Privacy and Identity Management in Europe for Life

Towards an Economic Valuation of Identity Management Enablers

Editors:	Sascha Koschinat (GUF) Gökhan Bal (GUF) Marvin Hegen (GUF) Kai Rannenberg (GUF)
Reviewer:	Hans Hedbom (KAU)
Identifier:	H6.1.2
Type:	Heartbeat
Class:	Public
Date:	June 6, 2010

Abstract

In the economy at large, there are inefficient and ineffective business processes in every industry. The current untapped potential of Identity Management (IdM) related Customer Data Assets and Functional Capabilities in many companies (e.g. Mobile Communication Providers (MCPs)) could help Service Providers (enterprises, and government) to interact with End Customers (consumers, and citizens) in more efficient and effective ways than they can today. Therefore these IdM Assets and Capabilities should not be seen as by-products of service provisioning, but rather as bundles of core-products, here called as IdM Enablers. The "IdM Enabler Concept" has emerged as a way to describe these IdM Assets and Capabilities. This document aims to identify potential IdM Assets and Capabilities of adequate companies that could be bundled to IdM Enablers and utilized to enable and provide new Value Added Services (VAS) to End Customers and Service Providers considering End Customers' Privacy. The identified IdM Assets, Capabilities, and Enablers will be analysed in order to prepare a way for an economic valuation of the "Identity Business" potentials.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n^{o} 216483 for the project PrimeLife.

SEVENTH FRAMEWORK PROGRAMME

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

Disclaimer: *The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.* *Copyright 2010 by Johann Wolfgang Goethe - Universität Frankfurt am Main (GUF).*

List of Contributors

This deliverable has been authored by PrimeLife partner organisation GUF. The following list presents the contributors for the individual parts of this deliverable.

Chapter	**Author(s)**
Introduction	Sascha Koschinat (GUF)
Identity Management (IdM) for an Identity driven Economy	Sascha Koschinat (GUF)
Identity Management (IdM) related Data Assets	Marvin Hegen (GUF)
Identity Management (IdM) related Functional Capabilities	Gökhan Bal (GUF)
Use Case Scenarios	Gökhan Bal (GUF)
Aim of the Heartbeat	Kai Rannenberg (GUF)

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the economy at large, there are inefficient and ineffective business processes in every industry. The current untapped potential of Identity Management (IdM) related Customer Data Assets and Functional Capabilities in many companies (e.g. Mobile Communication Providers (MCPs)) could help Service Providers (enterprises, and government) to interact with End Customers (consumers, and citizens) in more efficient and effective ways than they can today. Therefore these IdM Assets and Capabilities should not be seen as by-products of service provisioning, but rather as bundles of core-products, here called as IdM Enablers. The "IdM Enabler Concept" has emerged as a way to describe these IdM Assets and Capabilities. This document aims to identify potential IdM Assets and Capabilities of adequate companies that could be bundled to IdM Enablers and utilized to enable and provide new Value Added Services (VAS) to End Customers and Service Providers considering End Customers' Privacy. The identified IdM Assets, Capabilities, and Enablers will be analysed in order to prepare a way for an economic valuation of the "Identity Business" potentials.

Beginning with the IdM Enabler Concept in Chapter 2, this Heartbeat initially addresses potential IdM Service Providers of an "Identity driven Economy", such as IdM and Privacy enhancing Technology (PET) Providers, Internet Service Providers (ISPs), as well as Mobile Communication Providers (MCPs). While Chapter 3 examines the IdM Data Assets, Chapter 4 lists and describes in detail a collection of IdM related Functional Capabilities necessary in order to process and monetize the IdM Data Assets. To highlight the value and significance of IdM Data Assets and Functional Capabilities, relevant use case scenarios are required that are outlined in Chapter 5 and which aim to show implementations that on the one hand provide added values to services provided by Service Providers and on the other hand consider important Privacy principles.

Chapter 2

Identity Management (IdM) for an Identity driven Economy

Customer data, like account, attribute, authorization, authentication, and access information of an (digital) Identity is a key Identity Management (IdM) related asset for a value added Identity driven Economy. The management of Data Assets in business transactions between different market actors includes typically the creation, activation, storage, processing, delivery, deactivation, and deletion of this information by IdM related functions.

For this purpose IdM Data Assets need to be utilized in business transactions by IdM Functional Capabilities under certain technical, social, legal, and economic requirements and conditions. Particularly the Privacy needs and rights of the involved actors in each business transaction need to be considered and fulfilled by Privacy enhancing Technologies (PETs).

The “IdM Enabler Concept” has emerged as a way to describe these IdM Assets & Capabilities. This concept will be described in the following section.

2.1 Identity Management (IdM) Enabler Concept

The provisioning of IdM related Data Assets and Functional Capabilities by an IdM Service Provider to other actors of an Identity driven Economy can be seen as an IdM Service, that the IdM Service Provider offers to its IdM Customers (Service Providers, End Customers). According to that, an IdM Service consists of one or more bundles of the two major components IdM Data Assets and IdM Functional Capabilities. A respective single bundle of these two components will here be referred to as an IdM Enabler. Thus an IdM Service in turn typically consists of one or more IdM Enablers.

IdM Enablers consist of a valuable combination of IdM related Data Assets and Functional Capabilities. Data Assets in this circumstance are attributes of a user identity (End Customers, Service Providers) like name, place of birth, account details, and so forth, whereas Functional Capabilities are those functions that make IdM possible. The combination of both IdM related Functional Capabilities and Identity related Data Assets form an Enabler, which could be seen as a driver for a specific IdM Service.

By utilizing these IdM Enablers for their own purposes the IdM Customers can realize significant values or enable new Value Added Services (VAS). The value that the customers of the IdM Service Provider gain by utilizing its IdM Enablers will here be referred to as IdM enabled Value, and the new Value Added Services as IdM enabled Services.

The above mentioned IdM related concept is here referred to as the IdM Enabler Concept.

2.2 Identity Management (IdM) Service Providers

A well-balanced interplay of IdM Data Assets and Functional Capabilities for each business transaction could enable significant added values to the involved actors of an Identity driven Economy. Service Providers could enable new Value Added Services; improve the value of their existing services for their customers, and the efficiency and effectiveness of their business processes by analyzing and processing customer data under fulfilment with technical and economical conditions and compliance with legal and social Privacy requirements. End Customers could benefit from an increased supply of value added, personalized and low priced or free services in exchange for providing their personal data under compliance of their legal Privacy rights and individual social needs based on user defined policies.

This highly intertwined Identity driven Economy is based on an appropriate level of trust between the respective actors. This requires a well-balanced provision of IdM Assets and utilization of IdM Capabilities (e.g. Privacy enhanced Data Processing Capabilities) to assure the confidentiality, authenticity, integrity, and availability in the respective interactions. This is especially important for a decrease of risks and an increase of trust between the market actors compared to the current market situation and procedures of collecting, processing, and provisioning customer data for predominantly marketing and advertising purposes. Which current or future market players are in the position to enable the respective trust relationship is still an open question. Some of the current market actors are in a generally good position for this. And some of these in turn seem to be in a relative better position than others.

2.2.1 Internet Service Providers (ISPs)

Internet Service Providers (ISPs) like Google, Apple, Amazon, or Facebook have huge customer bases and a wide range of available Basic-, Communication-, Context-, Content-, Identification-, Device-, and/or Finance Data Assets about their customers. These Service Providers have early realized the enormous economic value of their customer data and usually operate on a highly scalable, two-sided, platform-based business model. On the one side of their business model they provide low priced or even free services to their customers in order to collect as much information as possible about each customer, and in order to provide this information on the other side of their business model to third parties for further revenue streams, predominantly Marketing & Advertising Service Providers.

Even if the ISPs are more or less successful with their business models, in consideration of:

- the vast customer rejection of behavioural advertising,
- the mostly missing consideration of customer participation in their business models,
- the often inadequate launch and marketing strategies to justify their two-sided service models and to generate customer acceptance,
- and the unclear and intransparent consideration of the customers' Privacy needs,

the Customer Data Assets of these ISPs are often deemed to be voyeuristic, temporary, fragmented, and speculative.

