Economic Valuation of Identity Management Enablers

Editors:	Sascha Koschinat (GUF)
	Gökhan Bal (GUF)
	Kai Rannenberg (GUF)
Reviewer:	Hans Hedbom (KAU)
	Gregory Neven (IBM)

Identifier:	D6.1.2
Type:	Deliverable
Class:	Public
Date:	May 20, 2011

Abstract

Telecommunications operators face an elementary change in their traditional business model. A potential direction of this change is business models that concentrate on the exploitation and monetisation of the huge amount of customer data that result from the usage of traditional communication services. Based on these data and other factors, such as telcos' longstanding relationships to their customers, and infrastructural assets and capabilities, telcos are a reasonable candidate for assuming the role of identity management service providers (IdMSPs). This document presents a method to evaluate privacy-enhancing IdM Services from the perspective of a telco acting as prospective IdM Service Provider. The basis for the valuation method is the concept of Identity Management Enablers, which is used to analyse and describe the services and scenarios on which the decision supporting method is based.

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

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

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	Authors (all GUF)
1 Introduction	Sascha Koschinat Gökhan Bal
2 The Identity Management Enabler Concept	Sascha Koschinat Gökhan Bal Marvin Hegen
3 Method for an Economic Valuation of IdM Enablers	Sascha Koschinat Gökhan Bal
4 Application of the Method	Sascha Koschinat Gökhan Bal
5 Summary, Conclusion and Outlook	Sascha Koschinat Gökhan Bal

Contents

List of Figures

List of Tables

List of Abbreviations

AgeVer	Age Verification
Auth	Authentication
BO	Baseline Option
BS	Baseline Scenario
DO	Delta Option
DS	Delta Scenario
EC	End Customer
IdM	Identity Management
IdMSP	IdM Service Provider
PPE	Privacy Policy Enforcement
SP	Service Provider
Telco	Telecommunications Operator
VAS	Value-added Service

Chapter 1

Introduction

Telecommunications operators (telcos) face an elementary change in their traditional business model. The reasons for this are manifold: tougher regulations, new technology (most notably VoIP and spectrum of free services), matured core business markets (voice and messaging), new market entrants, or advancing customer demands and expectations[1]. Thus, telcos are forced into decision-making about new business models. A potential direction of this change is business models that concentrate on the exploitation and monetisation of the huge amount of customer data that arise from the usage of traditional communication services, such as voice and data. One potential business model will be the provision of identity management services to third-party service providers. Factors that make telcos a reasonable candidate for assuming the role of identity management service providers (IdMSPs) are the mentioned customer data bases and other factors, such as telcos' longstanding customer relationships, and their infrastructural assets and capabilities. Nevertheless, due to the privacy-sensitivity of customer data and the legal liabilities that come with the processing of them, telcos (like other organisations) have concerns regarding the economic motivations to invest in identity management services [FaRi08]. Therefore, telcos need instruments to systematically assess the potential value of providing such identity management services. So far, there is a lack of such instruments that considers multilateral interests of all stakeholders involved, such as users' privacy needs.

To fill this gap, we developed a method to support the decision-making of telcos regarding investments into the provision of privacy-enhancing identity management services. Some steps of the method are structured following established economic methods. An essential part of the method is the *IdM Enabler Concept* that has emerged as a way to model *IdM Data Assets* and *IdM Functional Capabilities*. IdM Enablers are atomic[2] services that are composed of IdM Data Assets and IdM Functional Capabilities. Based on the previously mentioned arguments, we focus on telcos assuming the role of IdMSPs instead of other potential Internet-based service providers (e.g., Facebook, Google, or Amazon).

[1] http://www.telco2.net/manifesto/

[2] *atomic*: forming a single irreducible unit or component in a larger system. Thus, IdM Enablers are single irreducible components of IdM service provision that are provided to third-party service providers as a whole. (from oxforddictionaries.com)

The deliverable is structured as follows. Chapter 2 introduces the IdM Enabler Concept as an essential component of the valuation method. We explain what IdM Enablers are composed of and how they can be modelled. Further, different market players are introduced with a special focus on their suitability for assuming the role as identity management service providers. The chapter concludes with two example IdM Enablers to highlight the value and significance of IdM Data Assets and Functional Capabilities. In Chapter 3, we introduce the method for the valuation of IdM Enablers and give a step-by-step description. Each step is followed by an illustrative example. A more detailed execution of the method is presented in Chapter 4, where further IdM service scenarios are presented and evaluated with the method. Finally, Chapter 5 summarizes the main findings of this work, discusses the benefits and limitations of the method and gives an outlook on further potential developments.

Chapter 2

The Identity Management Enabler Concept

An inevitable precondition for the development of a method to evaluate IdM-enabling services is a clear conceptualization of IdM Enablers. Such a concept will in the first place help decision-makers to model their IdM service scenarios to prepare the valuation. A conceptualization of IdM Enablers is provided in this chapter (Section 2.2). The key elements of IdM Enablers – IdM Data Assets and IdM Functional Capabilities – are introduced in Sections 2.3 and Section 2.4. Chapter 2 concludes with a brief discussion on candidates for assuming the role of an IdMSP.

2.1 Why IdM Enablers?

In the economy at large, there are inefficient and ineffective business processes in every industry. The current untapped potential of identity-related customer data assets and functional capabilities in many companies (e.g., telecommunications operators) could help service providers to interact with end customers in a more efficient and effective way than today. Therefore, these IdM assets and capabilities should not be seen as by-products of service provision, but rather as bundles of core products. Given the huge amount of data in their databases, telcos need tools that present decision-relevant information, in a simple and structured way. Furthermore, when introducing identity management services into a market, they must be integrated into existing architectures of the telco's business model and also consider external market conditions, such as new technologies, regulations, or customer demand that also influence the outcome of a market introduction or investment decision. One key aspect in that is the consideration of users' privacy. The processing of personal data is privacy-sensitive and regulated by data protection laws. Thus, providing the user with appropriate control and transparency mechanisms is indispensable for IdM-related business models. So far, there is no model in theory or practice that considers all these factors. Motivated by this gap, the *IdM Enabler Concept* has emerged as a way to model IdM assets and capabilities to prepare and enable their valuation. This model helps to bundle IdM assets and capabilities to single objects ("IdM Enablers") and use them to provide new value-added services to end customers and service providers considering end customers' privacy.

2.2 The IdM Enabler Concept

The provision of IdM-related data assets and functional capabilities by an identity management service provider (IdMSP) to other actors of an identity-driven economy (service providers, end customers) is here called *IdM Service*. According to that definition, an IdM Service consists of one or more bundles of IdM data assets and IdM functional capabilities. A respective single bundle of these two components – more precisely a valuable combination of them – will here be referred to as an *IdM Enabler*, the driver for an actual IdM Service. Thus, an IdM Service in turn typically consists of one or more IdM Enablers.

IdM Data Assets (Section 2.3) in this context are attributes of a user identity, such as name, place of birth, account details, and so forth, whereas *IdM Functional Capabilities* (Section 2.4) are those functions that are required to process these data assets and make their management and provision possible. Figure 2.1 illustrates the IdM Enabler concept. In this example, the IdM Service is an "age verification service" (the IdM Enabler) that is composed of the IdM Data Asset "birth date" and the IdM Functional Capability "attribute verification". Note that neither the data asset nor the capability is provided to third parties. Instead, only the IdM Enabler "age verification" is provided. This example further shows the potential of the approach regarding privacy-enhancement. The result of the service is a Boolean (i.e., *true*, if customer's age ≥ 21; *false*, if customer's age < 21). The actual date of birth remains private. In this way, IdMSP customers can generate significant values or enable new value-added services and at the same time protect users' privacy. The IdM concept described above is here referred to as the *IdM Enabler Concept.*

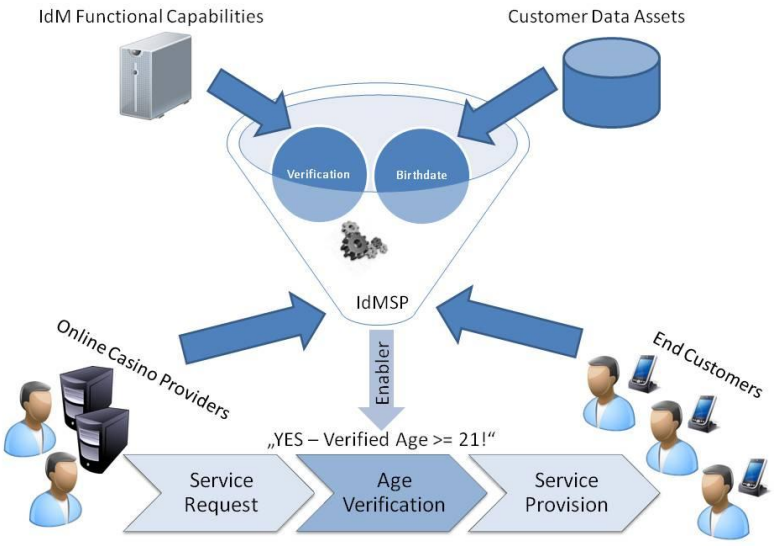

Figure 2.1: The IdM Enabler Concept

2.3 IdM 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 maybe the 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 real-time) customer information, terms, such as 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.

2.3.1 IdM 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 (Section 2.3.2.2), while indirect identification is based on combining and processing basic-, communication-, content-, context-, financial-, and device data (Sections 2.3.2.3-2.3.2.7).

Personal data can be used to create user profiles which are collections of data associated to a specific user. A profile can be seen as an explicit digital representation of a person’s identity which can be a risk for that person’s privacy.

2.3.2 Categories of IdM Data Assets

As described before, IdM Data Assets in the context of this deliverable are 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 IdM Data Assets. These are illustrated and discussed in further detail in the next sections. An essential aspect of this research was the identification of relevant user data for actual IdM business models in the internet economy. Different economic zones, regulation terms and legal restrictions played a minor part for this analysis.

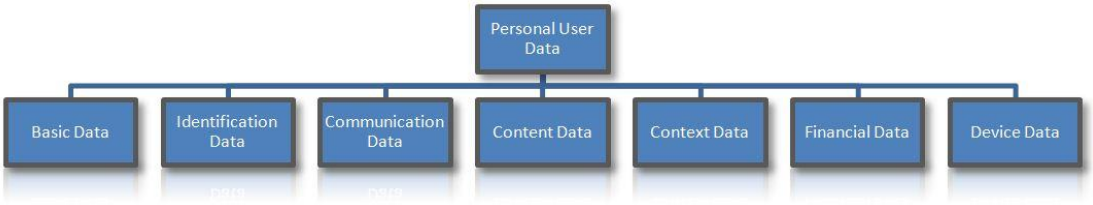

Figure 2.2: Categories of IdM Data Assets

2.3.2.1 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).

