**: Role 1 for actor 1; Role 2 for actor 1; . . . **Actor 2**: Role 1 for actor 2; Role 2 for actor 2; . . .
Goals and aspirations for the UC	Background and main message of the use case
Organization domain	E.g., security procedures, data privacy procedures, etc.
Regulations and policies to be taken into account	Policies, standards, best practices to be taken into account
Description of organization procedures	The "workflow" (or procedures) on organizational level used to achieve the goal of the use case
Components and services involved	What components and services of the system in question (described in the usage scenario) are needed/used to realize these procedures
Required preconditions	Any preconditions necessary to understand/implement the use case
Criteria for success	The expected output and the side effects
Failure conditions	What can go wrong
Failure handling	what to do about it
Related Ucs and those that are pre-requisite	May refer to technical UC describing the technical means to implement this UC.
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case
New specifications required between the actors	**Specifications and standards needed to establish the goals of the use case**

10.2.2.3 Technical

Technical use case template

ID	Title
Description	Short summary of the use case
Actors and roles	Actors and their roles participating in the scenario, e.g., described using a table as follows: **Actor** / **Roles** **Actor 1**: Role 1 for actor 1; Role 2 for actor 1; . . . **Actor 2**: Role 1 for actor 2; Role 2 for actor 2; . . .

Primary Actor	The actor who initiates the technical use case
Goals and aspirations for the UC	Background and main message of the use case
Platform, tools and the environment needed for execution of the UC	Technical requirements concerning the execution environment
Description of file formats, wire protocols, in-memory objects, and other artifacts needed for execution	"Artifacts" used in the use case
Components and services required for execution	What components and services of the system in question (described in the usage scenario) are needed/used to realize these procedures
Input params needed for initialization	Initial input values for the execution of the use case
Criteria for success	Expected process, outcome, side effect. Described by sequence charts, etc.
Failure conditions	what can go wrong
Failure handling	what to do about it
Related Ucs and those that are pre-requisite	Relevant use cases for the associated usage scenario.
Existing specifications to rely on	Specifications and standards already dealing with aspects related to the use case
New specifications required between the actors	**Specifications and standards needed to establish the goals of the use case**

10.3 Examples

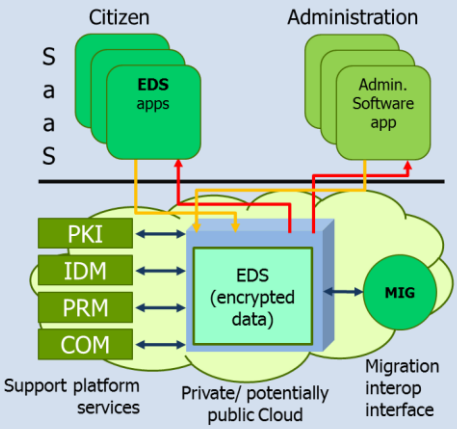
10.3.1 Usage Scenario: Electronic Document Safe

Usage scenario

US01	Electronic Document Safe (EDS)
Description	Bob and Clair, proud parents for the first time, face the next challenge in their life, namely to manage applying for *parenting benefit*. In Germany, this is a fairly complex procedure citizens have to cope with; a complete description is beyond the scope of this report. For the purposes of this section it is enough to understand that a number of documents are necessary to complete the application comprising at least the following: ■ Birth certificate of the child (issued by *the civil registry office*) ■ Certificates of salary (prior the data of birth of the child, issued by the employer) ■ Certificate of the *health insurance* on maternity benefit ■ Certificate of the *employer's* contribution to the maternity benefit ■ Declaration of planned working hours during acquisition of the parenting benefit (by the *parents*) ■ Certificate on planned working hours (issued by the *employer*) Fortunately, Bob and Clair own electronic document saves (EDS) to store and administrate these (and other) documents. Basically, an EDS is a secure storage for official documents. Government agencies or other parties such as employers can access the EDS to enter documents (such as official notifications, certificates of salary, rental contracts, insurance policies, etc.) for the owner of the EDS, and access those documents if necessary to perform an administrative procedure. EDS owners access the safe using a special application providing secure encrypted communication and save authentication. Additionally, government agencies, enterprises, insurance agencies, etc. can use open interfaces to enter documents into EDS, and to access its contents (these activities require an explicit authorization by the EDS user).
Category	**Technical**, **organizational**, **legal**
Domain	Public sector, public private partnership
Goals and purpose	Purpose of the usage scenario is to demonstrate how personal documents can be stored in public/hybrid Clouds while preserving evidence using cryptographic signatures. Current solution for electronic data exchange between citizen, enterprises, and administrations (e.g., the German ELENA system for electronic tax computation) base on massive data retention: Administrations acquire citizen data for future use. From the perspective of data privacy regulations, this practice is very questionable since data acquisition has to be based on a concrete purpose. Hence, the EDS provides an alternative to data retention. In principle, a private sector company could assume the role of an EDC provider as well: ■ Since data in the EDS are encrypted and thus not visible to the provider, the "data protection barrier" can be considered as comparable "low": In fact, there is a vivid discussion ongoing between German legal experts whether data encryption qualifies as sufficient data anonymization. ■ When owning an EDS, citizens approve that personal data are stored and processed electronically. Hence, data privacy applies only insofar as citizens have to trust the EDS provider. On the other hand, if an EDS is interpreted as a technical mean to support