Normally ISPs offer very limited platforms to support an Identity driven Economy with IdM related Functional Capabilities and can be regarded more as specialized providers of Customer Data Assets. The advertising business models of ISPs are responsible for Trade Offs between End Customers' Privacy requirements and advertising profits based on user profiling. Therefore ISPs do not have strong incentives to become specialized IdM Service Providers with respect to Privacy issues. In many cases the provisioning of Customer Data Assets is the major or even only source of revenue in their business models.

2.2.2 Identity Management (IdM) Providers

Specialized IdM Providers like VeriSign, Payment Network AG, OAuth, OpenID, Schufa, Idemix, U-Prove, or SIZCHIP provide a multiplicity of different IdM related Functional Capabilities like Account-, Attribute-, Authentication-, Authorization-, and Policy Functions that can be used by Service Providers (e.g. Online Shops) and End Customers. Whereas the majority of IdM related functionalities (e.g. End Customer data processing functionalities) is provided commercially with costs to Service Providers, most of the provided IdM related functionalities (e.g. Privacy enhancing functionalities) are available to End Customers for free.

The available IdM Solutions are normally of high expediency for their individual purposes, but very limited in their range of applicability in business transactions. Therefore several of these solutions need to be integrated by Service Providers or End Customers into a single and common business transaction in order to completely support all of the involved IdM related processes.

This often results in a lack of interoperability that makes it difficult to:

- interplay comprehensively between different IdM solutions,
- interplay comprehensively between the Service Providers' or End Customers' systems,
- map coherently the business logic in the respective business transactions.

Thus, many IdM Solutions receive only weak acceptance by Service Providers and End Customers because of their high complexity, low usability, and high integration costs.

There are also several legal and business related conditions that often complicate a complete implementation of IdM functionalities in business transactions, especially with regard to Privacy enhancing IdM functionalities. In many business transactions there needs to be at least one trustable third party that could ensure the confidentiality, authenticity, integrity, and availability of these business transactions and their involved actors. Therefore this trusted party needs to collect, process, store, and forward the relevant data of each business transaction until there are no legal claims between the involved actors and even for a certain time afterwards. But many Privacy enhancing functionalities prevent the needed business transaction data from that.

Additionally, the currently provided IdM platforms and services are in most cases very limited to support comprehensively an Identity driven Economy. Providers of these platforms and services can more be seen as specialized providers of IdM functionalities and not of IdM related Data Assets.

2.2.3 Mobile Communication Providers (MCPs)

Mobile Communication Providers (MCPs) like Vodafone, T-Mobile, Orange, Telefonica, Telecom Italia, O2, KPN Mobile, or Bouygues provide a wide range of Voice-, Messaging-, Data-, and Broadband Services to nearly every End Customer of an Identity driven Economy over a simple one-sided business model with the End Customers as their only revenue source. Thereby resides an enormous amount of Customer Data Assets as a by-product of the current MCPs' one-sided service provision. Owing to different circumstances, MCPs have not only more but also more valuable Customer Data Assets concentrated in their databases than other businesses. By being legally obligated and economical appropriate to collect and process a wide and deep range of Basic, Communication-, Context-, Content-, Identification-, Device-, and Finance Customer Data Assets, it are above all the unique or much more pronounced differentiating factors of the Mobile Economy to the pure IP-based, Fixed Line or Offline Economy that enables MCPs to extract even more valuable information about End Customers than other businesses.

The higher ubiquity, reachability, security, convenience, locatability, connectivity, and identifiability enabled by the networks and infrastructures of MCPs, contribute to the unique and relatively good position of the MCPs for the potential role of an IdM Service Provider. The high degree of End Customers' trust in MCPs concerning the protection of their personal data and respecting their Privacy is based on the absence of the pressure to be dependent on selling customer information for more revenue streams than from their current core businesses. MCPs have strong one-sided core business models and act on a high regulated and controlled market. In combination with the MCPs internal applied methods and functionalities to process their customer data, MCPs have predominantly well fulfilled conditions to become trusted custodians of their customers' Identities.

However, in order to help Service Providers and End Customers interact in more efficient and effective ways than they do today, it is essential for MCPs to create open and standardized platforms. Therefore MCPs' Customer Data Assets need to be reorganized, extracted, and bundled from multiple in-house databases. Functional Capabilities need to be established, implemented in-house, and made available for third party applications or services by standardized APIs to provide controlled access to the MCPs' Customer Data Assets or context relevant representations of them. Large parts of the IdM related infrastructure of MCPs need to be restructured and renewed before they can be used for such IdM purposes. Privacy enhancing IdM functionalities and protocols need to be established and implemented for every kind of supported or enabled business transaction. A clear and transparent consideration of the End Customers' Privacy needs to be implemented to generate customer acceptance. Particularly legal aspects need to be considered and implemented into the whole organizational and operational business and technology infrastructure of the MCP. Last but not least, the End Customers' participation must be considered to generate customer incentives and to justify such a new two-sided business model of MCPs in general.

2.3 Mobile Communication Provider (MCP) operated Identity Management (IdM) Service Provider

This section describes the utilization of IdM related Customer Data Assets and Functional Capabilities in order to improve business processes or services provided to End Customers by third party Service Providers.

In this case a MCP operated IdM Service Provider operates on a two-sided business model. On the End Customer (downstream) side the MCP uses its core business IT and network infrastructure to provide end customers with Voice, Messaging, Data, and Broadband Services. Thereby, the MCP generates a first solid revenue stream accompanied with a wide and in-depth access to its customers' data (Assets). The available customer data of a typical MCP can be divided into the following seven categories of Customer Data Assets:

1. Basic Data
2. Identification Data
3. Communication Data

4. Content Data
5. Context Data
6. Financial Data
7. Device Data

These categories will be described and discussed in detail in the following Chapter 3.

In addition to Customer Data Assets, the MCP can access a huge set of different IdM related functions to process all its customer data for in-house purposes. Through an open platform and standardized APIs, the MCP can provide these Functional Capabilities to third party Service Providers in order to enrich or improve their processes or services with more valuable information about End Customers (Assets). Furthermore, Service Providers can enable IdM related business processes and services even without requesting any additional data from the End Customers. In doing so, the MCP generates an additional revenue stream on the Service Provider (upstream) side of its two-sided business model. The IdM related Functional Capabilities which a MCP typically provides, can be classified to the following five categories of IdM Functional Capabilities:

1. Account Functions
2. Attribute Functions
3. Authentication Functions
4. Authorisation Functions
5. Policy Functions

These categories will be described in detail in Chapter 4.

Service Providers can request Data Assets and/or Functional Capabilities through a provided IdM Platform by the MCP in order to integrate and utilize them in their own business processes and to improve their services for End Customers or even to enable new services that otherwise could not be provided. Thus, Service Providers significantly increase the efficiency and effectiveness of their IdM related business processes, improve their services for End Customers qualitatively and quantitatively and gain additional flexibilities and options for current and future business operations and decisions.

Not only Service Providers can benefit from these IdM enabled Added Values. End Customers could also profit from:

- an increased choice of value added services, personalized products or services under consideration of individual characteristics, needs, and contextual situations,
- free or reduced prices for products and services in exchange for personal data,
- a higher degree of security, enabled by the secure infrastructure of the MCP which supports its End Customer’s Identities and their personal information custodial in every IdM supported or enabled business transaction, and thus from
- an increased trust in business transactions with Service Providers and other End Customers that don’t know each other.

A key enabler to have End Customers providing their data for enabling IdM Value Added Services is a Customer data Portal (CDP). Provided through the IdM Platform, the CDP allows End Customers to control their personal data and to define individual Privacy policies for their particular circumstances and purposes (e.g. assigning different partial Identities to different services). If the MCP can successfully implement an adequate CDP, the above mentioned benefits are sufficient incentives for a critical mass of End Customers.