Table 2.1: Basic 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

2.3.2.2 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, such as 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.

Table 2.2: Identification Data

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

2.3.2.3 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 advertisement purposes. While user-generated content apparently is uploaded by the user himself, content the user is interested in is mostly logged from search queries, website usage patterns and content downloads.

Table 2.3: Content Data

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

2.3.2.4 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 2.3, the user context can be separated in five categories.

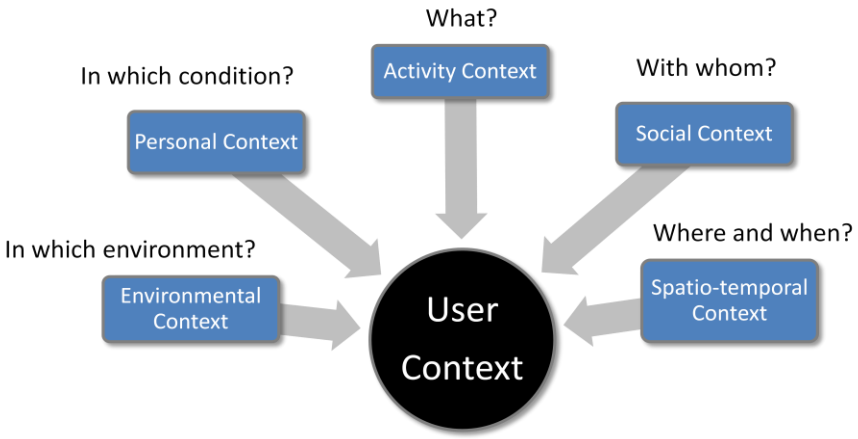

Figure 2.3: Different Dimensions of Context Data

Context data is especially used in context-aware services to personalize services and thus increase the usability and the value of them. Any additional context data can 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.

Table 2.4: Context Data

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

2.3.2.5 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.

Table 2.5: Communication Data

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

2.3.2.6 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, his payment information (credit card, bank account details) and his buying patterns. Besides this typical financial data, also data such as place of residence etc. could be of interest with credit profiling: this shows a typical situation of overlapping data attributes.

Table 2.6: Financial Data

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	

2.3.2.7 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).

Table 2.7: Device Data

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

2.3.3 Value and Quality of IdM Data Assets

For the valuation 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 successfully on the IdM-Market, we need to understand the value of their customer and 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 who is interested in advertisement campaigns: when personal user data is complete and thus of high

value? The answer: that depends on the needs of the data consumer. If the data consumer is interested in a widespread anonymous marketing campaign, such as bulk mails, 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].

2.3.4 Privacy requirements for IdM 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 of PrimeLife. In the meantime, this urgent need for enhanced privacy settings has been recognized by ISPs and telcos 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 what personal data are provided 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, such as ISPs [PRIM08, S. 20]. Furthermore, there must be mechanisms that guarantee that a data consumer just requests the data required for the corresponding service (data minimisation). One example for data minimisation is the electronic ID card, which has been 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 a telco and its mobile infrastructure into a good position to implement these IdM Services.

2.4 IdM Functional Capabilities

This section deals with IdM Functional Capabilities in-depth.

2.4.1 IdM 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 meta system. 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 therefore 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. IdM Functional Capabilities on their own cannot be seen as the whole of IdM. Figure 2.4 illustrates a simple IdM Scenario. It highlights which part of the IdM is covered by the Functional Capabilities. Other components are the involved parties, such as the end customer, IdM service provider, and content provider or IdM Data Assets. The service-oriented approach of this work will influence the shaping of the set of Functional Capabilities. The aim was to compose a set of IdM Functional Capabilities which can be used for an economic valuation. Consequently, the results can differ from work of technical standardisation of IdM where economic aspects have no main priority.

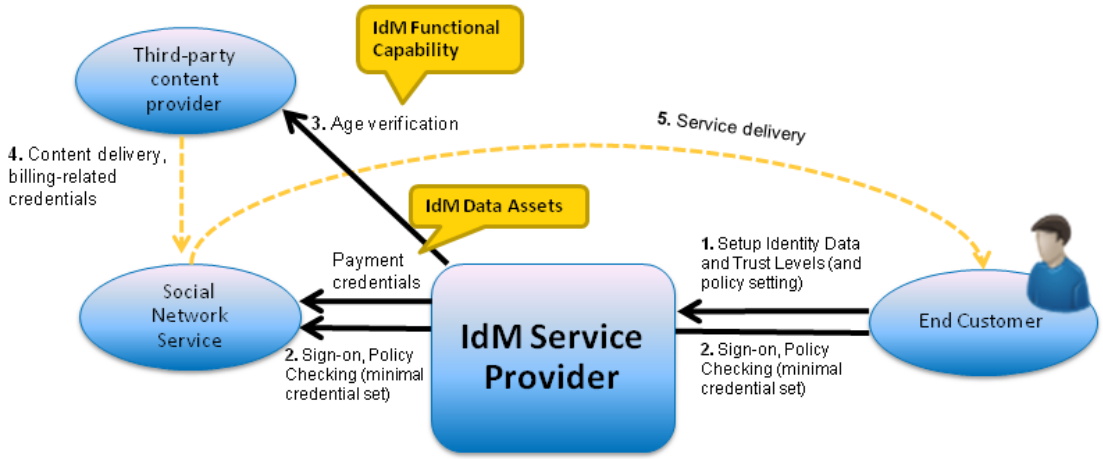

Figure 2.4: IdM Enabler Scenario

2.4.2 A Collection of IdM 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 a comprehensive set of 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[3], Facebook[4], OpenID[5]). In the following the Functional Capabilities will be listed and explained. Furthermore, the functions will be categorized as shown in Figure 2.5.

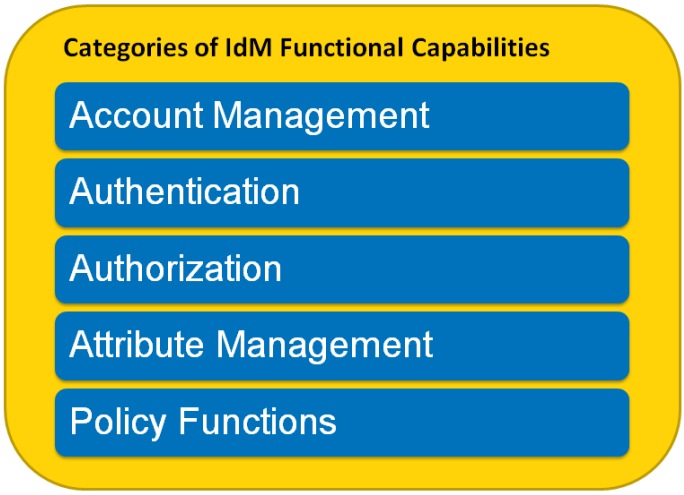

Figure 2.5: Categories of IdM Functional Capabilities

2.4.2.1 Account Functions

Functions in this category 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.

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

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.

2.4.2.2 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.

2.4.2.3 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.

2.4.2.4 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[6].

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.

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.

---

[6] 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.

2.4.2.5 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[7]**:** 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[8]**:** 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.

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.

2.5 IdM Service Providers

In the digital economy, there exist several market players that come into consideration for assuming the role of an IdMSP. A well-balanced interplay of IdM data assets and functional capabilities for business transactions could enable significant added values to *all* involved actors of identity-driven economies. Service providers could provide new value-added services, increase

[7] 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.
[8] See above.

the value of their existing services, and improve the efficiency and effectiveness of their business processes by analyzing and processing customer data while fulfilling technical and economical requirements and being compliant with legal and social privacy requirements. End customers could benefit from an increased offer of value-added, personalized, and low priced or even free services in exchange for the (privacy-respecting) provision of personal data.

This highly intertwined identity-driven economy relies on an appropriate level of trust between the respective actors. This requires a trust-enhancing provision of IdM Data Assets and utilization of IdM Functional Capabilities (e.g. privacy-enhanced data processing capabilities) to assure the confidentiality, authenticity, integrity, and availability in the respective interactions. This is especially important when considering the current personal data processing practices of data aggregators, such as advertisers. As mentioned before, the question of who would be the best candidate to enable the required trust relationships is still open. A few relevant market actors coming into consideration are presented in the following sections.

2.5.1 Internet-based Service Providers (ISPs)

Internet-based Service Providers (ISPs), such as Google[9], Apple[10], Amazon[11], or Facebook[12] have huge customer bases and hold a wide range of data assets containing information about their customers. These service providers have early realized the economic value of customer data and therefore usually operate on a highly scalable, two-sided business model. On the one side of their business model they provide low-priced or even free services to their customers and thereby collect information about their customers. On the other side of their business model they provide this information to third parties as a source of further revenue streams, predominantly to marketing and advertising service providers.

Even if ISPs are relatively successful with their business models, in consideration of the following aspects, the customer data assets of these ISPs are often deemed to be voyeuristic, temporary, fragmented, and speculative:

- The vast customer rejection of behavioural advertising,
- the often 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 lack of transparency in personal data processing.

Usually ISPs offer very limited platforms to support identity-driven economies with IdM-related functional capabilities. Therefore, they and can be regarded as specialized providers of customer data assets. The advertisement-based business models of ISPs make it hard to find good trade-offs between fulfilling end customers' privacy requirements and the profits that come from advertisement based on user profiling. Privacy issues are the main reason why ISPs do not have strong incentives to become IdMSPs. In many cases the provision of customer data assets is the major or even the only source of revenue in their business models.

[9] http://www.google.de/intl/de/corporate/
[10] http://www.apple.com/
[11] http://www.amazon.com/
[12] http://www.facebook.com/

2.5.2 IdM Providers

Specialized IdM providers or protocols, such as VeriSign[13], Payment Network AG[14], OAuth[15], OpenID[16], Schufa[17], Idemix[18], U-Prove[19], or SIZCHIP[20] provide a multiplicity of IdM-related functional capabilities, such as account-, attribute-, authentication-, authorization-, and privacy policy enforcement functions that can be used by service providers (e.g. online shops) and end customers. Whereas for service providers, the majority of IdM-related functionalities are provided with fees (e.g. end customer data processing functionalities), for end customers most of the IdM-related functionalities are available for free (e.g. privacy-enhancing functionalities).