	administrative processes, governmental public guarantee obligations apply: Government agencies are responsible to ensure the continuing availability of this service (up to 120 years for certain types of documents). Hence, the question arise how a private sector provider is capable to give sufficient guarantees on its own continued existence, future business orientation, etc. A possible solution is to maintain a governmental Cloud provider as "fall back", while allowing public sector providers to participate on the emerging market of electronic document storage. Of course, interoperability between private and public sector platforms to operate EDS like system is mandatory.
Actors and Roles	

Actor	Roles
Citizen	Document & EDS owner Document/data provider or consumer
Public EDS space provider	Safe provider
Government agency (Administration)	Document/data provider or consumer
Certificate Provider	Certificate provider (OCSP)
PKI provider	Key management provider

Software layers	PaaS, SaaS
Deployment models	Public, hybrid
Components and services required for execution, and proposed architecture	 A number of additional components are required: ■ Key management for encryption of documents and communication channels ■ Identity management for access authentication and authorization ■ A process management to embed the EDS as software service in a Cloud infrastructure. ■ A communication service providing secure and reliable transfer of electronic documents. Access to the EDS is provided by two mechanisms: ■ An EDS app allows the EDS owner to access the contents of his/her safe, to organize them, and to delete if required. In a primitive form, such an app provides simple browser, file management and access right management functionalities. ■ Enterprises and administration who generate documents and access them via specific software applications access the EDS by means of a specific adapter layer. Finally, in order to design a case for public private partnership, it becomes crucial that means are available to transfer documents in the EDS tenant storage between providers: EDS owners cannot rely on the continued availability and sufficient service level of a private enterprise; therefore, a migration interface (MIG) have to be available to transfer the contents of the EDS from one provider (and EDS implementation) to

	another: of course, the transfer syntax need to follow accepted and established data representation standards.
New specifications required between the actors	■ **UC-Organizational**: Specifications for "dynamic" (i.e., temporary, short-term) Cloud bursts (SLA, security, data protection, etc.) ■ **UC-Technical**: Data migration protocol specification and Migration interface (MIG) specification
Related use cases	**UC-Legal, UC-Organizational, UC-Technical**