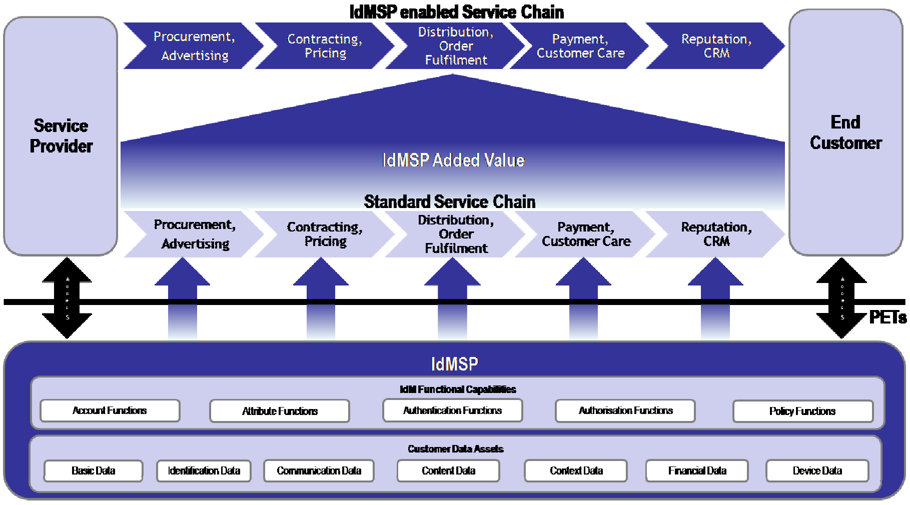

Figure 1: Concept of a Mobile Communication Provider (MCP) operated Identity Management (IdM) Service Provider (IdMSP)

Figure 1 illustrates the concept on a MCP operated IdM Service Provider for an exemplary E-Sales business transaction between a Service Provider and an End Customer. The Service Provider offers a common Internet E-Sales Service (e.g. Amazon Marketplace) to the End Customer. The service is shown in Figure 1 as Standard Service Chain which is subdivided in the five components:

1. Procurement & Advertising
2. Contracting & Pricing
3. Distribution & Order Fulfilment
4. Payment & Customer Care
5. Reputation & CRM

In each of these components different IdM related problems can be identified which influence the efficiency or effectiveness of the Service Providers' processes of service provisioning. For this purposes the IdM Service Provider offers its IdM related Customer Data Assets and Functional Capabilities through an open and standardized platform. The Service Provider can access this platform to request and utilize the Data Assets and/or Functional Capabilities to enhance and improve several of its Standard Service Chain components and processes of service provisioning. For this purpose the IdM Service Provider additionally offers a CDP to the End Customers, which enables them to control their data and to define individual data processing policies. So placed at its disposal the End Customer is empowered to control which Data Assets can be processed for and utilized by which Service Provider in which way and contextual situation.

An exemplary application of the MCP operated IdM Service Provider could be in the domain of Payment transactions. In many of these transactions one of the involved actors (Service Provider, End Customer) must perform efforts in advance. Either the End Customer has to pay before he gets the demanded service or the Service Provider delivers the service before it gets paid. So, one of these actors has to take the risk of losing the performed effort without getting any effort in return. Because of this risk many business transactions even don't come about. In the above mentioned concept the trusted IdM Service Provider could play the role of a mediator between both actors. Based on its knowledge of both sides the IdM Service Provider is able to increase the trust by bailing for the transaction partners. As a result business transactions that otherwise would not come about get enabled. This requires the IdM Service Provider to validate the Data Assets that it possesses about both sides and to provide respective results to the involved actors by utilizing IdM related Functional Capabilities.

There are some issues in the IdM Enabler Concept that have not been addressed or discussed at all. This type of model has Privacy problems or at least the potential for Privacy problems regarding concentration of user information at the MCP. There is also the question of the added value of the business model if a user decides to use multiple providers to “spread the risk” of data concentration. There are also potential lock-in effects which potentially the MCP likes but not the End Customers and Service Providers. These open problems will be addressed in future work.

Chapter 3

Identity Management (IdM) related Data Assets

In the past data was an unpleasant coefficient which occurred in the process of transactions. Data and its handling were seen as necessary expense factors, but not as key strategic assets. Today this way of thinking has completely changed. Customer data has become the maybe most important asset for each information- and communication-related company (e.g. Google).

Due to the rapidly growing amount of data each company produces and the need for more actual (or even realtime) customer information, terms like data quality and data governance gained more and more influence. Therefore, customer data has to be considered as corporate asset which can enable new (two-sided) services and business models.

3.1 Identity Management (IdM) related Data Assets in the context of PrimeLife

Individuals in the information society are in focus of PrimeLife research and, therefore, also the essential factors for this data asset study. In the context of PrimeLife data assets are not overall data used by companies for data mining or data management, but mostly personal data these companies gather from their customers or users.

Personal data is defined as „any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social Identity;“ [EUDA95]. In context of this work direct identification is accomplished with the help of identification data (Chapter 3.2.2), while indirect identification is based on combining and processing basic-, communication-, content-, context-, financial-, and device data (Chapter 3.2).

Personal data can be used to create user-profiles which are collections of data associated to a specific user. A profile can be understood as an explicit digital representation of a person`s Identity which can be a risk for that person`s Privacy.

3.2 Categories of Identity Management (IdM) related Data Assets

As described before IdM related Customer Data Assets in the context of this paper are always personal data. Based on an analysis of current data handling of influential IdM market players (e.g. Google, Amazon, Facebook, etc.) data attributes gathered from these players have been identified and categorized into seven categories of Customer Data Assets which are illustrated in Figure 2 and discussed in further detail in the next chapters. Essential research point was the identification of relevant user data for actual IdM-related business models in the internet economy. Different economic zones, regulation terms and legal restrictions played a minor part for this analysis.

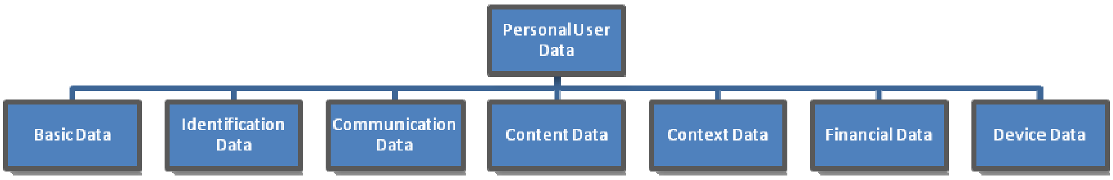

Figure 2: Categories of IdM related Customer Data Assets

3.2.1 Basic Data

The category of basic data includes reference data which describes a natural person and its properties (e.g. name, address, telephone number). Compared to personal data in general basic data excludes communication or interaction data.

The attributes belonging to other data categories may overlap with basic data attributes. In this cases the data attribute of the other category is used for a special, for this data category relevant, use case (e.g. E-Mail as identification data).

Name	Address	Contact info	Job/School	Other
First name	Street	Phone	Position	Citizenship
Last name	City / Zip	E-Mail	Address	Eye Colour
Title	Country	IM	Education	Size

Table 1: Example Basic Data

3.2.2 Identification Data

Identification data can be used to uniquely identify a person or a specific user [CUTL08]. This category includes data necessary for identification by user input like username/password combination, automatic identification on the basis of e.g. a phone number, and biometric identification by face recognition or fingerprint. One major aspect for the quality of identification data, and even the quality of a complete data set, is the possibility to uniquely identify a person. A name for example can be seen as weak identification data, because of the possibility of redundancies, while the passport number is unique and verified by a state authority.

Identification data	
Name	Passport Number
Cookies	Digital Signature
Username	Fingerprint
IP Address	Biometric Picture

Table 2: Example Identification Data

3.2.3 Content Data

Content is information and experience that may provide value for an end-user or audience in specific contexts. The value of content data is different in dependence to the content data consumer and its context. For one individual content (e.g. Newspaper Article) is informative and new, while another, which already knows the content, does not regard the content as information.