Normally, the available IdM solutions are 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 gain 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 ensures 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 identity-driven economies. Providers of these platforms and services can more be seen as specialized providers of IdM functionalities and not of IdM-related data assets.

2.5.3 Telecommunications Operators

Telecommunications operators (telcos), such as Vodafone[21], T-Mobile, Orange[22], or Telefónica[23], provide a wide range of voice-, messaging-, data-, and broadband services to nearly every end

[13] http://www.verisign.com/
[14] https://www.payment-network.com/
[15] http://oauth.net/
[16] http://openid.net/
[17] http://www.schufa.de/
[18] http://www.zurich.ibm.com/security/idemix/
[19] http://www.credentica.com/
[20] http://sizchip.siz.de/cms/SIZCHIP/
[21] http://www.vodafone.com/content/index.html
[22] http://www.orange.com/
[23] http://www.telefonica.com/

customer of an identity-driven economy over simple one-sided business models with the end customers as their only revenue source. Thereby resides an enormous amount of customer data assets as a by-product of telcos' one-sided service provision. For several reasons, both the quantity and the quality of the customer data assets stored in telcos' databases are higher compared to the data of other players in the market. 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 telcos 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 telcos contribute to a unique position of the telcos for the potential role of an IdM Service Provider. The high degree of end customers' trust in telcos regarding the protection of their personal data is based on the absence of pressure to be dependent on selling customer data for more revenue streams than from their current core businesses. Telcos have strong one-sided core business models and act on a high regulated market. In combination with the telcos internally applied methods and functionalities to process their customer data, telcos have predominantly well fulfilled conditions to become trusted custodians of their customers' identities.

However, in order to help service providers and end customers interact more efficiently, it is essential for telcos to build open and standardized platforms. Therefore, telcos' customer data assets need to be reorganized, extracted, and bundled from multiple in-house databases. Functional capabilities need to be implemented and made available for third-party applications or services through standardized APIs to provide controlled access to the telcos' customer data assets or context-relevant representations of them. Parts of the IdM-related infrastructure of telcos need to be restructured before they can be used for such IdM purposes. Further, privacy-respecting IdM functionalities and protocols need to be established and implemented for every kind of supported or enabled business transaction. End customers' privacy needs have to be considered and personal data processing practices have to be made transparent in order to gain customer acceptance. Particularly legal aspects need to be considered and implemented into the whole organizational and operational business and technology infrastructure of the telco. 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 telcos in general.

Chapter 3

Method for an Economic Valuation of Identity Management Enablers

This chapter introduces a decision support approach that can help telcos in decision-making about investments in or market launches of privacy-enhancing IdM services. The previously introduced IdM Enabler Concept forms the basis for the valuation method described in this chapter. The valuation approach can be used as a decision support instrument for potential providers of privacy-enhancing IdM services and consulting agencies acting in this domain. It is focused on decision situations, where an IdM service provider (IdMSP) has to decide:

- whether to invest in a privacy-enhanced IdM service,
- in which one of at least two alternative privacy-enhancing IdM services to invest.

The introduced approach enables a decision maker to capture this complex decision problem in a structured way and to break it down to separate and transparent parts. This enables the division and parallelization of tasks, and specialisation on separate aspects of the decision problem. The decision maker has thereby the ability to include not only qualitative but also quantitative figures in the decision making process. Beyond that, the proposed instrument is also qualified as a communication platform or rather as a basis for discussions between members of a decision-making work force to achieve a common decision basis. Another important aspect of the valuation approach is the consideration of impacts of an investment or market launch decision on other market participants and their interdependent impact on the decision maker. By these measures the decision maker will have a structured and standardized procedure for a repeatedly upcoming decision problem.

3.1 The Anatomy of the Valuation Approach

Before describing the method in detail, we want to give information on its structure. Two perspectives are relevant for this purpose: The **procedural perspective** and the **structural perspective**. These two perspectives are introduced in the following.

Procedural Perspective

From the procedural point of view, the method consists of **six process steps**, which are performed sequentially. A detailed description of each step will be given in Section 3.3:

1. Description of the Baseline Option and feasible Delta Options.
2. Identification of each stakeholder's costs and benefits.
3. Selection key costs and benefits.
4. Clustering and mapping of key costs and benefits.
5. Assessment and aggregation of IdMSP's clustered costs and benefits.
6. Visualisation of IdMSP's aggregated cost and benefits.

Structural Perspective

The second perspective is the **structural** perspective. It comprises the structural **elements** (components) that are used across each step of the method. The following elements will be described in Section 3.3:

- Perspective of each stakeholder
- Cost and Benefit Dimensions
- Costs and Benefits
- Key Costs and Benefits
- Cost/Benefit Values
- Dimension Values
- Decision Values
- Cause-Effect Chains
- Weighting Factors for Cause-Effect Chains

3.2 Components of the Method – The Structural Perspective

Perspective of Each Stakeholder

Since decisions of the decision maker (IdMSP) have interdependent consequences for itself as well as for the other market participants (end customers and service providers), the impacts on other market participants are included in the valuation process. Therefore, on the highest level, the approach differentiates between different perspectives for each stakeholder. Each perspective includes the impacts of an investment or market launch decision from an end customer's, service provider's, or IdMSP's point of view.

Cost and Benefit Dimensions

Each perspective is assembled of multiple cost and benefit dimensions. Each dimension is a decision-relevant factor for each stakeholder regarding the demand, the procurement or provision of a privacy-enhancing IdM service. These dimensions can be deducted from the individual value perception of a respective stakeholder. Regarding the demand decision, private consumers' intentions, such as maximizing privacy or minimizing risks, play a key role, while business

consumers, procurers, or providers of privacy-enhancing IdM services have rather economical intentions, such as maximizing revenues or minimizing costs. Based on these diverse value perceptions, the approach uses different dimensions for private consumers and business consumers, procurers, or providers of privacy-enhancing IdM services. These dimensions reflect the entire spectrum of all decision-relevant factors for the demand, the procurement, or the provision of a privacy-enhancing IdM service for each of the respective stakeholders.

For the private consumers' (end customers') perspective, the decision-relevant dimensions of **(1.) privacy**, **(2.) risk**, **(3.) performance**, and **(4.) effort** were derived from various models of technology adoption and privacy research. The perspectives for business consumers and procurers (service providers), or institutional providers of privacy-enhancing IdM services (IdMSPs) are composed of other dimensions. These dimensions were derived from various models for developing and sketching out new or existing business models and external factors that influence given business models, e.g. the "Business Model Canvas"[24]. The perspective of an institutional consumer, procurer, or provider of privacy-enhancing IdM services is composed from the following dimensions: (**1.) cost structure**, **(2.) revenue streams**, and **(3.) external risks**.

Costs and Benefits

Expected economic effects related to each dimension will be listed in the form of costs and benefits. Costs and benefits are qualitative or quantitative parameters that represent positive or negative effects of consuming, procuring or providing a specific IdM service. Costs and benefits are clustered into related cost and benefit dimensions. Tables 3.1 – 3.5 summarize proposed costs and benefits for each dimension of end customers and service providers or IdMSPs.[25]

Table 3.1: Costs and Benefits of End Customer Cost-Benefit Dimension "Privacy"

Data Minimization	Indicates the compliance with the principle of data minimization. **Less**: End Customer has to provide more information; **Higher**: End Customer has to provide less information; **Equal**: No change
Anonymity	Indicates the change in the anonymity level of the end customer. **Less**: End Customer's anonymity level decreases; **Higher**: End Customer's anonymity level increases; **Equal**: No change
Unlinkability	Indicates the change in the level of unlinkability of end customer's data. **Less**: Higher linkability of end customer's data; **Higher**: Less linkability of end customer's data; **Equal**: No change
Undetectability	Indicates the change in the level of undetectability of end customer's data. **Less**: Higher undetectability of end customer's data; **Higher**: Less undetectability of end customer's data; **Equal**: No change
Unobservability	Indicates the change in the level of unobservability of end customer's data. **Less**: Higher unobservability of end customer's data; **Higher**: Less unobservability of end customer's data; **Equal**: No change

[24] http://nonlinearthinking.typepad.com/nonlinear_thinking/2008/07/the-business-model-canvas.html

[25] The Cost and Benefit items of the dimension "Privacy" are based on the Pfitzmann-Hansen Anon Terminology [PH2010]

Pseudonymity	Indicates the change in the pseudonymity level of the end customer. **Less**: End Customer's pseudonymity level decreases (towards revealing the user's identity); **Higher**: End Customer's pseudonymity level increases (towards anonymity); **Equal**: No change

Table 3.2: Costs and Benefits of End Customer Cost-Benefit Dimension "Risks"

Risk of Unavailability	Indicates the change in the risk of unavailability of the service for the end customer. **Less**: Lower risk of unavailability **Higher**: Higher risk of unavailability **Equal**: No change.
Risk of Data Misuse	Indicates the change in the risk of data misuse. **Less**: Lower risk of data misuse **Higher**: Higher risk of data misuse **Equal**: No change.
Risk of Service Failure	Indicates the change in the risk of service failure. **Less**: Lower risk of service failure **Higher**: Higher risk of service failure **Equal**: No change.
Risk of Additional Efforts	Indicates the change in the risk of additional efforts (e.g. through correction of transactions) **Less**: Lower risk of additional efforts **Higher**: Higher risk of additional efforts **Equal**: No change.
Risk of Acceptance	Indicates the change in the risk of missing acceptance (e.g. through the lack of service provider support for the service) **Less**: Lower risk of missing acceptance **Higher**: Higher risk of missing acceptance **Equal**: No change.
Financial Risks	Indicates the change in the level of financial risks **Less**: Lower financial risks **Higher**: Higher financial risks **Equal**: No change.
Risk of Frauds	Indicates the change in the risk of frauds **Less**: Lower risk of frauds **Higher**: Higher risk of frauds **Equal**: No change.
Risk of Identity Thefts	Indicates the change in the level of risk of identity thefts **Less**: Lower risk for identity thefts **Higher**: Higher risk for identity thefts **Equal**: No change.