10.3.2 Use Cases

10.3.2.1 Legal: Data Privacy Regulations

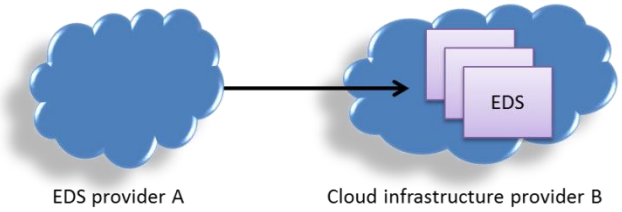
Legal Use Case

UC-Legal	**Document release towards an administration**
Description	The use case describes how a public administration requests a document from a citizen in the course of an administrative process.
Actors and Roles	Actor: Citizen — Roles: Document & EDS owner, Document provider Actor: EDS provider — Roles: Safe provider Actor: Government agency (Administration) — Roles: Document consumer Actor: Certificate Provider — Roles: Certificate provider (OCSP) Actor: PKI provider — Roles: Key management provider
Goals and aspirations for the UC	According to German data regulation laws, personal data (which are assumed to be represented by the documents referred to in this use case) are allowed to be collected and processed only if ■ There is a law permitting, or ■ The owner of these data has agreed. Moreover, the administration needs a concrete reason such as an administrative process initiated by a citizen's application. Citizens have the right to be informed which personal data are available to an administration, and for which purposes they are used. The use case describes a process which ensures that these legal requirements are met.
Legal domain	Data privacy
Area	Germany
Legal frameworks, laws, etc., to be taken into account	■ Date privacy laws in Germany (on federal and federal state level) ■ Data privacy directive of the European Union Since documents stored in the EDS provide evidence about the citizen, electronic signatures and certification is required. Hence, a number of additional regulations have to be taken into account. The most important ones are: ■ German Signature Law ■ European Signature Directive
Required preconditions	■ Citizen registration at EDS provider ■ Application at the administration by the citizen
Description of procedures to ensure legal compliance	■ Administration requires a certain document from Citizen for a certain purpose. It delivers information about the purpose and the legal foundation of the data collection. ■ Citizen releases the requested document in his/her EDS for access by the administration, and sends access information to the administration. ■ Administration retrieves the document. If necessary, signatures and certificates are validates.
Compliance criteria	Collection of personal data is done in compliance with German data protection

	laws. In particular, the user knows about the data collection and processing, is informed about its purpose.
Related Ucs and those that are pre-requisite	NONE
Existing specifications to rely on	BSI Baseline Protection Catalogs, privacy protection laws, Signature law.
New specifications required between the actors	NONE

10.3.2.2 Organizational: Cloud Burst

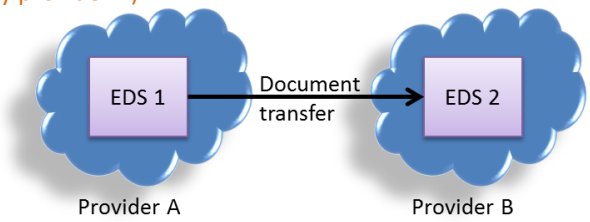
Organizational Use Case

UC-Organizational	**Cloud burst – Change Management**
Description	To reduce its own operational costs, the EDS provider decides to accept an IaaS offer from another Cloud provider an use its virtualized resourced to provide the EDS service. 
Actors and Roles	**Actor** / **Roles** **Citizen** – Document & EDS owner **EDS provider A** – Safe provider **IaaS provider B** – Cloud infrastructure provider
Goals and aspirations for the UC	The use case raises a number of questions, for instance: ■ What legal requirements have to be fulfilled by provider B? ■ How to establish trust between citizen, administration, and provider B? ■ How to formulate (and to ensure) SLAs between A and B? ■ How to implement data protection requirements at provider B (which includes system level monitoring and reporting on system level)? We concentrate in this use case on the specific aspect of such an outsourcing situation, namely change management. In contradiction to the "self-service" aspect of Cloud Computing, security requirements (in particular in connection with the collection and processing of personal data) require detailed agreements on service management between contractual partners.
Organization domain	Outsourcing
Regulations and policies to be taken into account	BSI Baseline Protection Catalogs (12)
Description of organization procedures	Provider A requires that B proves the establishment of a proper change management, including the documentation and reporting of measures for ■ Changes in IT systems (new hardware, software, network connections, applied updates and security patches, etc.) ■ Changes in the strategic orientation of provider B ■ Changes in user and administrator role structure, user groups ■ Involved sub-contractors
Components and services involved	System level as well as service level (i.e., EDS related) components and services.
Required preconditions	NONE

Criteria for success	Establishment of an effective change management by provider B. A is able to validate that necessary security requirements (e.g., related to data privacy) are effectively fulfilled by B.
Failure conditions	1) Problems caused by infrastructural changes 2) Change of business model of B resulting in changed service levels or pricing 3) Involvement of sub-contractors
Failure handling	1) Re-negotiation of requirements on change management (or discontinuation of contract) 2) Re-negotiation of prices and SLA (or discontinuation of contract) 3) Definition and establishment of a change management concept including new sub-contractors (or discontinuation of contract)
Related Ucs and those that are pre-requisite	NONE
Existing specifications to rely on	BSI Baseline Protection Catalogs (12) on data protection, outsourcing, change management
New specifications required between the actors	**Specifications for "dynamic" (i.e., temporary, short-term) Cloud bursts (SLA, security, data protection, etc.)**

