Mulilateral Privacy in Clouds: Requirements for Use in Industry

Ina Schiering
Ostfalia University of Applied Science
Wolfenbüttel, Germany

Markus Hansen
Independent Centre for Privacy Protection Schleswig-Holstein
Kiel, Germany

IFIP Summerschool: Privacy and Identity Management for Life, Nice, September 10th, 2009
Cloud Services

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements

Methods

- Dynamically utilisable, scalable IT services
- Use of virtualisation and scalability
The different *interacting partners* in a cloud environment are

- Cloud Users
- Cloud Providers
- Resource Owners
Cloud User

Introduction
- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements

Methods

• Uses a cloud service
• A company is e.g. a cloud user
Cloud services are offered by cloud providers

Ina Schiering, Markus Hansen
Resource Owner

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements
- Methods

- Resource Owner is an interacting party who owns resources
Types of Cloud Services

Cloud services are distinguished concerning the complexity of the technology stack they deliver.

- Types of cloud services are:
  - **IaaS** - Infrastructure as a Service
  - **PaaS** - Platform as a Service
  - **SaaS** - Software as a Service
Infrastructure as a Service

- storage
- compute
- printing services
Platform as a Service

- Resources and infrastructure software as web servers, data bases, etc. (e.g. LAMP-Stack)
Software as a Service

- Software for complex processes e.g.
  - Email,
  - ERP (Enterprise Resource Planning),
  - CRM (Customer Relationship Management)
  - ECM (Enterprise Content Management)
Types of Clouds

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements
- Methods

Cloud services are also distinguished concerning where the cloud service is situated:

- Internal clouds
- External clouds
- Hybrid clouds
• Cloud user, cloud provider and resource owner are the same instance
External Clouds

Introduction
- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements
- Methods

- Cloud services offered by an external supplier
- All physical resources are out of reach of the cloud user
Hybrid Clouds

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy

Requirements

Methods

- Mixture of internal and external cloud providers
Interacting partners in a cloud can be visualized as a finite, directed, cycle-free graph:

- **Vertices** - Interacting partners
- **Edges**
  - From cloud provider to cloud user
  - From resource owner resp. cloud provider to another cloud provider
Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements

Methods

Interacting partners in a cloud can be visualized as a finite, directed, cycle-free graph:
Cloud Network - Special Nodes

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements

Methods

Cloud user:
- Vertex without successor

Resource owner:
- Vertex without predecessor
Cloud Subnet

Introduction
- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements

Methods

For each **cloud user** at a certain **point in time** the **cloud subnet** is the sub-graph induced by the

- the cloud user,
- all cloud providers and
- all resource owners

that are utilized to provide the cloud service to the specified cloud user.
Cloud Subnet

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- **Graph Representation**
  - Reasons and Risks
  - Multilateral Privacy Requirements

Ina Schiering, Markus Hansen
Cloud Subnet

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- **Graph Representation**
- Reasons and Risks
- Multilateral Privacy

Ina Schiering, Markus Hansen
Why to use cloud services?

Reasons for cloud users:

- limited IT know-how
- limited IT investment
- interesting service levels difficult to realise
  - mirroring over different physical sites
  - off-site backup
  - high availability of the computing platform
Why to use cloud services?

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements
- Methods

Reasons for cloud users:

- realisation of complex processes
  - Email
  - CRM - Customer Relationship Management
  - ECM - Enterprise Content Management
  - ERP - Enterprise Resource Planning
Risks of cloud services?

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy Requirements
- Methods

Cloud User needs legal warranties concerning

- security
- data privacy

since person-related data are operated not only from the cloud provider but from the whole cloud subnet at any point in time.
Multilateral Security

Allows all parties of an interaction

- to express their security objectives
- recognizing conflicting objectives
- negotiating compromises
- enforcing objectives within the scope of the compromise
- with no party taking precedence over another.

Mechanisms of effective control are needed.
Multilateral Privacy

Introduction

- Interacting Partners
- Types of Cloud Services
- Types of Clouds
- Graph Representation
- Reasons and Risks
- Multilateral Privacy

Requirements

Methods

Allows all parties of an interaction

- to express their privacy objectives
- with no party taking precedence over another.

Mechanisms of effective control are needed.
Cloud Requirements

What sort of requirements?
- Functional Requirements
- Non-Functional Requirements

Whose requirements?
- Cloud user
- Cloud provider / resource owner
Introduction

Requirements

- Functional
- Non-Functional
- Cloud User
- Cloud Provider

Methods

**IaaS**
- Type and clock rate of the CPU
- Amount of memory, disk space

**SaaS**
- E.g. collaborative work on documents
- Search options for data stored
Non-Functional Requirements

Introduction

Requirements

- Functional
- Non-Functional
- Cloud User
- Cloud Provider

Methods

Operational Requirements

- Start, stop, configure the service
- Automatic provisioning

Service Level Agreements (SLA)

- Availability, reliability, scalability
- Data integrity, privacy, access control
- Legal regulations
## Legal Regulations

### Introduction

### Requirements
- Functional
- **Non-Functional**
  - Cloud User
  - Cloud Provider

### Methods

- Data Protection Directive
- E-Privacy Directive
- EuroSOX
Any person-related data has to be processed

- fairly and lawfully, **for limited purpose**
- adequate, relevant, not excessive, **accurate**
- not be kept longer than necessary
- processed in accordance with the subjects rights
- **secure**
In cloud environments important:

- transfer of personal information to countries outside the EU providing an adequate level of privacy protection

- Transfer of data to the USA: Safe Harbour Agreement
SOX, EuroSOX

**SOX (Sarbanes-Oxley Act):** reaction to accounting scandals e.g. Enron, Worldcom

- Demands e.g. an internal control system for corporations in the US and all subsidiaries

**EuroSOX:** similar requirements have evolved in the EU

- Resulting e.g. in the german law BilMoG (Bilanzmodernisierungsgesetz)
Central prerequisites for compliance with these regulations are the following

- Transparent and documented business processes
- Transparent and documented IT environment
- Identity Management
- Based on the above control objectives can be formulated and checked by an internal control system
Requirements of Cloud Providers

All the requirements named above are mainly requirements of the cloud users.