Table 3.3: Costs and Benefits of End Customer Cost-Benefit Dimension "Performance"

International Usage	Indicates the change in the potential for international usage **Less**: International usage is restricted or complicated **Higher**: More potential for international. **Equal**: No change.

Transaction Duration	Indicates the change in transaction durations. **Less**: Transactions are slower **Higher**: Transactions are faster **Equal**: No change.
Usability	Indicates the change in the usability of the service **Less**: Service is less usable **Higher**: Service has higher usability **Equal**: No change.
24/7 Usage	Indicates the change in the potential for 24/7 usage **Less**: 24/7 usage is restricted or not supported **Higher**: More potential for 24/7 usage **Equal**: No change.
SP Acceptance	Indicates the change in the level of SP acceptance **Less**: Less acceptance of service providers for this service **Higher**: Higher acceptance of service providers for this service **Equal**: No change.
Possibilities to abort transactions	Indicates the change in the possibilities for the user to abort transactions **Less**: Less support for aborting transactions **Higher**: Higher support for aborting transactions **Equal**: No change.
Possibilities to inspect transactions	Indicates the change in the possibilities for the user to inspect transaction history **Less**: Less support for inspecting transaction history **Higher**: Higher support for inspecting transaction history **Equal**: No change.
Possibilities for bonus programs	Indicates the change in the potential for loyalty programs **Less**: Less potential for loyalty programs **Higher**: More potential for loyalty programs **Equal**: No change.
Possibilities to control transaction	Indicates the change in the possibilities to control transactions (e.g. transparency of transactions) **Less**: Less possibilities to control transactions **Higher**: More possibilities to control transactions **Equal**: No change.

Table 3.4: Costs and Benefits of End Customer Cost-Benefit Dimension "Efforts"

Efforts for hardware	Indicates the change in the efforts the EC has to put into (additional) hardware **Lower**: The EC needs less hardware compared to Baseline Scenario **Higher**: The EC needs additional hardware compared to Baseline Scenario **Equal**: No change.
Efforts for software	Indicates the change in the efforts the EC has to put into (additional) software (e.g. buying, installation, maintenance, etc.) **Lower**: The EC needs less software compared to Baseline Scenario **Higher**: The EC needs to put more efforts into software **Equal**: No change.
Efforts for registration	Indicates the change in the efforts the user has to put into registration processes **Less**: Less efforts for registration processes **Higher**: Higher efforts for (additional) registration processes **Equal**: No change.

Usage fees	Indicates the change in the usage fees for the service **Less**: EC has to pay less usage fees **Higher**: EC has to pay more usage fees **Equal**: No change.
Registration fees	Indicates the change in the registration fees for the service **Less**: EC has to pay less registration fees **Higher**: EC has to pay more registration fees **Equal**: No change.

Table 3.5: Costs and Benefits of SP and IdMSP Cost-Benefit Dimension "Cost Structure"

Key Partners	Indicates the change in associations with other service providers especially in exploitable synergies **Less**: Lower efforts for providing service **Higher**: Higher efforts for providing service **Equal**: No change.
Key Activities	Indicates the changes in key activities (e.g. implementation efforts) **Lower**: Lower efforts for key activities **Higher**: Higher efforts for key activities **Equal**: No changes.
Key Resources	Indicates the changes in required resources (e.g. hardware or software) **Lower**: Lower efforts for less required resources. **Higher**: Higher efforts for additional required resources. **Equal**: No changes.

Table 3.6: Costs and Benefits of SP and IdMSP Cost-Benefit Dimension "Revenue Streams"

Customer Relationships	Indicates the changes in relationships to end customers **Less**: Less revenue streams from end customer. **Higher**: Higher revenue streams from end customer **Equal**: No changes.
Distribution Channels	Indicates the changes in available distribution channels **Less**: Less revenue streams from end customer. **Higher**: Higher revenue streams from end customer **Equal**: No changes
Customer Segments	Indicates the changes in marketing effectiveness and monetization of customer information **Less**: Less revenue streams from end customer. **Higher**: Higher revenue streams from end customer **Equal**: No changes

Table 3.7: Costs and Benefits of SP and IdMSP Cost-Benefit Dimension “External Risks”

Risk of Technological Change	Indicates the changes in risk of not staying up-to-date with technological evolutions **Lower**: Lower risk of staying up-to-date with technological evolutions **Higher**: Higher risk of staying up-to-date with technological evolutions **Equal**: No changes.
Customer Demand	Indicates the changes in risk of not staying up-to-date with demand evolutions of end customers **Lower**: Lower risk of staying up-to-date with demand evolutions of end customers **Higher**: Higher risk of staying up-to-date with demand evolutions of end customers **Equal:** No changes**.**
Legal Environment	Indicates the changes in risk of being compliant with evolutions in regulation **Lower**: Lower risk of staying compliant with evolutions in regulation **Higher**: Higher risk of staying compliant with evolutions in regulation **Equal:** No changes.
Social Environment	Indicates the changes in risk of not maintaining the corporate image during social evolutions **Lower**: Lower risk of maintaining the corporate image during social evolutions **Higher**: Higher risk of maintaining the corporate image during social evolutions **Equal:** No changes**.**
Competitive Forces	Indicates the changes in risk of not overcoming challenges by competitive evolutions **Lower**: Lower risk of overcoming challenges by competitive evolutions **Higher**: Higher risk of overcoming challenges by competitive evolutions **Equal:** No changes.

Key Costs and Benefits

Key costs and benefits are a subset of all costs and benefits. Key costs and benefits are those costs and benefits that are considered to be relevant for the investment or market launch decision. Only key costs and benefits influence the decision maker’s overall decision. Non-key costs and benefits will be excluded from the valuation.

Cost/Benefit Values

Cost/benefit values represent the qualitative or quantitative economic value of a cost or benefit for a respective stakeholder.

Dimension Values

Dimension values represent the aggregated qualitative or quantitative economic value of all cost/benefit values clustered into a dimension.

Decision Values

Decision values of each perspective represent the aggregated qualitative or quantitative value of all dimension values.

Cause-Effect Chains

Cause-effects chains are used to model interdependent effects between costs and benefits of all stakeholders. Further, cause-effect chains make it possible to aggregate single cost/benefit values to dimension values, and dimension values to decision values for each stakeholder, which in turn can be represented by a one-dimensional decision value of the decision maker. Whereas the perspectives of each stakeholder and the dimensions of each perspective are pre-determined by the method, cause-effect chains and costs and benefits are shaped by the decision-maker based on experience and logical reasoning.

Weighting Factors for Cause-Effect Chains

The decision maker weights cause-effect chain elements, when mapping the causing values to caused values. The causing value is first multiplied with the weighting factor and then added to the caused value. The weight of a causing value must be ≥ 0 and ≤ 1. The sum of the weights of all values of each perspective or stakeholder must be 1.

3.3 Process Steps of the Method – The Procedural Perspective

This section presents the method from the procedural perspective. To demonstrate each step of the approach in a more pragmatic and less abstract way, they will be consistently applied to the following example use case: An IdMSP has to decide whether to invest in the provision of a new privacy-enhancing age verification service for end customers of online casino providers. Further IdM service scenarios will be evaluated in more detail in Chapter 4.

3.3.1 Step 1 - Description of the Baseline Option and Delta Options

In the first step, the IdMSP describes the status quo of the examined IdM Service. This mainly comprises a description of how a specific IdM Service is currently implemented in practice by other providers. This status quo scenario is called the Baseline Scenario (BS). Thus, the Baseline Option (BO) represents the decision alternative not to provide any of the alternative IdM Services at all. After the description of the BS, the IdMSP needs to describe all alternative scenarios of the IdM Service that shall be considered to enhance the Baseline Scenario. These alternative scenarios are here called the Delta Scenarios (DS). Analogous to the Baseline Option, a Delta Option (DO) represents the decision alternative to invest in one of the DSs. For performing Step 1, we recommend using established measures, such as UML diagrams. Especially sequence diagrams reveal valuable information on information flows between the stakeholders and also on required process steps. In the following, we present the Baseline Scenario (BS) and the two Delta Scenarios (DS) with such sequence diagrams.

Demonstration of Step 1

In this example, the decision maker (the IdMSP) identified two alternative designs for an enhanced age verification service (AgeVer): Delta Scenario 1 (DS1) and Delta Scenario 2 (DS2). In this case, the IdMSP has the following options to act in the IdM ecosystem: Invest in DO1, in DO2 or do not invest at all (BO). The IdMSPs decision for the BO would leave the state of the resulting environment unchanged as shown in Figure 3.1.

In this example, the end customer of an online casino needs to provide the online casino provider with a valid proof of his age. The end customer provides this information by, e.g., entering his date of birth into a special web form. This process has to be replicated for any age-based service the end customer wants to use.

Opting for DO1 would result in the modified market situation represented by DS1 (Figure 3.2). To use the age verification service, the end customer needs to create an account with the IdMSP and needs to provide a valid proof for his date of birth. This usually will involve an external age verification process. After being successfully registered with the IdMSP, a verified legal age certificate will be provided by the IdMSP. The end customer can use this certificate at any point in time and without the involvement and the knowledge of the IdMSP in order to verify its legal age to the online casino provider. The end customer can request additional verified legal age certificates to be presented to other age-based services. Alternatively, the IdMSP could issue generic, service provider independent credentials, e.g., in the form of an anonymous credential [CL01].

Opting for DO2 would result in a modified market situation represented by DS2 (Figure 3.3).

In DS2, the end customer needs to create an account with the IdMSP and provide a valid proof for his date of birth with the help of an external age verification process. After successful registration, when the end customer wants to use the online casino service, he provides the online casino provider a reference to his age verification provider. The online casino provider then requests the IdMSP for verified age information. Thus, the end customer is not involved in the age verification process.