10.3.2.3 Technical: Document Migration

Technical Use Case

UC-Technical	**Document Migration from Provider A to Provider B**
Description	The UC describes the migration process of documents from one EDS (EDS 1) hosted by EDS space provider A into another one (EDS 2) (hosted by provider B): 
Actors and roles	**Actor** / **Roles** **Citizen** – Document & EDS owner **EDS provider A** – Document sender **EDS provider B** – Document receipient **Certificate Service Provider** – Certificate provider
Primary actor	Provider B (on behalf of citizen)
Goals and aspirations for the UC	Since documents may contain evidence records and thus need to be signed in order to ensure authenticity, migration from one EDS provider to another has to be compliant with laws and regulations valid for the authorities who have issued these document and that are entitled for further processing. In Germany, a number of regulations have to be considered (see UC-Legal). The definition of proper procedures for document migration from one EDS into another one reflects the particular requirement that EDS users have to be prevented from lock-in situations.
Platform, tools and the environment needed for execution of the UC	■ Cooperative identity management between provider A and B for proper authentication of the owner and authorization of the transfer ■ Cooperative security context between provider A and B (to ensure encryption of documents during transfer)

Description of file formats, wire protocols, in-memory objects, and other artifacts needed for execution	Cryptographically signed documents containing evidence records can be implemented as XML based data structures. The technical guideline (19) recommends using the following structuring of data and metadata (referred to as XML based Archival Information Package – XAIP) ■ An archive **package header** with information about the logical structure(s) of the XAIP document and the sender. ■ a data section for **meta information** for description of the transactional and archiving context of the content data, ■ a data section for the **content data** (the guidelines supports – amongst others – encrypted documents), and ■ in the event of the storage of electronically signed documents, a data section for the storage of signatures, certificates, signature verification information, and electronic time stamps. This **certificate section** contains an Evidence Record which serves to prove the intactness of the integrity and authenticity of the archived data objects. The transfer of XAIP represented documents can be done using any transmission protocol supporting data encryption.
Components and services required for Execution	■ Migration interface (MIG) – compare usage scenario US01 ■ Certificate service ■ Signature validation service ■ Encryption service
Input params needed for initialization	NONE
Criteria for success	Compare the interaction outlined in Figure 35. The initial and final stages of the interaction. The establishment and release of a common security context between provider A and B have not been modeled in detail. Since a general trust relation between A and B cannot be assumed, a detailed description required actors (e.g., an additional identity management service provider) and interactions is likely to be very complicated and thus is beyond the scope of this document. It should be noted that data migration is not considered in the guideline (19). Therefore, the statements done in this use case are not supported by the BSI.
Failure conditions	1. Validation of user credentials fails 2. Establishment of a common security context fails 3. Invalid access permissions (several stages) 4. Signature validation fails 5. Certificate validation fails 6. CSP is not reachable
Failure handling	Cases 1. – 5. Abort and roll-back of the transaction. Notification of (a) document owner, (b) providers, (c) resp. data protection official. Case 6. As before, but an additional notification sent to the CSP
Related Ucs and those that are pre-requisite	User registration at providers A and B.
Existing specifications to rely on	(19) (and annexes)
New specifications required between the actors	**Data migration protocol specification** **Migration interface (MIG) specification**