In this research we divided content data in user-generated content (e.g. Videos, Blogs, Docs, Presentations, etc.) and content users are interested in (e.g. Music, Videos, Books, Games, etc.). Both content types allow conclusions on user interests which makes them interesting for advertising purposes. While user generated content apparently is uploaded by the user itself, content the user is interested in is mostly logged from search queries, website usage patterns and content downloads.

User generated content	**Content users are interested in**
Photos	Movies / Videos / TV Series
Videos	Music
Blog-Posts	Websites
Docs, Presentations & Spreadsheets	Applications

Table 3: Example Content Data

3.2.4 Context Data

Context is any data that can be used to characterize the situation of an entity [DEYA01]. This includes any kind of data which can be used to characterize the relevant situation of a person, a place or any other object and their relationships among each other [KASP06, S. 151-152]. As shown in Figure 3 the user context can be separated in five categories.

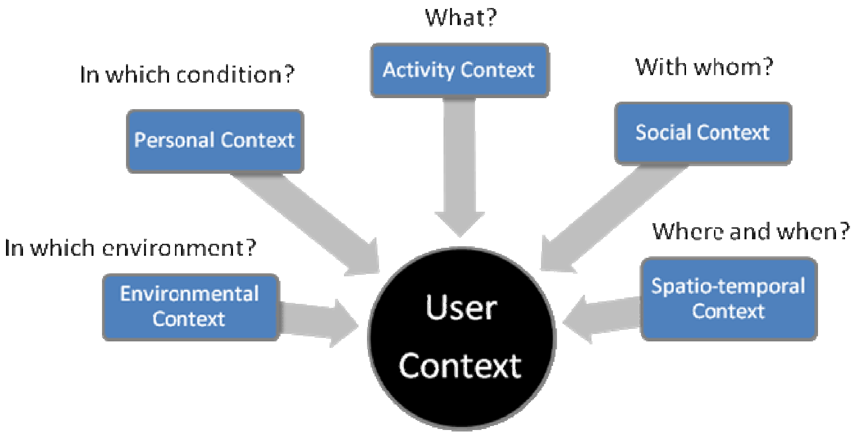

Figure 3: Categories of User Context

Context data is especially used in context aware services to personalize services and thus increase the usability and the value of it. Each additional context date can possibly increase the value of a service. For example a mobile friend finder application, which already uses a person's location and its relationships, anyhow could improve its user value by adding social context information about the user is interested in women or men. This effect is described in economic theory as diminishing marginal utility. If the service value is observed alone, a maximum of relevant context data seems to be desirable. But on the other hand a large amount of context data is contradictory to the principle of data minimisation and causes significant Privacy issues.

Environmental	Personal	Activity	Social / Relationships	Spatio-temporal
Temperature	Physical (pulse, blood pressure, weight)	Events	Co-workers	Location
Light	Mental (mood, expertise, angriness)	Tasks	Friends	Direction
Noise		Mobile Phone presence	Relatives	Time

Table 4: Example Context Data

3.2.5 Communication Data

Communication is a process of transferring information from one entity to another by imparting thoughts, opinions or information by speech, writing or signs [WIKI09a]. The category of communication data contains all data about communication processes as text & multimedia messages, voice communication, data transfer protocols and information about sender and receiver.

Text	Multimedia	Voice	Data transfer	Participants
E-Mails	MMS	Calls	Traffic	Sender
SMS	Video calls	Voicemail	Frequency	Receiver
Chats		Voice Messages	Size	

Table 5: Example Communication Data

3.2.6 Financial Data

This data category deals with the financial status and the credit worthiness of a user and how money is spent and budgeted. Data assets examined in the category of financial data are a user`s financial status, its payment information (credit card, bank account details) and its buying patterns. Besides this typical financial data, also data like place of residence etc. could be of interest with credit profiling: This shows a typical situation of overlapping data attributes.

Financial status	Credit Card	Bank account	Buying patterns
Income	Holder	Holder	Financial Transactions
Savings	Card type	Account number	Usage behaviour
Stock portfolio	Card number	Bank code	

Table 6: Example Financial Data

3.2.7 Device Data

In this research paper the definition of devices is restricted to information devices. This includes any machine or device that is usable for the purposes of computing, telecommunicating, reproducing, and presenting encoded information [WIKI09b]. Device data means specific information about the user`s device (e.g. the IMEI of a mobile phone).

Device Data	
Device and hardware Ids	Battery life information
Device type	Manufacturer (Brand)
OS	Memory information

Table 7: Example Device Data

3.3 Value and Quality of Identity Management (IdM) related Data Assets

For evaluation of data sets or specific data attributes it is necessary to differentiate between data of high and low quality. For example the name of a user is of higher quality if it was certified from a state authority (e.g. ID check for verification when concluding a mobile phone contract) compared to a name attribute gathered from free unverified text input field in an internet application.

Data quality is often referred to as correctness of data. Of course this is one major data quality aspect, because it has big impacts on the results of Data Mining, Customer Relationship Management or Advertising Campaigns. However, data correctness is just one element in a wide list of data quality dimensions in the literature [FISH09]. A much more relevant definition of quality is given by DIN 55350 which defines quality as a combination of characteristics regarding the usability of a unit for a defined purpose. Therefore, data is from high quality if it fits to the data consumer's requirement and also its context specific scope of applications [SATT09] [BATI06].

To evaluate the ability of each potential IdM Service Provider to act successful on the IdM-Market, we need to understand the value of their customer & network data assets for their data consumers, those who use these data assets. For a valuation of these assets we need to consider the key quality factors that influence the data value and that are important to the data consumers. To find these key quality factors it is necessary to consider in addition to the potential data consumers also their context specific scope of applications. Consider for example a data consumer which is interested in advertising campaigns: When is personal user data complete and thus of high value? The answer: It depends on the needs of the data consumer. If the data consumer is interested in a widespread anonym marketing campaign like bulk mails for example, the user data would be useful if it includes the address of a person. For another data consumer who is looking for a specific person or specific characteristics the same data would be incomplete or worthless. Instead of just analyzing the data attributes out of context, this complexity necessitates to do a business application or service specific valuation of IdM Data Assets [WANG96].

3.4 Privacy requirements for Identity Management (IdM) related Data Assets

"Users should always be aware of what data is being collected." [LANG01]

There are considerable Privacy issues in our data consuming internet economy. To put individuals (back) in control of their personal data is a major aspect of Prime as well as PrimeLife. In the meantime this urgent need for enhanced Privacy settings has been recognized by ISPs and MCPs all over the world. But currently available Privacy setting mechanisms are often just rudimental or complex to use. They are used as marketing instruments to compensate negative press reports about data abuse, but do not support comprehensive setting possibilities. Future IdM Services require differentiated Privacy mechanics in dependence to the affected Customer Data Assets, Functional Capabilities and data consumers. Even if Privacy settings also have extensive impacts on functions, services and maybe complete business cases they are always data-related and, therefore, need to be implemented in the layer of Data Assets in the IdM Enabler Concept.

The requirements for Privacy enhancing IdM Solutions collected during the Prime project can be re-used for this model [PRIM08, S. 20]:

- User control and consent
- Justifiable parties

- Data minimisation
- Policies and policy enforcement
- Human measure
- Multiple Identities and accountability

Users should be able to control which personal data are given to whom and for what purpose (user control and consent). Therefore, it is the user's task to trade off his Privacy against the value of a service by disclosing his data. For this decision it is necessary that the user is informed about which parties get access to his personal data (justifiable parties). The IdM Service Provider has to implement technical measures to enforce this requirement, especially with respect to the use of personal data by third parties like ISPs [PRIM08, S. 20]. Furthermore there must be a mechanism which guarantees that a data consumer just requests the data required for the corresponding service (data minimisation). One example for data minimisation is the electronic Passport, which will be launched in Germany in 2010. Apart from enhancing the possibilities for Identity checks by providing biometric identifiers, the new ID card will enable citizens to prove their Identity to Service Providers and administrative authorities over the Internet. An online Service Provider who wants to use the electronic Identity check has to get a governmental verification which requires him to specify the purpose of collection, processing and storing of the data. Due to the underestimation of Privacy issues an IdM Service Provider should reduce complexity of Privacy settings to increase usability (human measure). Another important task for an IdM Service Provider is to strongly enforce the agreed policies (policy enforcement). Services based on user identification do not necessary require a verified user identification (e.g. user`s real name). For this kind of services users must have a choice to operate anonymously, pseudonymously or known (multiple Identities and accountability) [PRIM08, S. 20].