Cloud providers, resource owners have also requirements they need to impose:

- **Operational requirements**: monitoring, measuring, reporting and billing for services.
- **Comply with legal regulations**, e.g. export control regulations.
What are the measures and means to realize the requirements of all interacting partners in the cloud?

- **Federated Identity Management** as a basis to realise access control and reporting.
- **Cloud Interfaces** as a cloud service should be started dynamically in an automated way.
- **Certification and Control** to check that the requirements are fulfilled
Cloud Interfaces

Interfaces for cloud services are differentiated according to types of cloud services

- **SaaS**: Often a web interface (Salesforce, Gmail) or a special user client is used
- **IaaS, PaaS**: provider specific API, examples for provider APIs are:
  - Amazon EC2 API,
  - Sun Cloud API
  - ...

Introduction
Requirements
Methods
- Federated Identity Management
- Cloud Interfaces
- Certification and Control
Cloud Interfaces

Notation for the APIs based on
- **XML**
- **JSON** (JavaScript Object Notation)

Type of information
- **Functional requirements** (mainly)
Risks of Present Cloud APIs

Introduction
Requirements
Methods

Non-functional requirements:
- compliance
- availability
- scalability
- privacy
- data security

Vendor lock-in:
- Dynamic change of cloud provider implies change of API in application
Standardisation initiatives start based on the cloud APIs in industry for IaaS:

**OCCI-WG** (Open Cloud Computing Interface Working Group)

- Start of API for IaaS based on cloud APIs in industry
- Non-functional requirements based on use cases
- Relies on RESERVOIR architecture
Requirements in APIs

Introduction

Requirements

Methods

- Federated Identity Management
- Cloud Interfaces
- Certification and Control

- **Format for data interchange** as e.g. XML, JSON

- **Categories of requirements:**
  - Low, medium, high availability instead of 93.5%

- **Categories defined in the documentation**

- **Automated check**
Automated Check of Requirements

There are 3 scenarios:

1. **Cloud user** requests a service

2. **Standard Requirements**
   Cloud provider provides a cloud service where a typical requirements is met

3. **Cloud provider, resource owner** is added to the cloud network
1. Cloud User Requests a Service

- Cloud User requests a requirement from the cloud provider
- Cloud provider requests if all direct predecessors in the cloud network support the requirement
- Inductively repeat that step until resource owners are reached
- Resource Owners could at least answer to the request
1. Cloud User Requests a Service

Introduction
Requirements
Methods

- Federated Identity Management
- Cloud Interfaces
- Certification and Control
1. Cloud User Requests a Service

Introduction

Requirements

Methods

- Federated Identity Management
- **Cloud Interfaces**
- Certification and Control

Ina Schiering, Markus Hansen
1. Cloud User Requests a Service (2)

Introduction
Requirements
Methods
- Federated Identity Management
- Cloud Interfaces
- Certification and Control

- Answers are acknowledge, non-acknowledge
- Cloud Providers derive their answer from the answers of all direct predecessors
- Cloud user receives an acknowledge or non-acknowledge message
1. Cloud User Requests a Service (2)

Introduction
Requirements
Methods
- Federated Identity Management
- Cloud Interfaces
- Certification and Control
1. Cloud User Requests a Service (2)

**Introduction**

**Requirements**

**Methods**

- Federated Identity Management
- **Cloud Interfaces**
- Certification and Control
Introduction

Requirements

Methods

- Federated Identity Management
- Cloud Interfaces
- Certification and Control
1. Cloud User Requests a Service (2)

Introduction

Requirements

Methods

- Federated Identity Management
- Cloud Interfaces
- Certification and Control
1. Cloud User Requests a Service (2)

Introduction
Requirements
Methods

- Federated Identity Management
- **Cloud Interfaces**
- Certification and Control
2. Standard Requirements

- For standard requirements e.g.
  - Data is only stored and processed in the EU
  - High availability
- Cloud Providers can offer special cloud services where this requirement is already met

Introduction

Requirements

Methods
- Federated Identity Management
- Cloud Interfaces
- Certification and Control
3. Cloud Provider, Resource Owner is Added

- Cloud provider, resource owner express the requirements they have when added to a cloud network
- These requirements are propagated through the cloud network as is done with user requirements before answering the request of the cloud user
Every interacting partner pretends to fulfil security and privacy requirements.

But how can cloud users be sure?
Certification and Control

Traditional Approach:
- Have a contract where requirements are stated (SLA)
- Control in a regular manner

Not feasible in a dynamic cloud environment

Alternative: Certifications
- Common Criteria
- ICPP Privacy Seal
Certificates

- Certificates can be handed through from resource owner and cloud provider to the cloud user
- Rely on trusted third parties instead of direct control

Open question: Can certification frameworks cope with dynamically interacting systems
Cloud services can be used for processing

- person-related and
- business-critical data
when appropriate

- Cloud APIs
- Certification mechanisms are used.
Thank you for your attention

Questions