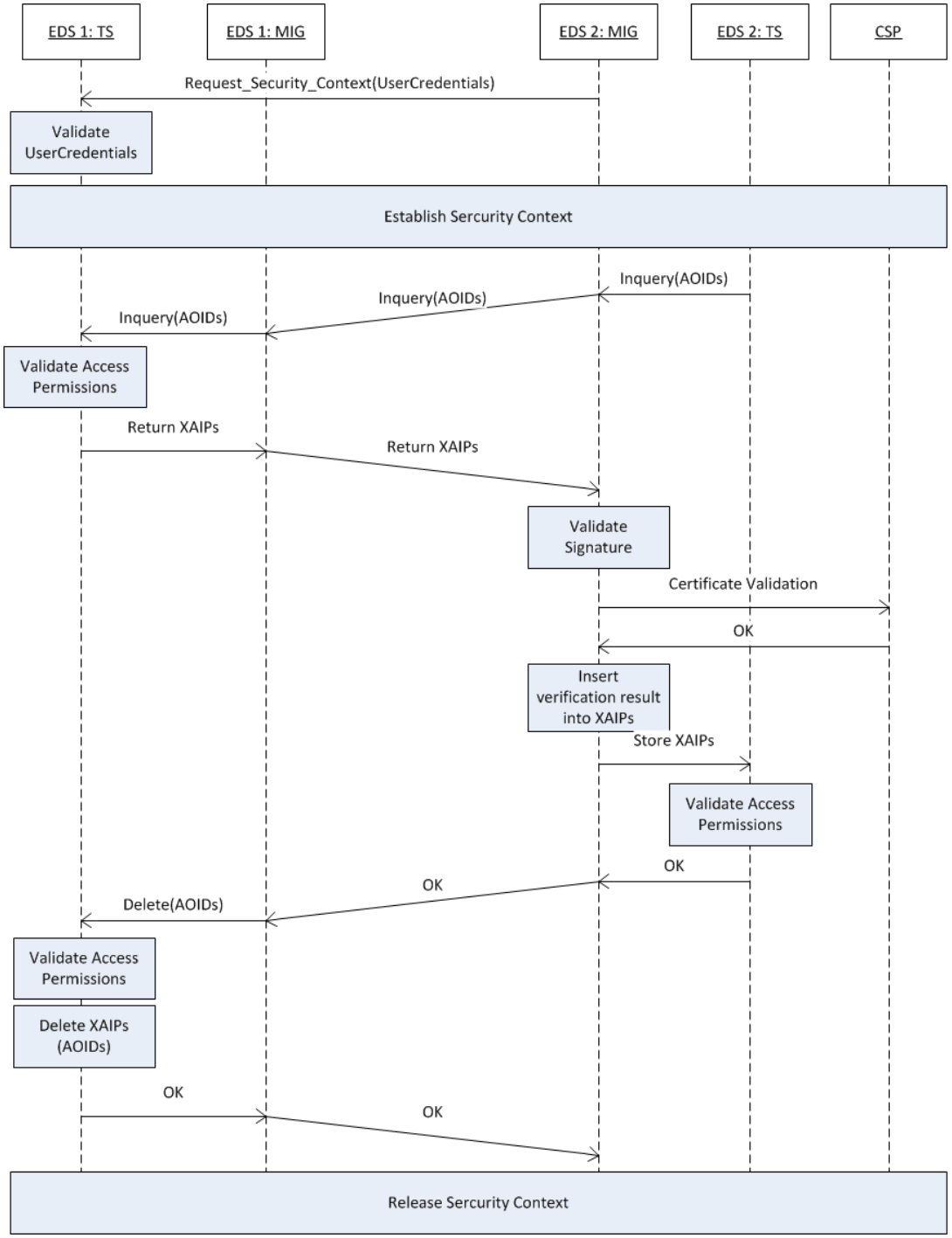


Figure 35: Document migration from EDS 1 (provider A) to EDS 2 (provider B)

Both EDS are modeled as two components: The migration interface (MIG), and the tenant storage (TS). AOID abbreviates Archive Object Identifier. The diagram has been derived from the message sequence charts for retrieval, archiving, and deletion as given in (19). Since the architecture described in this document is more detailed than the one given for the EDS, some necessary simplifications have been made. It illustrates how sequence charts can be used to describe success criteria for technical use cases (compare the associated row in the description table for “UC-Technical” above)

11 Acronyms

API	Application Programming Interface
BIT	Federal Office for Information Technology (Bundesstelle for Informationstechnik)
BITKOM	Federal Association of Information Technology Providers, Telecommunication and New Media (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien)
BMI	Federal Ministry of the Interior (Bundesinnnenministerium)
BMWi	Federal Ministry of Economics and Technology (Bundesministerium für Wirtschaft und Technology)
BSI	Federal Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik)
CCUCDG	Cloud Computing Use Case Discussion Group
CMS	Content Management System
CMSP	Complaint Management Service Provider
DMTF	Distributed Management Task Force
DOMEA	Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang
DVDV	Deutsche Verwaltungsdiensteverzeichnis
EDS	Electronic document safe
ELENA	Elektronisches Entgeltnachweisverfahren
ENISA	European Network and Information Security Agency
EU	European Union
G2Cloud	Government to Cloud business model
G2Cloud2B	Government to Cloud Business business model
G2Cloud2C	Government to Cloud to Citizen business model
G2Cloud2G	Government to Cloud to Government business model
IaaS	Infrastructure as a service
IMI	European Internal Market Information System
INPOL	Information System for Federal Polices (Informationssystem der Polizeien der Länder)
IP	Internetworking Protocol
ITIL	Information Technology Infrastructure Library
MIG	Migration Interface
MIG	Migration Interface
NIST	National Institute of Standards and Technology
PaaS	Platform as a service
PDA	Personal Digital Assistant
PDF	Portable Document Format
PSC	Point of Single Contact
RA	Responsible Administration
REST	Representational State Transfer
SaaS	Software as a service
SAJACC	Standards Acceleration to Jumpstart Adoption of Cloud Computing
SGCC	Study Group on Cloud Computing
SLA	Service level agreement
SLA	Service Level Agreement
SLO	Service Level Objective
SME	Small or Medium Enterprise
SMS	Short Message Service
SOA	Service Oriented Architecture
UML	Unified modelling language
VM	Virtual Machine
VPN	Virtual Private Network
XAIP	XML Archival Information Package
XÖV	XML for Public Administration (XML in der öffentlichen Verwaltung)
AOID	Archive Object Identifier
TS	Tennant Storage