These requirements for Privacy enhancing IdM Services must be implemented by an IdM Service Provider. The requirement of continuous available control mechanisms brings an MCP and its mobile infrastructure into a good position to implement these IdM Services. In this context the CDP, which brings increased usability and user control to the IdM Enabler Concept, will play a fundamental role to implement Privacy requirements.

Chapter 4

Identity Management (IdM) related Functional Capabilities

In the context of the IdM Enabler Concept, IdM related Customer Data Assets and Functional Capabilities were introduced in Chapter 2. This chapter deals with IdM related Functional Capabilities in-depth.

4.1 The Idea of Identity Management (IdM) related Functional Capabilities

There exist a series of research activities that deal with the topic “Identity Management”. Most of them examine the general concept of digital Identities with respect to their relevance, use cases, formats, protocols, and so on. There also exist research activities with the goal to specify IdM Frameworks or an Identity metasystem. Some of these activities also regard the functional view on IdM. Nevertheless, there exists no established work that provides a comprehensive and service oriented cataloguing of IdM Functions. Specifications of Liberty Alliance [LIBE09] or SWIFT [SWFT09] are not sufficient to enable an economic valuation of IdM Enablers. The research exercise in that is to compose a collection of technical functions which explicitly have to do with IdM. In other words, IdM related Functional Capabilities are those functions that make IdM technically and organizationally possible. Anyway, IdM Functional Capabilities on their own cannot be seen as the whole of IdM. Figure 4 illustrates a simple IdM Scenario. It highlights which part of the IdM is covered by the Functional Capabilities. Other components are the involved parties like the End Customer, Identity Service Provider, and Content Provider or IdM related Data Assets. The service oriented approach of this work will influence the shaping of the set of Functional Capabilities. The aim is to compose a set of IdM Functional Capabilities which can be monetized. Consequently, the results can differ from work of technical standardisation of IdM where monetization has no main priority.

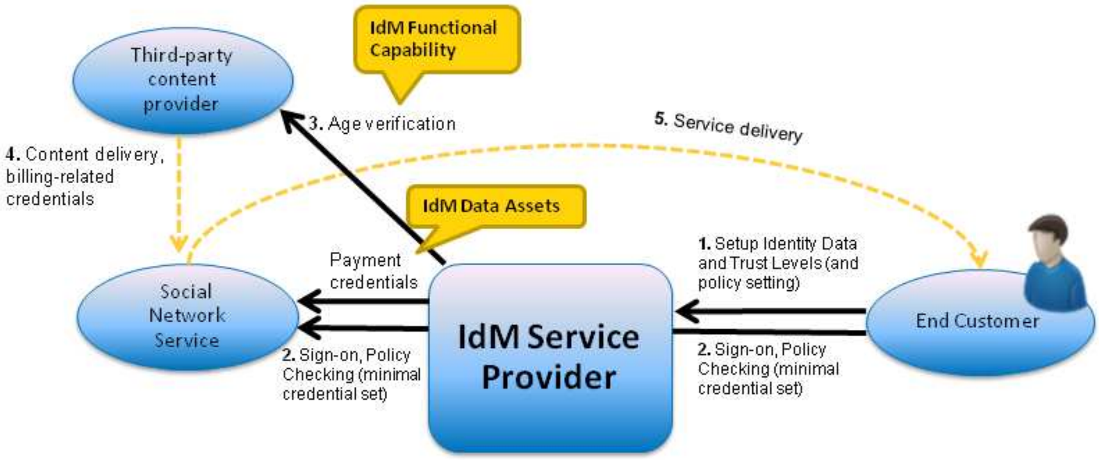
IdM Functional Capability
Third-party content provider
3. Age verification
5. Service delivery
4. Content delivery, billing-related credentials
IdM Data Assets
Payment credentials
1. Setup Identity Data and Trust Levels (and policy setting)
Social Network Service
IdM Service Provider
End Customer
2. Sign-on, Policy Checking (minimal credential set)
2. Sign-on, Policy Checking (minimal credential set)

Figure 4: Simple IdM Service Scenario

4.2 List of Identity Management (IdM) related Functional Capabilities

In this section a collection of IdM Functional Capabilities will be presented. The collection is the result of research that aimed to identify all functions that are relevant for IdM. Some functions were taken from public research papers; some were extracted from existing IdM related services (e.g. Google services[1], Facebook[2], OpenID[3]). In the following the Functional Capabilities will be listed and explained. Furthermore, the functions will be categorized as shown in Figure 5.

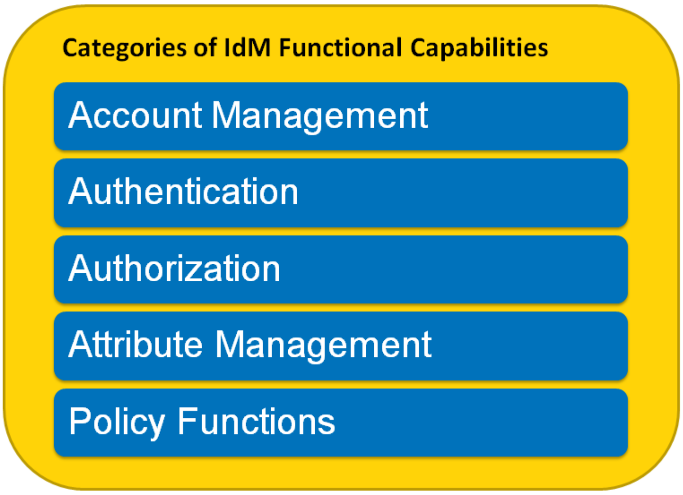

Figure 5: Categories of IdM Functional Capabilities

[1] http://www.google.de/intl/de/options/
[2] http://www.facebook.com/
[3] http://openid.net

4.2.1 Account Functions

Functions categorized as Account Management mainly focus on the account lifecycle from creation to deletion of a user account and the related Data Assets.

Account Federation: Bringing together two (or more) logically separated accounts that were initially set up with distinct service and Identity providers. This requires linking any dataset or information contained in one account with the other accounts. Users retain their individual accounts with each provider in the Authentication Domain while, simultaneously, establishing a link that allows the exchange of user information between them.

Account Consolidation (or Account Merging): The result of merging two logically separated accounts is a new account that contains the sum of all Data Assets contained in both accounts.

Account Transfer: Transfers all information contained in one account to another account which possibly already contains some information. The first account will then be eliminated.

Identity Account Creation: The process of preparing a new account for an Identity. This includes setting up a new (trusted) domain for the new Identity with a separated storage for account related data. Further, initial configurations have to be made (e.g. creating Privacy policies with default values).

Identity Suspension: A digital Identity can be disqualified for service usage, meaning that this Identity can’t make use of services until it is unblocked. The blocking is initiated by the IdM Service Provider in order to protect other Service Providers.

Identity Freezing: The possibility for a user to deactivate this account temporarily. A frozen Identity account will not be used by an IdM Service Provider. That implies that no information that is assigned to that account will be used.

Partial ID Creation: A user can generate several partial Identities with different sets of Identity related data and policy configurations. The user can use different partial Identities with different services.

Partial ID Deletion: The user can delete previously created partial Identities.

Service Account Creation: The process of preparing and generating a new account for a Service Provider that wants to make use of the IdM Service Provider services. This includes setting up a new (trusted) domain for the new service account with a separated storage for account related data. Further, initial configurations have to be made (e.g. creating service policies with default values).