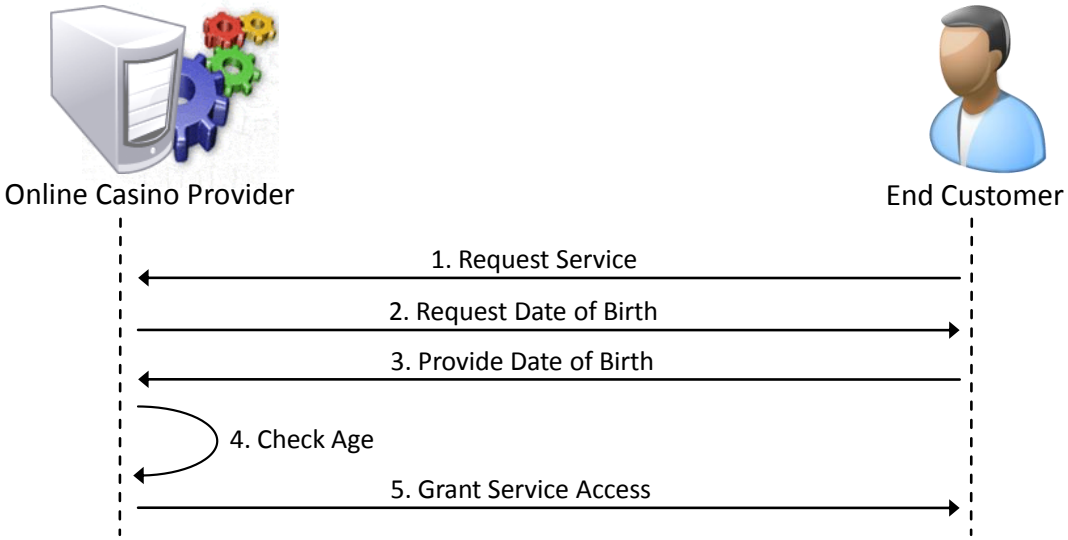

Figure 3.1: AgeVer - Baseline Scenario

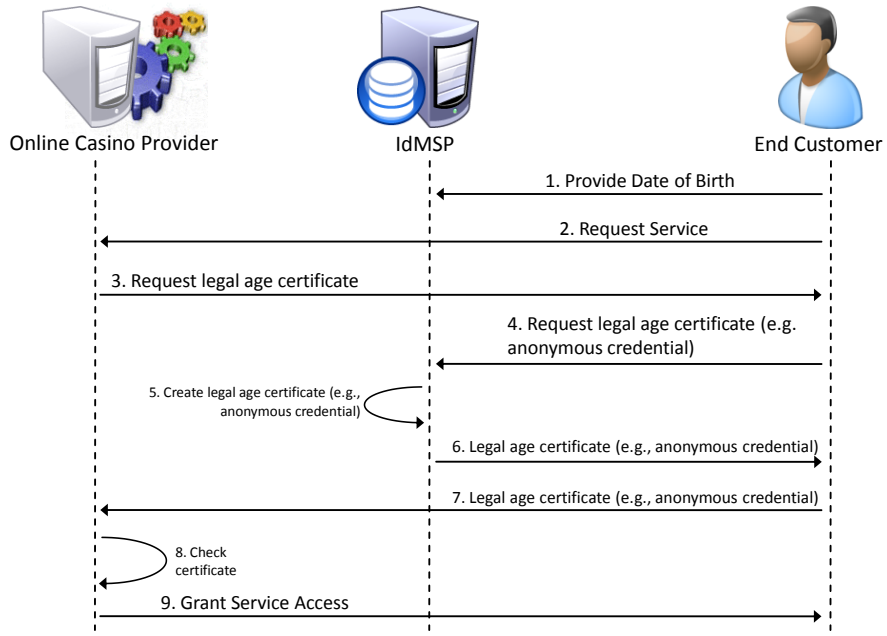

Figure 3.2: AgeVer - Delta Scenario 1

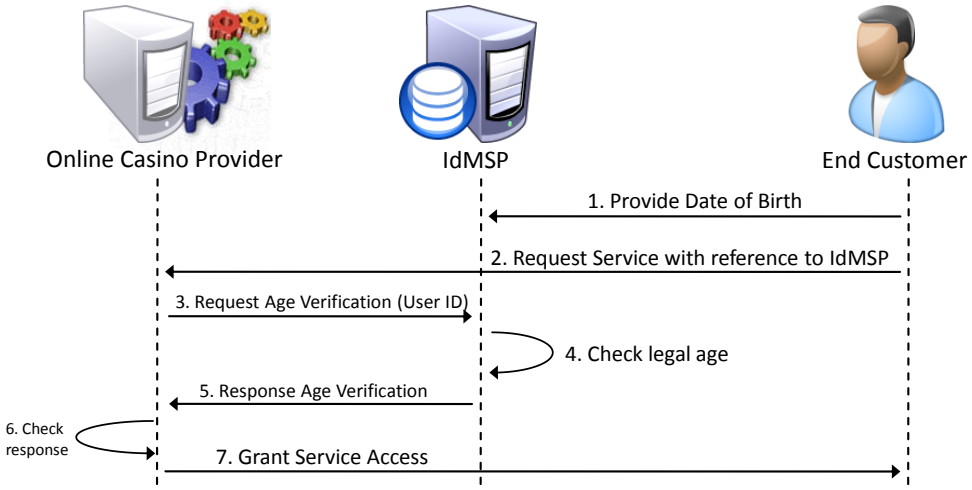

Figure 3.3: AgeVer - Delta Scenario 2

3.3.2 Step 2 - Identification of each Stakeholder's Costs and Benefits

The anticipated impacts and the expected costs and benefits of a specific scenario are crucial factors for decision making. Therefore, the corresponding costs and benefits need to be identified for all DS'. During this step, the BS has to be taken as the reference value (the baseline). That allows for the prediction and valuation of the consequences of the DS' in the form of costs and benefits. This step of the method can be performed by experts or by the usage of an appropriate explanatory model. As the costs and benefits of the IdMSP partially depend on the costs and benefits of the other market players (end customers and service providers), these have also to be anticipated and evaluated in this step. Using the cost/benefit dimensions and the cost and benefit items introduced in Section 3.2 helps performing this step in a structured way. Further, this will make the comparison between different scenarios easier.

Demonstration of Step 2

The identified costs and benefits are described in a way that they express the expected economic changes that result from introducing a respective DS based on the BS. Each identified cost and benefit has an influence on the overall benefit that is expected. The results of the example execution of step two are presented in Figure 3.4 and Figure 3.5. In this table, the three main columns represent the perspectives of the stakeholders “End Customer”, “Service Provider”, and “IdM Service Provider”. In these columns, the costs and benefits are listed according to the cost/benefits dimensions. Costs are labelled with a “**+”,** benefits are labelled with a **“-“.** Cost/Benefits items where no changes occurred compared to the Baseline Scenario are labelled with a “●”.

Age Verification Service Scenario - Delta Option 1 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
+ Higher data minimization by less required data
− Less anonymity by additional party (IdMSP) involved
− Less unlinkability by usage of age certificate (IdMSP)
● Equal undetectability
● Equal unobservability
− Less pseudonymity by usage of age certificate (IdMSP)

Risks
− Higher risk of unavailability of service by more required infrastructure
− Higher risk of data misuse by additional party (IdMSP)
− Higher risk of service failure by additional process and communication errors
+ Lower risk of efforts for inspection and correction of transactions by IdMSP-issued age certificate
● Equal acceptance risk
+ Lower financial risk by IdMSP-issued age certificate
+ Lower risk of frauds by IdMSP-issued age certificate
+ Lower risk of identity thefts by IdMSP-issued age certificate

Performance
● Equal potential for international usage
− Higher transaction duration by additional process steps
● Equal usability
● Equal 24/7 usage
● Equal SP acceptance
+ More possibilities to abort transaction by additional process steps
+ More possibilities to inspect transactions by additional logs
+ More possibilities for bonus programs by additional party (IdMSP)
+ More control over authentication process by additional parameters

Efforts
● Equal hardware efforts
− Higher efforts by additional registration process (IdMSP)
− Higher efforts by additional usage fees (IdMSP)
− Higher effort by additional registration fee (IdMSP)
− Higher efforts by higher transaction duration
● Equal software efforts

Service Provider (SP)

Key Partners
+ Lower customer efforts by additional key partner (IdMSP's end customer base)

Key Activities
− Higher implementation and operation efforts by age certificate verification process

Key Resources
● Equal implementation and operation efforts

Customer Relationships
● Equal revenues

Distribution Channels
+ Higher revenues by additional distribution channel (IdMSP)

Customer Segments
● Equal revenues

Technological Change
+ Lower risk by using additional up-to-date technology

Customer Demand
+ Lower risk by additional end customer satisfaction (privacy needs)

Legal Environment
+ Lower risk of being compliant by IdMSP-issued age certificate

Social Environment
+ Lower risk by better end customer image (privacy)

Competitive Forces
+ Lower risk of competitors by additional value added service (privacy)

IdM Service Provider (IdMSP)

Key Partners
+ Lower customer efforts by additional key partner (SP's customer base)

Key Activities
− Higher implementation and operation efforts by additional processes

Key Resources
− Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
+ Higher revenues by additional customers and stronger lock-in effects

Distribution Channels
+ Higher revenues by additional distribution channel (SP)

Customer Segments
+ Higher revenues by additional information about customers

Technological Change
+ Lower risk by providing up-to-date technology

Customer Demand
+ Lower risk by additional customer satisfaction (privay needs)

Legal Environment
− Higher risk of being compliant by offering advanced privacy technologies

Social Environment
+ Lower risk by better customer image (innovative)

Competitive Forces
+ Lower risk of competitors by additional value added service (privacy)

Figure 3.4: AgeVer - Identification of Costs and Benefits (DO1 vs. BO)

Age Verification Service Scenario - Delta Option 2 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
+ Higher data minimization by less required data
− Less anonymity by additional party (IdMSP) involved
− Less unlinkability by usage of age certificate (IdMSP)
− Less undetectability by additional process steps
● Equal unobservability
− Less pseudonymity by usage of age certificate (IdMSP)

Risks
− Higher risk of unavailability of service by more required infrastructure
− Higher risk of data misuse by additional party (IdMSP)
− Higher risk of service failure by additional process and communication errors
+ Lower risk of efforts for inspection and correction of transactions by IdMSP-issued age certificate
● Equal acceptance risk
+ Lower financial risk by IdMSP-issued age certificate
+ Lower risk of frauds by IdMSP-issued age certificate
+ Lower risk of identity thefts by IdMSP-issued age certificate

Performance
● Equal for international usage
− Higher transaction duration by additional process steps
+ Higher usability by less process steps for end customer
● Equal 24/7 usage
● Equal acceptance
− Less possibilities to abort transaction by less process steps for end customer
+ More possibilities to inspect transactions by central log
+ More possibilities for bonus programs by additional party (IdMSP)
− Less control about data handling by less process steps for end customer