12 Glossary

English	German	Explanation
Administrative district	Landkreis	Administrative unit on municipal level comprising usually one city (or several neighbored cities) and it's (their) rural proximity.
Administrative procedure	Fachverfahren	Procedure to implement a core duty of a public administration (e.g., tax computation). Usually supported by a **public sector software application**,
Agency under public law	Anstalt des öffentlichen Rechts	Public agency to realize cooperation on federal state level
Basic Protection Catalogs	Grundschutzkataloge	Security guidelines provided by the Federal Office for Security in Information Technology (12).
Data protection official	Datenschutzbeauftragter	Official responsible to validate and enforce data privacy regulations. Data protection officials are established on governmental, federal, and municipal level. Additionally, enterprises (and administrations) exceeding a certain size are entitled to establish a data protection officer.
Federal Council of Germany	Bundesrat	One of the two houses of the German parliament
Federal government	Bundesregierung	General German government
Federal Office for Security in Information Technology	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Federal office responsible to provide guidelines and technical specification for security related procedures. The BSI provides in particular the so-called **Baseline Protection Catalogs** (12) comprising a comprehensive list of threads and countermeasures. Although the BSI addresses public and private sector institutions as well, these catalogs are mandatory for the public sector.
Federal state government	Landesregierung	Government on federal state level
German Federal Parliament	Bundestag	One of the two houses of the German parliament
German government service repository	Deutsches Verwaltungsdiensteverzeichnis (DVDV)	Shared repository providing information about available public services that is designed and operated by the German Central IT-Department
Government agency	Behörde, Regierungsstelle	
Governmental public guarantee obligation	Gewährträgerhaftung des Staats	Guarantee that governmental duties and functions are continued independent of the state of the current responsible administrations.
Municipal special purpose association	Kommunaler Zweckverband	Cooperation under public law for a specific purpose (e.g., to provide IT services for several administrations) on municipal level.
Public Sector Software Application	Anwendung für Fachverfahren	Software to implement electronic support for an **administrative procedure**.
Public sector service	Verwaltungsleistung	Service provided by a government agency.
Resident's administration	Einwohnerwesen	Comprises tasks such as citizen registration, issuing of identity related documents, etc.
State office	Landesbetrieb	Specific office under public law to provide specific services to an administration (e.g., IT services) on federal level.

State treaty	Staatsvertrag	Treaty between German federal states

13 References

1. **Microsoft; Brow, Gregg; Jahromi, Babak.** *Use Cases for Cloud Computing.* s.l. : Microsoft, September 2010.

2. **National Institute of Standards and Technology.** *Cloud System Use Cases (draft).* 2010.

3. **Distributed Management Task Force.** *Use Cases and Interactions for Managing Clouds - A White Paper from the Open Cloud Standards Incubator.* s.l. : DMTF, June 2010. DSP-IS0103.

4. **Cloud Computing Use Case Discussion Group.** *Cloud Computing Use Cases - White Paper.* [Hrsg.] cloudusecases.org. July 2010.

5. **Mell, Peter und Grance, Timothy.** *The NIST Definition of Cloud Computing.* s.l. : NIST, July 2009.

6. —. The NIST Definition of Cloud Computing (Draft). [Online] January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf. Special Publication 800-145.

7. **Distributed Management Task Force.** *Interoperable Clouds - A White Paper from the Open Cloud Standards Incubator.* [Hrsg.] DMTF. November 2009. DSP-IS0101.