Service Registration: The registration of a Service Provider to the IdM Service Provider. The Service Provider has to provide the necessary information that is needed in order to the IdM Service Provider being able to let users have access to the services. These information include service usage policies that define the requirements that have to be fulfilled if a user wants to have access to that service.

User ID Registration: The initial step for any IdM activity. During the registration a user has to provide a minimal set of Identity related information in order to create a unique account for the user. Service Providers have the possibility to define the minimal set of information that is required to register to a service. After registration a new account for the user will be generated.

4.2.2 Attribute Functions

Attribute management functions cover all necessary needs to mange attributes which could be comparing them to a given value, providing them on request, modifying them, accumulate them to create new attributes etc.

Age Verification: A trusted party confirms or answers in the negative the age of an Identity to a requesting service. This can be compared to a digital signature to the attribute age. This process requires the trusted party to possess the correct information about the age of the Identity.

Attribute Provisioning: Transmitting an existing attribute of an Identity to a requesting party (e.g. Service Provider). For Privacy reasons, this requires checking with the policy settings of the concerning person (policy based) or asking him for permission (transaction based).

Attribute Revocation: Withdrawal of a previously issued attribute. After the revocation, the attribute is devalued, meaning that is contains no information anymore.

Attribute Tracking: For dynamic attributes (attributes that can have different values on different times) a Service Provider can offer “subscriptions”. Any time the value of a subscribed attribute changes, the Service Provider gets an update for that attribute.

Credential Generation: The process of generating specific attributes containing assertions about a digital Identity. This requires the generating entity to possess the information that is relevant to derive such an assertion.

Credential Signing: Attribute Signing takes ‘Attribute Provisioning’ one step further by enhancing the reliability level. This is done by adding a digital signature to the attribute. This makes it possible to gather attributes for later usage. Furthermore, this makes it possible to provide such attributes to third parties that are not in a (business) relationship with the signing party.

4.2.3 Authentication Functions

The following authentication functions group all necessary functionalities to manage authentication and handling of necessary tokens or credentials for the authentication process to take effect.

Attribute Verification: A Service Provider can request the IdM Service Provider to check the correctness of the information of an attribute. This function differs from “Attribute Provisioning” or “Attribute Signing” in the fact that the attribute has its origin not in the IdM Service Provider. The Attribute was generated elsewhere.

Authentication: A user provides a claim to the IdM Service Provider and then the IdM Service Provider verifies the claim. Possible Variants:

- **Multilevel-Authentication:** This enables a user or Service Provider to define for each Trust Level which credential types to use.
- **Multiple Factor Authentication:** Multiple-factor authentication requires a user to provide more than one authentication credential in order to get access to a resource.
- **One-Factor Authentication:** Simple authentication by providing one authentication credential.

Authentication Context Information Provisioning: The authentication context contains information about the mechanisms used for the authentication process. Having this information, one can make (subjective) statements about the reliability of the authentication.

Authentication Credential Issuing: Creating and issuing authentication tokens to the users. For example this can be secure elements like smart cards, security sticks, etc.

Authentication Token Transfer: An authentication token contains information about an authentication that has taken place successfully. Transferring the authentication token to a Service Provider securely means transferring the authentication state to that Service Provider. The user then is also authenticated against the Service Provider without actually authenticating again.

Authentication Method Selection: The possibility for a user to select the authentication method for authenticating. Furthermore a Service Provider can define the authentication method that he requires to get access to the services.

Credential Management: Authentication Credentials can be changed by a user at anytime. This includes setting new passwords, requesting new tokens, etc. (technically, this would be equal to providing new credentials).

Identification: The process of identifying the subject that is interacting with a system. As identification is a part of an authentication process (e.g. by providing a user ID), the usage is not limited to authentication.

Multiple Login: Multiple Login enables a user to login to a Service Provider with two (or more) different partial Identities on the same machine at the same time. An example would be running the same service (e.g. Google Calendars) with different partial Identities (private and work) at the same time. This is not always possible without additional efforts.

Partial Single Sign-On (Selective Sign-On) (SSO): Allows a user to login one time and have access to several resources. This differs from SSO in the fact that the user can select a subset of services to which he wants to be logged in automatically when signing in. The user can create several instances of "Partial SSO". He can assign services, policies, authentication methods and data to such an instance.

Single Logout: The user logs out from multiple services with one click. The logout request is communicated to all affected Service Providers by the IdM Service Provider.

Single Sign-On: Classical SSO. The user is automatically authenticated and logged in to all multiple services after signing in one time. The user then gets automatically access to the service if he is allowed access to it.

4.2.4 Authorization Functions

As the authentication functions take care of all necessary functionalities around the authentication of users the following listed authorization functions cover all necessary authorization functionalities to provide regulated access to resources[4].

Access Right Delegation: Authorize the access to a resource from another digital Identity (temporarily). Delegation implies that the actual Identity gives away his rights temporarily. Access right is passed back with a re-delegation.

Authorization: An Identity is given the right to get access to a specific resource for a specific time frame.

[4] Although there are possibilities to model and implement authorisation with authentication (e.g. anonymous credentials), in this work authorization function are listed in a dedicated category. This can be reasoned by the fact that authorization functions can still be provided independently from authentication mechanisms (either in combination with authentication functions or solely). This suits to the service oriented approach as described at the beginning of this chapter.

Edit Authorization Token: Provides interfaces for editing an authorization token. Editing includes changing the access subject, changing the access object or reconfiguring the access policy.

List Authorized Objects: Lists all objects to which a given subject is authorized to access.

List Authorized Subjects: Lists all subjects which are authorized to access to a given resource.

Provide Authorization Token: Provides authorization tokens to users. Authorization token provisioning is always triggered by a token request. A request can be made by a user (for himself) or a Service Provider (for his users).

Request Authorization Token: A user or Service Provider requests an authorization token which grants a subject access to an object. During the request, the requestor can define the access policy of the authorization token.

Revoke Authorization Token: Revokes a previously issued authorization token. Revocation overrules the access policy of the authorization token. After revocation an authorization token is invalid.

Revoke Signed Authorization Token: Revokes a signed authorization token.

Sign Authorization Token: Takes authentication token provisioning one step further by enhancing the trust level. A digital signature is added to the token to be able to check the genuineness of the token.

Validate Authorization: Checks the request for access to a resource against an authorization token.

4.2.5 Policy Functions

With the help of the following policy functions an IdM System is able to provide individualized (policy based) services to Up- and Downstream Customers. These functions help both sides of the IdM System to define there needs to enable the IdM System to make automated decisions based on the comparison of these policies.

Edit Trust Level: An interface for editing the trust levels is provided to Service Providers and users.

Policy Activation: Activate a policy for usage.

Policy based Data Provisioning[5]**:** User can define the requirements that have to be met by a Service Provider to get private information. This mechanism cares for only revealing user data if the policy requirements are met.

Policy based Service Provisioning[6]**:** A Service Provider can define the requirements that have to be met by a user to get access to specific resources. This mechanism cares for only granting access to the services if the policy requirements are met.

Policy Deactivation: Deactivate a policy. Any requirement stated in that policy will be ignored.

Policy Editing: IdM Service Provider provides interfaces for editing a policy.

[5] In this work we use the term, ‘provisioning‘ intentionally, because it fits the service oriented view of this work. The IdM Service Provider actively provides services to third parties.

[6] See above.

Policy Enforcement: Policy Enforcement is part of a service level agreement (SLA) that guarantees that all policies will be checked in any transaction. The core assurance is that each policy requirement will be considered.

Policy Generation: IdM Service Provider provides interfaces for generating new policies.

Policy Update: Parts of a policy can be bound to (external) conditions. The IdM Service Provider will update the affected parts automatically.

Service dependent Partial ID selection: A user with several digital Identities (partial Identities) can configure the assignment of these Identities to services. The IdM Service Provider then automatically selects the assigned Identity when the user connects to a service.