Efforts
● Equal hardware efforts
− Higher efforts by additional registration processes
− Higher efforts by additional usage fees (IdMSP)
− Higher effort by additional registration fee (IdMSP)
− Higher efforts by higher transaction duration
● Equal software efforts

Service Provider (SP)

Key Partners
+ Lower customer efforts by additional key partner (IdMSP's end customer base)

Key Activities
− Higher implementation and operation efforts by additional process steps

Key Resources
− Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
+ Higher revenues by stronger lock-in effects and more potential customers

Distribution Channels
+ Higher revenues by additional distribution channel (IdMSP)

Customer Segments
● Equal revenues

Technological Change
− Higher risk of selecting wrong technologies (IdMSP)

Customer Demand
+ Lower risk by additional satisfaction of end customers usability and privacy needs

Legal Environment
+ Lower risk of being compliant by outsourcing age verification processes

Social Environment
+ Lower risk by better end customer image (usability and privacy)

Competitive Forces
+ Lower risk of competitors by value added service

IdM Service Provider (IdMSP)

Key Partners
+ Lower customer efforts by additional key partner (SP's customer base)

Key Activities
− Higher implementation and operation efforts by additional processes

Key Resources
− Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
+ Higher revenues by additional customers and stronger lock-in effects

Distribution Channels
+ Higher revenues by additional distribution channel (SP)

Customer Segments
+ Higher revenues by additional information about customers

Technological Change
− Higher risk by providing wrong technologies

Customer Demand
+ Lower risk by additional customer satisfaction (usability and privacy needs)

Legal Environment
− Higher risk of being compliant by offering privacy and usability technologies

Social Environment
+ Lower risk by better customer image (privacy and usability)

Competitive Forces
+ Lower risk of competitors by additional value added service (privacy and usability)

Figure 3.5: AgeVer - Identification of Costs and Benefits (DO2 vs. BO)

3.3.3 Step 3 - Selection of Key Costs and Benefits

To reduce the overall complexity, in this step, the IdMSP has to reduce the set of costs and benefits to a subset of key costs and key benefits for each stakeholder. The IdMSP excludes all costs and benefits he does not consider as relevant for its decision.[26] As the following steps of the method (steps 4 - 6) are based on this reduced subset of costs and benefits, the selection of key costs and key benefits is crucial for the overall result. There is no strict rule for performing this step, since the results are highly dependent on the decision maker's preferences and perceptions. Since Step 3 is performed after the costs and benefits have been identified for *each* Delta Scenario, one potential way of selecting key costs and benefits is to exclude any cost/benefit item that has the same value in all Delta Scenario valuations. The rationale behind that is that these items will not have an impact on the overall valuation.

Demonstration of Step 3

Figure 3.6 and Figure 3.7 show the result of the example application of this step of the method. Non-key costs and benefits are greyed out. In our example we followed the strategy of excluding all cost/benefit items that have the same value in each Delta Scenario valuation. For example, the cost/benefit item "risk of unavailability" has been rated as higher in both, DO1 and DO2. Thus, this item will not be a distinguishing factor of any of the Delta Scenarios.

[26] Note that the result of this step is highly dependent on the decision maker's individual valuation of each cost and benefit.

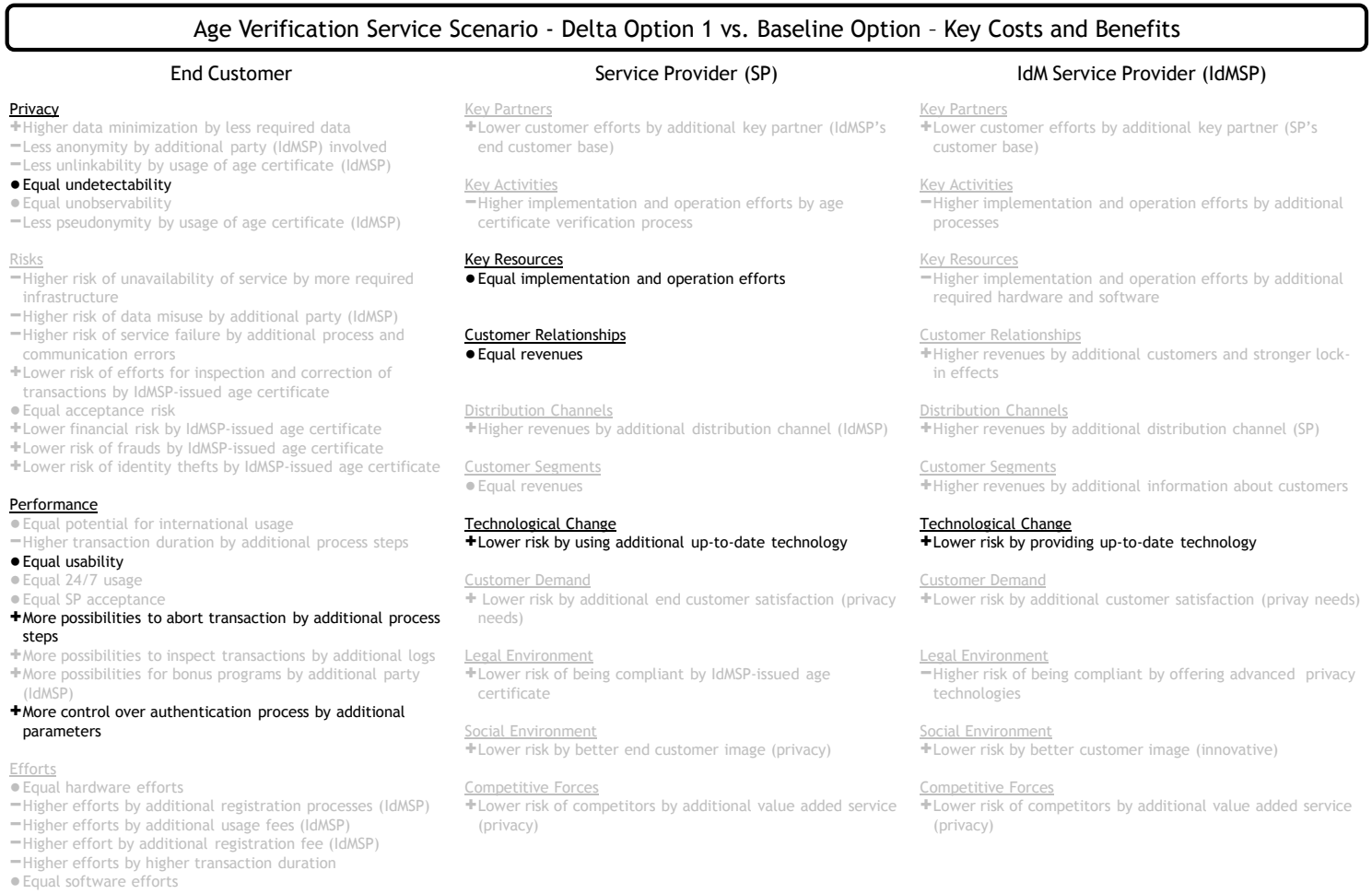

Figure 3.6: AgeVer - Selection of Key Costs and Benefits (DO1 vs. BO)

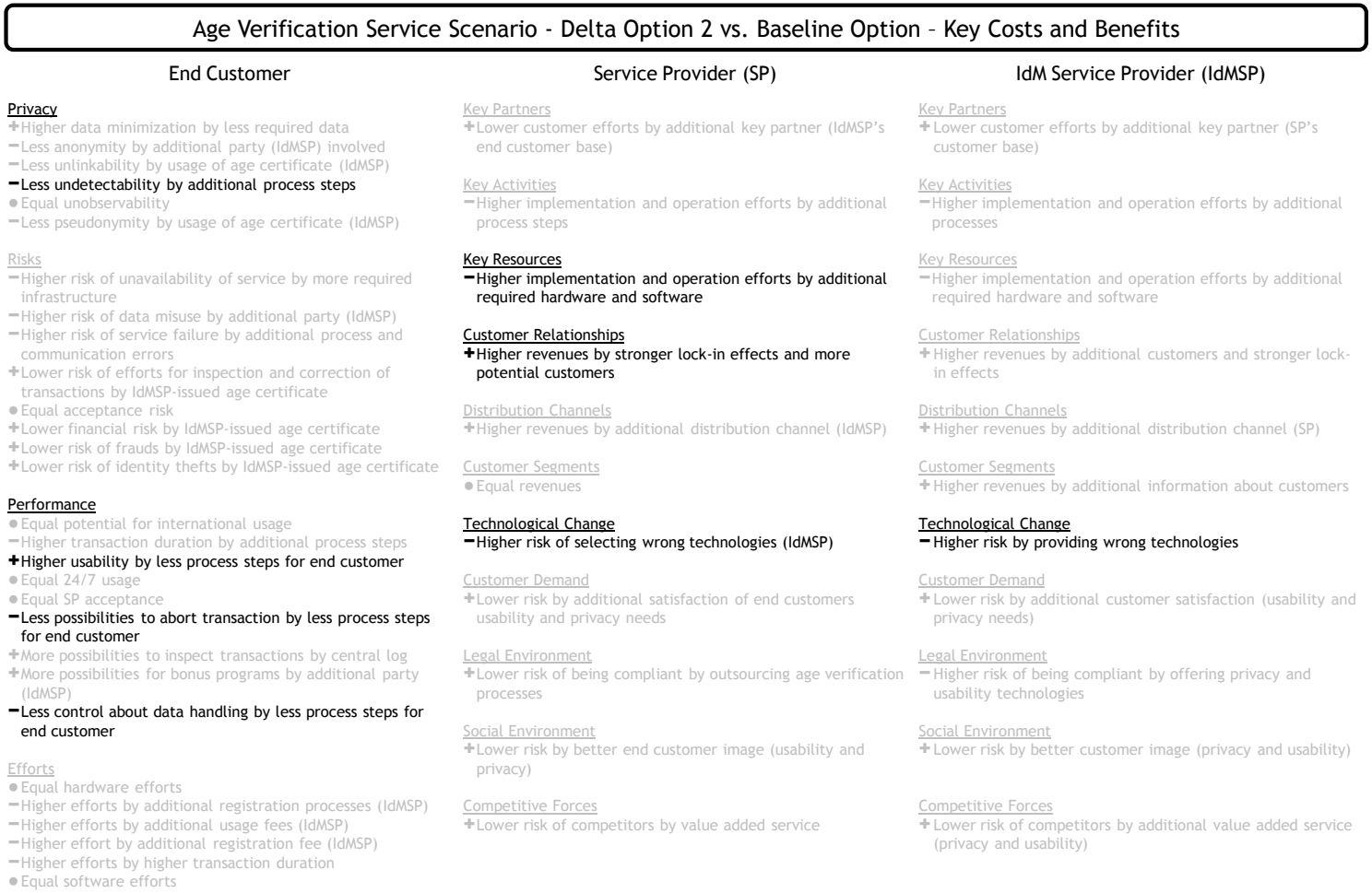

Figure 3.7: AgeVer - Selection of Key Costs and Benefits (DO2 vs. BO)

3.3.4 Step 4 – Clustering and Mapping of Key Cost and Benefits

The key costs and benefits identified for each stakeholder have to be mapped to the IdMSP by cause-effect chains. The central idea of cause-effect chains is to create a model of the resulting costs and benefits that particularly considers their interdependencies. A single cost or benefit of a market player causes economic effects on the respective market player itself and on all other players of that ecosystem. The aim of the cause-effect chains is to let all economic effects of the other market players flow into the IdMSP's costs and benefits. As a result, the IdMSP will get a set of mapped costs and benefits representing the economic consequences caused by the other market players. After mapping all costs and benefits to the IdMSP, Step 4 will usually result in a large set of different costs and benefits with a variety of scale units. To reduce complexity and ease the process, clustering by equal scale units or dimensions such as revenues, costs, or risks, to a (as small as possible) set of decision-relevant factors, is needed.