8. —. *Architecture for Managing Clouds - A White Paper from the Open Cloud Standards Incubator.* [Hrsg.] DMTF. June 2010. DSP-IS0102.

9. **opencloudmanifesto.org.** Open Cloud Manifesto. [Online] 2009. http://www.opencloudmanifesto.org/.

10. **Cockburn, Alistair.** *Writing Effective Use Cases.* s.l. : Addison-Wesley Professional, 2000.

11. **Badger, Lee und Grance, Timothy.** *Standards Acceleration to Jumpstart Adoption of Cloud Computing.* [Powerpoint presentation] [Hrsg.] NIST. May 2010.

12. **Catteddu, Daniele.** Security & Ressilience in Governmental Clouds. *www.enisa.europa.eu.* [Online] 2011. http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

13. **BSI - Federal Office for Security in Information Technology.** IT-Grundschutz International. [Online] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html?https=1&https=1&nsc=true.

14. **The European Parliament and the Council of the European Union.** Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. [Online] 12 December 2006. [Cited: 31 August 2009.] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT.

15. **COMMISSION OF THE EUROPEAN COMMUNITIES.** *HANDBOOK ON IMPLEMENTATION OF THE SERVICES DIRECTIVE.* Luxembourg : Office for Official Publications of the European Communities, 2007.

16. **European Commission.** Internal Market Information System - IMI. [Online] 2009. [Cited: 31 August 2009.] http://ec.europa.eu/internal_market/imi-net/index_en.html.

17. **Ignacio Blanquer (Ed).** *D4.1 – User Community Requirements – First Release 1.4.* Venus-C: Virtual multidisciplinary EnviroNments USing Cloud Infrastructures. September 2010.

18. **European Network and Information Security Agency (ENISA).** *Cloud Computing Risk Assessment.* 2009. avail. at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

19. —. *Security and Resilience in Governmental Clouds.* 2011. avail. at http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

20. **BSI - Federal Office for Security in Information Technology.** BSI Technical Guideline 03125: Preservation of Evidence of Cryptographically Signed Document. [Online] https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03125/BSITR03125.html.

21. **Breitenstrom, Christian, Brunzel, Marco und Klessmann, Jens.** *Elektronische Safes für Daten und Documente.* Fraunhofer FOKUS. Berlin : s.n., 2008. http://www.fokus.fraunhofer.de/de/elan/_docs/_hpp-gruppe/esafe_white-paper_081219.pdf.

22. **Steffens, Petra.** *Entwicklung von Prozessketten zwischeen Wirtschaft und Verwaltung: informations- und Meldepflichten von Arbeitgebern.* Kaiserslautern : s.n., 2009. http://www.fokus.fraunhofer.de/de/elan/_docs/machbarkeitsstudie-los3_090330.pdf.

23. **Deussen, Peter H., Strick, Linda und Peters, Johannes.** *Cloud Computing für die öffentliche Verwaltung.* [Hrsg.] ISPRAT. Berlin : s.n., November 2010. ISPRAT-Studie.

24. **BSI - Federal Office for Security in Information Technology.** *BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter.* s.l. : Bundesamt für Sicherheit in der Informationstechnologie, 2010.

25. **Fraunhofer FOKUS.** *Cloud-Computing in der öffentlichen Verwaltung - Chancen und Herausforderungen dynamischer IT-Dienstleistungen.* Berlin : Fraunhofer FOKUS, 2010.

26. **BMWi.** *Aktionsprogramm Cloud Computing.* s.l. : BMWi, 2010.

27. **Bitkom.** *Cloud Computing - Was Entscheider wissen müssen.* s.l. : Bitkom, 2010.

28. **Vitako.** *Cloud Computing - Entdecke die Möglichkeiten.* 2010. Vitako Aktuell.

29. **European Commission.** *The Future of Cloud Computing - Opportunities For European Cloud Computing Beyond 2010.* [Hrsg.] European Commission - Expert Group Report. s.l. : European Commission, 2010. European Commission - Expert Group Report.

30. **Bundesstelle für Informationstechnik - BIT.** Das Deutsche Verwaltungsdiensteverzeichnis (DVDV). [Online] BIT. http://www.bit.bund.de/BIT/DE/Zentrale__Dienste/DVDV/.

31. **Microsoft.** Open Data Protocol. [Online] 2011. http://www.odata.org.