Service Level based Policy Generation: A Service Provider can define policies for each service level it provides. Each service level can have different requirements that have to be met by a user. The IdM Service Provider provides interfaces to define such interfaces.

Sticky Policy Generation: Sticky policies are (cryptographically) bound to a data set. The data can only be read if policy requirements are met. IdM Service Provider provides interfaces to create such sticky policies.

Trust Level based resource Access: A Service Provider defines subsets of resources to which a user can have access when entering a specific trust level.

Chapter 5

Use Case Scenarios

To highlight the value and significance of IdM Data Assets and IdM Functional Capabilities, relevant use case scenarios are required. Such selected and representative use case scenarios will be presented and introduced in this chapter. The use cases will be used throughout the whole document and future work to demonstrate specific aspects on Privacy, Value Added Services, IdM Data Assets and Functional Capabilities. For each use case, the parts related to IdM Enablers will be extracted and highlighted. From an IdM (and Privacy) perspective, a more detailed analysis is needed, as there exist a series of alternative ways to perform the mentioned tasks. This includes different ways to manage Identity related data (Data Assets) of the End Customer (e.g. where are they stored? Who has control over them?) and different ways to provide them to requesting parties (different functions, different policy implementations and so on). In this work we aim to show implementations which on the one hand add value to the services provided by the Upstream Customers (e.g. Service Providers) and on the other hand consider important Privacy principles. The use cases and the analysis in the following chapters will show that these two goals are not necessarily contradictory.

5.1 Use Case 1 – Online Shopping Scenario

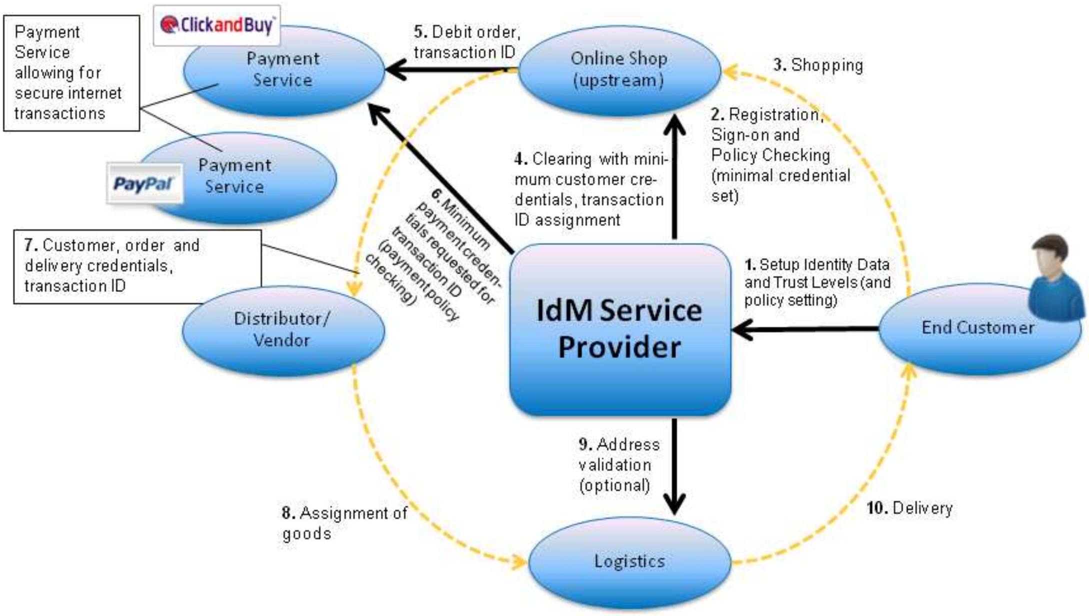
Payment Service allowing for secure internet transactions
ClickandBuy
Payment Service
PayPal
Payment Service
5. Debit order, transaction ID
Online Shop (upstream)
3. Shopping
2. Registration, Sign-on and Policy Checking (minimal credential set)
4. Clearing with minimum customer credentials, transaction ID assignment
6. Minimum payment credentials requested for transaction ID (payment policy checking)
7. Customer, order and delivery credentials, transaction ID
Distributor/ Vendor
IdM Service Provider
1. Setup Identity Data and Trust Levels (and policy setting)
End Customer
9. Address validation (optional)
8. Assignment of goods
Logistics
10. Delivery

Figure 6: Use Case 1 – Online Shopping Scenario

Figure 6 illustrates a classical online shopping scenario. The setting is as follows. A web user (Downstream Customer of the MCP) wants to buy products on an online shopping portal (Upstream Customer of the MCP). In general, this requires a registration on the shopping portal, buying items, paying the items, and delivering the items to the Downstream Customer.

5.1.1 Description of the scenario

In order to make use of the IdM Services that a MCP provides, a user has to register with the IdM Platform of the MCP (1). As a customer of the MCP, the user already has provided basic Identity related data to the MCP (name, address, phone number, birth date, bank account information...). For some of these, the customer presented his Identity card to the MCP. Therefore, the reliability of these information possessed by the MCP are very high, since the source of them is a government issued Identity card. Besides these data, the user has the possibility to extend the data set by further information which the MCP does not possess already. The user also can define Privacy policies that the MCP has to consider when providing any kind of information to third parties. Later, the user wants to buy products on an online shopping portal which also requires registration. As the user is a Downstream Customer of the IdM Infrastructure and the online shopping portal is an Upstream Customer of it, the Functional Capabilities of the MCP IdM Infrastructure can be used to support the registration. The MCP can register the customer with the shopping service and provide the information necessary for this registration (2). Any data provisioning has to match with the policies of the user. If the policy preferences of the user match with the minimum requirements of the Online Shop, the user is registered at the Online Shop. The user who is automatically signed on at the shop now can browse the portal for the desired products (3). Having selected the products, the user triggers the transaction. The next step is clearing the transaction. Therefore the Online Shop possibly requests additional data from the MCP about the user because of the new contractual situation (e.g. for customer care purposes). Again, this request has to match with the user's Privacy policy. A transaction ID is negotiated between the MCP and the Online Shop (4). For Privacy reasons, this ID will be used to refer to the ongoing transaction when interacting with third parties. In the next step, the Online Shop makes a debit order at the Payment Service Provider. It provides only the payment related information and the mentioned transaction ID (5). The Payment Service Provider requests additional information from the MCP that is relevant for the payment process (e.g. bank account information). It refers to the transaction by presenting the transaction ID to the MCP. Policies have to be checked for this (6). For the delivery of the products, the Online Shop contacts the vendor and provides him with the necessary information to be able to deliver the items. This includes the items to deliver and the address of the customer (7). Alternatively the vendor only gets the information about the items to deliver and the transaction ID. The logistics would then get the transaction ID and the package to deliver. The address could be requested from the MCP by providing the transaction ID (8). The MCP would then provide the address information (9) and the package would be delivered (10).

5.1.2 Privacy aspects

As one can see in the use case description, Privacy principles significantly give direction to the shaping of the MCP IdM architecture. Table 8 lists corresponding Privacy principles and explains how they are considered in the architecture.

Privacy Principle	How the principle is achieved in use case	Points of Consideration
User Consent and Control	Any data provisioning to third parties requires the user's consent. In Use Case 1 this can be achieved by explicitly asking him for confirmation before critical payment related data is sent.	1., 2., 4., 6.
Justifiable Parties	Only those parties are involved that are necessary in an online shopping portal scenario.	Whole scenario.
Policies and Policy Enforcement	The MCP IdM infrastructure supports the generation, editing and enforcement of Privacy policies.	1., 2., 4., 6.
Multiple Identities and Accountability	The concept of multiple Identities is supported by the MCP IdM subsystem. However, this is not utilized in use case 1.	