The clustering of all costs and benefits by similar scale units or by critical success factors that are relevant for the achievement of IdMSPs individual objectives, results in a set of costs and benefits that is easier to handle. With this clustering, the effects of a group of similar costs or benefits will be represented by a single effect in an aggregated form. For example, more new service providers and a higher degree of service provider loyalty will result in more revenue.

Demonstration of Step 4 (Clustering and Mapping)

All key costs and benefits derived in Step 3 (Section 3.3.3) will now be clustered and mapped step by step to the IdMSP (Figure 3.8 and Figure 3.9):

- Mapping end customer's key costs and key benefits to other costs and benefits of the end customer.
- Mapping end customer's costs and benefits to costs and benefits of the service provider.
- Mapping service provider's costs and benefits to costs and benefits of IdMSP.

The last two columns in the tables in Figure 3.8 and Figure 3.9 show the results of this step.

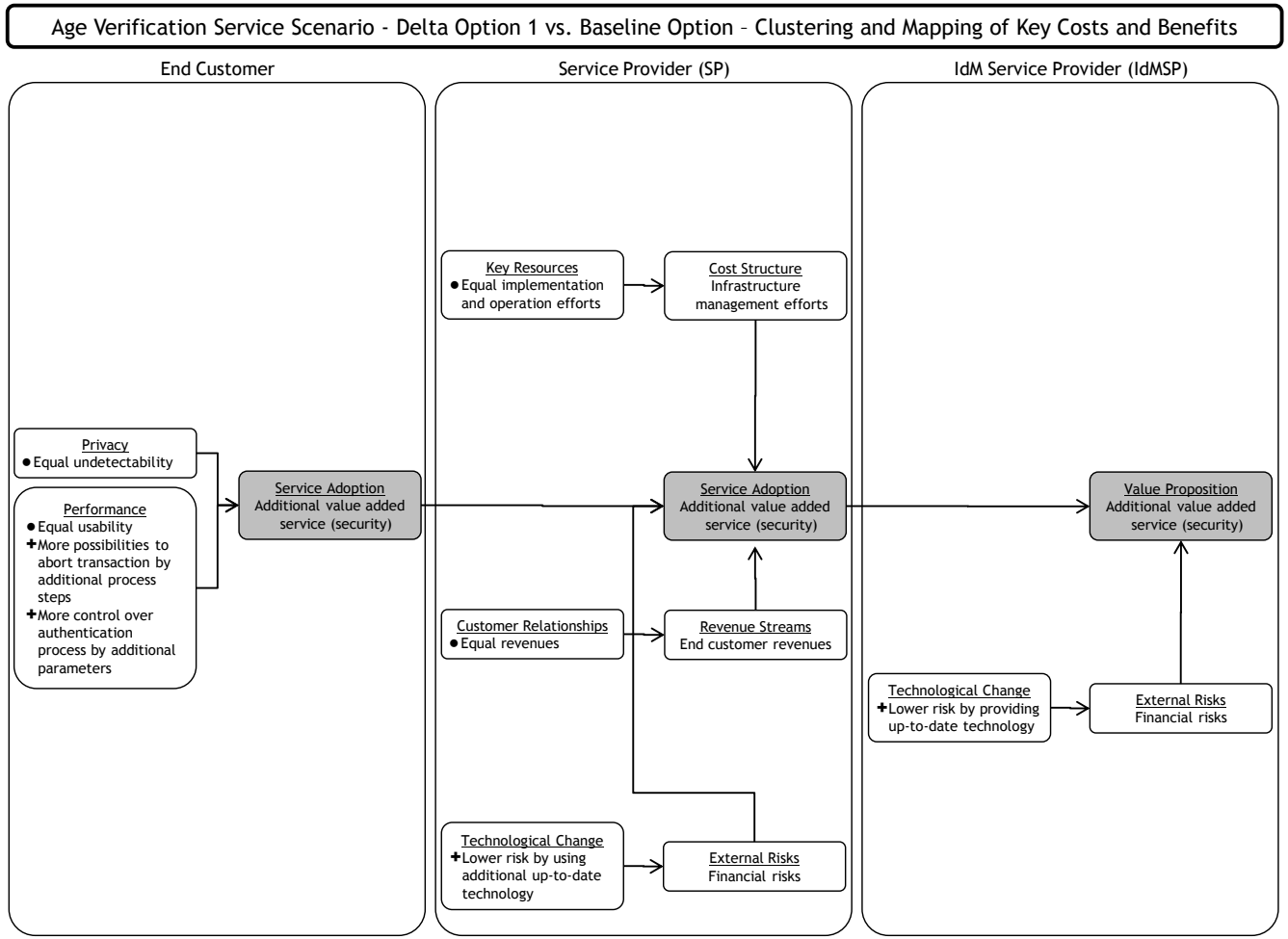

Figure 3.8: AgeVer - Clustering and Mapping of Key Costs and Benefits (DO1 vs. BO)

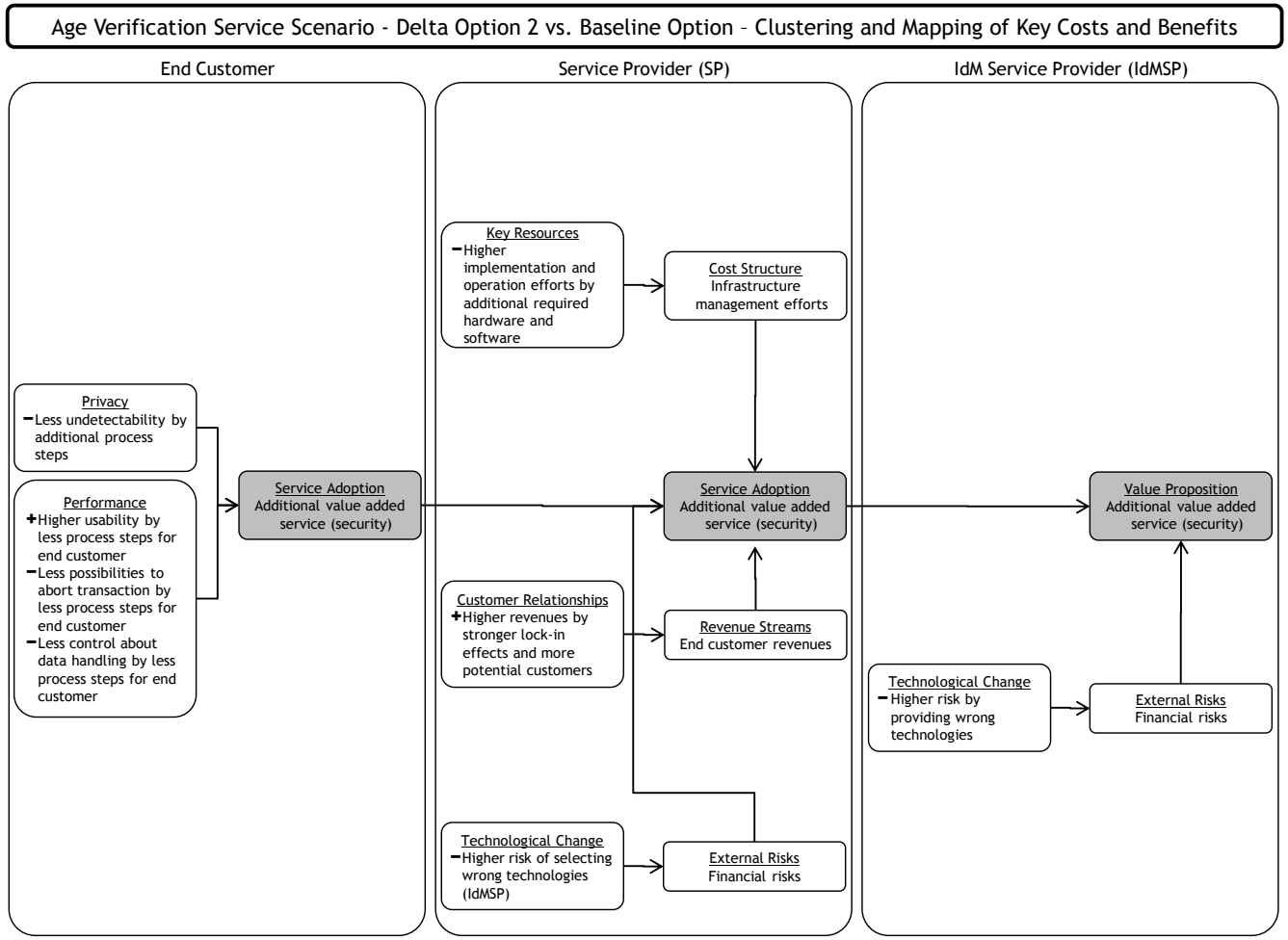

Figure 3.9: AgeVer - Clustering and Mapping of Key Costs and Benefits (DO2 vs. BO)

3.3.5 Step 5 - Assessment and Aggregation of Clustered Costs and Benefits

The effects resulting from the cost and benefit clustering in Step 4 (Section 3.3.4) can be positive or negative and of different importance to the IdMSP. Therefore the effects need to be aggregated to an overall effect for each of the chosen dimensions.