Table 8: Consideration of Privacy Principles in Use Case 1

5.2 Use Case 2 – Age Verification

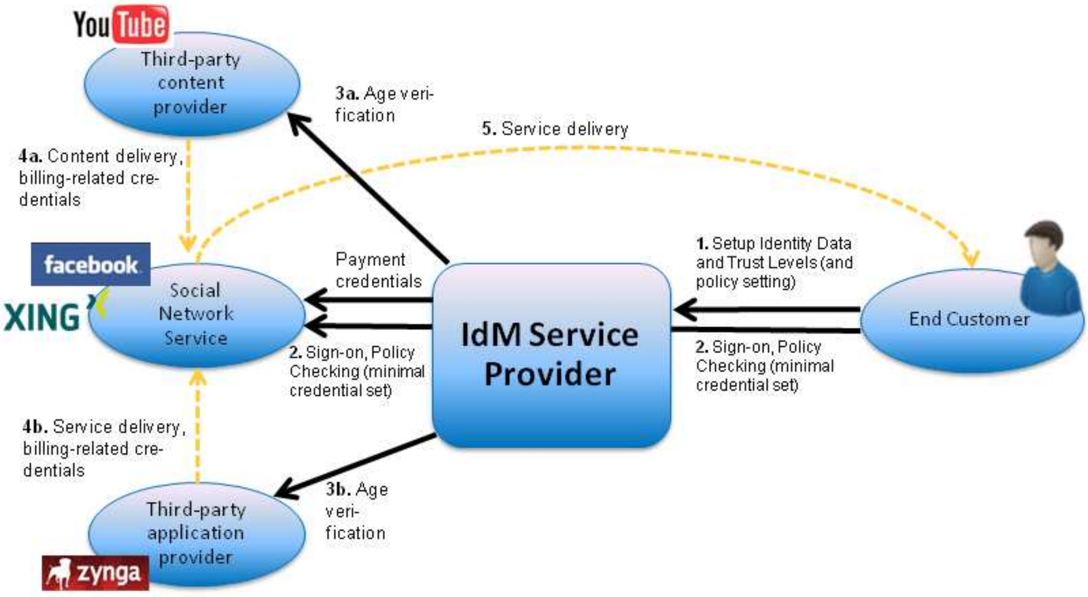
YouTube
Third-party content provider
3a. Age verification
5. Service delivery
4a. Content delivery, billing-related credentials
facebook
XING
Social Network Service
Payment credentials
2. Sign-on, Policy Checking (minimal credential set)
IdM Service Provider
1. Setup Identity Data and Trust Levels (and policy setting)
End Customer
2. Sign-on, Policy Checking (minimal credential set)
4b. Service delivery, billing-related credentials
3b. Age verification
Third-party application provider
zynga

Figure 7: Use Case 2 – Age Verification

Figure 7 illustrates social network scenario (SNS) with content provisioning from third party services. The content to be provided underlies certain age restrictions (e.g. user has to be at least 18 years old).

5.2.1 Description of the Scenario

1.) Like in the online shopping scenario, the user has to register with the MCP IdM platform and setup initial Identity data and Privacy policies.

2.) After registration to the social networking service the user is automatically signed on to the social networking service platform.

3.) The user is interested in specific multimedia contents which third party content provider offer over the SNS platform and starts a request for these. As the desired contents have age restrictions, the content providers request the MCP for age verification. The MCP knows the birth date of its customer through his Identity card. Therefore it has a reliable source on which the verification of the age can base. After checking the age the MCP provides the content provider with the result of the verification.

4.) If the result was positive, the content providers deliver the content over the SNS platform to the user. Additionally, if the content is going to be charged, the content providers provide the SNS billing-related credentials (e.g. amount).

5.) In the last step the SNS delivers the content as a service over its platform to the user.

5.2.2 Privacy Aspects

In use case 2 Privacy aspects are also considered. Table 9 lists the Privacy principles and their consideration in use case 2.

Privacy Principle	How the principle is achieved in use case	Points of Consideration
User Consent and Control	Any data provisioning to third parties requires the user's consent. In Use Case 2 this is achieved by the Privacy policies configured by the user or by explicitly asking the user for confirmation before any data provisioning.	1., 2., 3.
Justifiable Parties	The content provider's participation is clear. The SNS' participation can be reasoned with its platform that is well-suited for content provisioning. Because of their huge user basis, SNS are a valuable channel for bringing content to the customers. This way of distributing content is already used in practice and will be even more important in near future. The SNS could also play the content provider which would make the third-party needless, but content delivery is not the SNS's core competence.	Whole scenario.
Policies and Policy Enforcement	The MCP IdM infrastructure supports the generation, editing and enforcement of Privacy policies.	1., 2., 3.
Multiple Identities and Accountability	The concept of multiple Identities is supported by the MCP IdM subsystem. However, this is not utilized in use case 2.	

Table 9: Consideration of Privacy Principles in Use Case 2

Chapter 6

Aim of the Heartbeat

Aim of this Heartbeat was to describe a first draft of a newly developed IdM Enabler Concept as an approach to evaluate the economic potential of IdM Data Assets and Functional Capabilities. The foundation for the valuation process is formed by the concept of IdM Enablers, which are composed out of IdM related Customer Data Assets and IdM related Functional Capabilities. This draft model acts as starting point for discussion and future development of a final IdM Enabler Model. This model will then be described in Deliverable D6.1.2 and form the basis for the final valuation approach.

The discussion aims to take into account all aspects of the model, like Data Assets, Functional Capabilities and the contra dictionary approaches of service driven vs. user centric IdM. Further we expect the experts group to make suggestions

- with regard to completeness, correctness and the like of the proposed Data Assets, Functional Capabilities, as well as
- on the composition of Data Assets and Functional Capabilities, especially whether these compositions result in valuable IdM Enablers.

References

[CL02] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In International Conference on Security in Communication Networks (SCN), volume 2576 of Lecture Notes in Computer Science, pages 268–289. Springer Verlag, 2002.

[BATI06] Batini C. and Scannapieco M.: Data Quality – Concepts, Methodologies and Techniques. Springer, 2006.

[CUTL08] Cutler, R.: Liberty Identity Assurance Framework. http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-Identity-assurance-framework-v1.1.pdf

[DEYA01] Dey, A.K.: Understanding and Using Context. Personal Ubiquitous Computing 5(1), 4–7 (2001)

[EUDA95] EU Data Protection Directive (95/46/EC): http://eur-lex.europa.eu/Notice.do?val=307229:cs&lang=en&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=95/46/EC~&checktexte=checkbox&visu=#texte

[FISH09] The Data Asset: How Smart Companies Govern Their Data for Business Success http://books.google.com/books?id=OzzXdFI37rIC&printsec=frontcover&dq=data+asset&ei=VKhNS7nzJI6szASz-r36Cw&hl=de&cd=1#v=onepage&q=&f=false

[KASP06] Kaspar, Christian Markus (2006): Individualisierung und mobile Dienste am Beispiel der Medienbranche. Ansätze zum Schaffen von Kundenmehrwert. Univ., Diss.--Göttingen, 2005. Göttingen: Univ.-Verl. Göttingen (Göttinger Schriften zur Internetforschung, 3).

[LANG01] Langheinrich, M.: Privacy by design – principles of Privacy-aware ubiquitous systems.In Abowd, G., Brumitt, B., Shafer, S., eds.: Proceedings of Ubicomp 2001. Volume 2201 of Lecture Notes in Computer Science., Springer (2001) 273–291

[LIBE09] The Liberty Alliance Project. http://www.projectliberty.org/

[PRIM08] PRIME white paper, Third and final version, May 2008, https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf

[SATT09] Sattler K.: Data Quality Dimensions. Technical University of Ilmenau, llmenau, Germany 2009.

[SWFT09] EU ICT FP7 Project SWIFT. http://www.ist-swift.org/

[WANG96] Wang R. and Strong D. Beyond Accuracy: What Data Quality Means to Data Consumers. J. Inf. Syst., 12(4):5–34, 1996.

[WIKI09a] Wikipedia Article: Communication. http://en.wikipedia.org/wiki/Communication

[WIKI09b] Wikipedia Article: Information Device.
http://en.wikipedia.org/wiki/Information_device