During the aggregation, each effect needs to be individually weighted by the IdMSP. Where applicable, this can be done by adding concrete values or ranges of values for each effect, but usually the aggregation will be based on appropriate scales or grades defined by experts of the IdMSP, such as very good (+ +), good (+), medium (0), bad (-), and very bad (- -).

Demonstration of Step 5

Based on the results of Step 4, the IdMSP now assesses the intensity of each dimension influencing effect by using the abstract value classes negative (-), equal (●), and positive (+). For example, for the comparison between the DS1 and the BS (Figure 3.10 and Figure 3.11), the decision maker rates the end customer's effect "undetectability" as equal (●), the effect "more possibilities to abort transactions by additional process steps" as positive (+), and the effect "more control over authentication process by additional parameters" as positive (+). At the end, and under the assumption that each effect has the same influence (weighting factor = 1) on the end customer's Decision Value "Service Adoption", the decision maker expects the end customer to adopt DS1 with an overall Service Adoption value of +2 (e.g. medium positive), when it opts for DO1. Based on the IdMSP's preferences for each dimension and the results shown in Figure 3.11, the IdMSP can now deduce the decision whether or not it should provide its age verification service as represented by DO1.

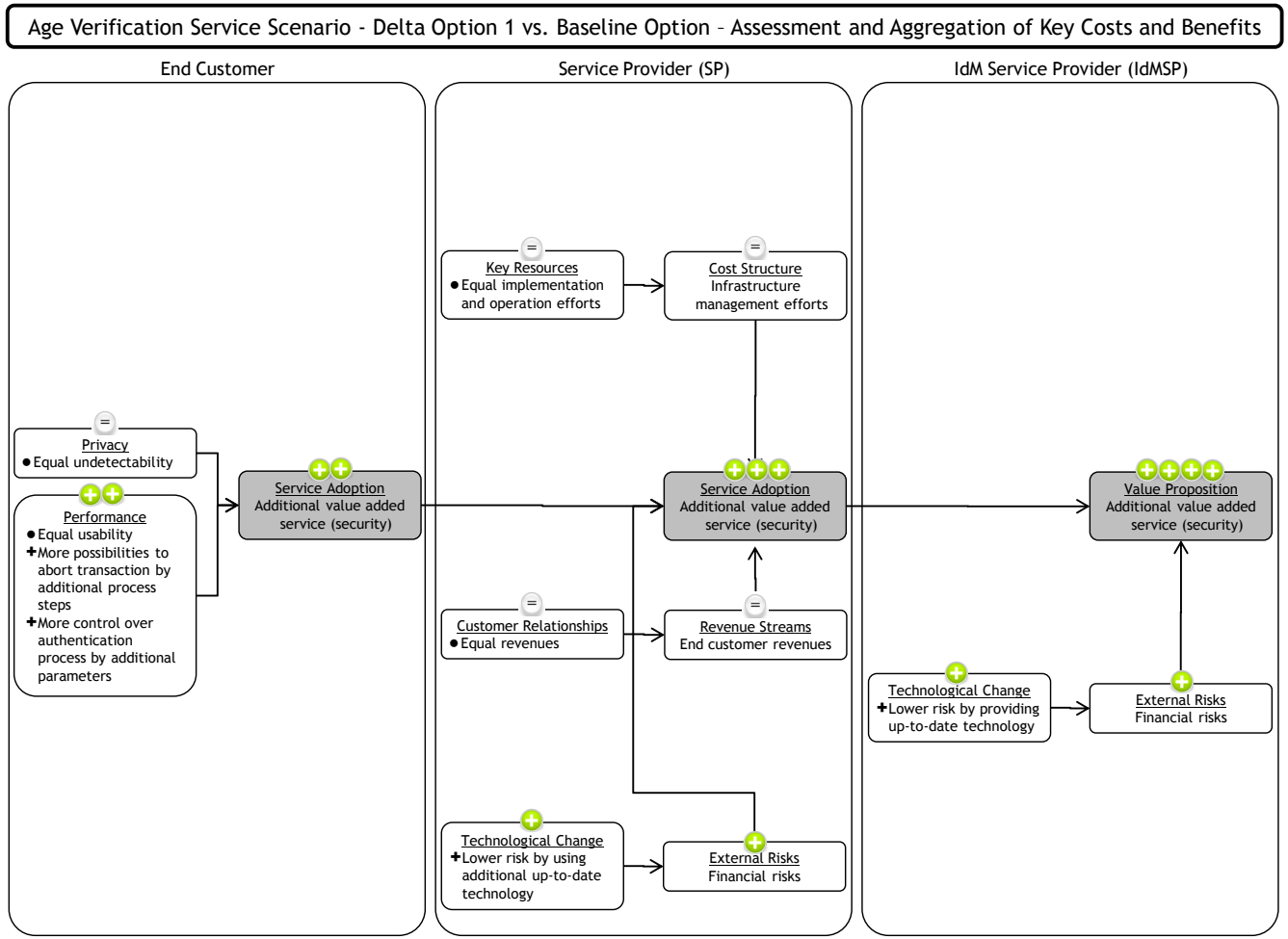

Figure 3.10: AgeVer - Assessment and Aggregation of Key Costs and Benefits (DO1 vs. BO)

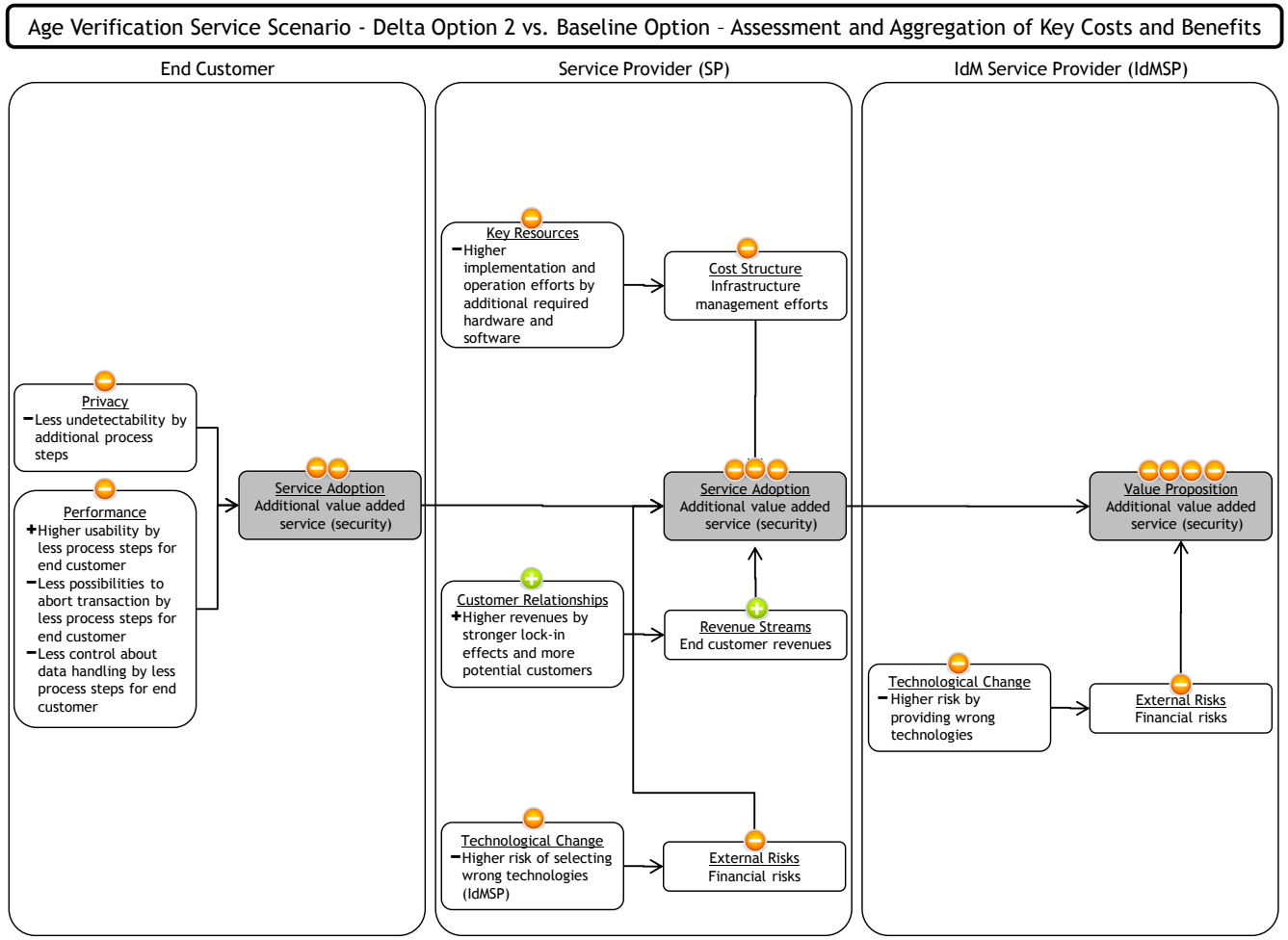

Figure 3.11: AgeVer - Assessment and Aggregation of Key Costs and Benefits (DO2 vs. BO)

3.3.6 Step 6 - Visualisation of Aggregated Costs and Benefits

Finally, the aggregated costs and benefits will be visualised in order to further simplify complex decision situations and to support the IdMSP. For this purpose, two figures need to be created: one for the aggregated dimension values (see Figure 3.12) and one for the decision values (see Figure 3.13). The first figure visualizes for each stakeholder the aggregated dimension values with bar charts. We recommend plotting the values of both valuation results (DO1 vs. BO and DO2 vs. BO). This allows a direct comparison between both delta scenarios. The second figure visualizes for each valuation (DO1 vs. BO and DO2 vs. BO) the resulting decision values for each stakeholder,

Demonstration of Step 6

Visualisation example (see Figure 3.12 and Figure 3.13): Based on the results of Step 6, the IdMSP should also valuate the relative advantages of its DOs as shown in Figure 3.13. We want to emphasize that the scales used in this figures are not linear, that is e.g. a dimension value "revenue streams" rated +4 does not imply twice as much revenue as with a dimension value "revenue streams" of +2. Thus, these scales are more appropriate for ranking purposes. Figure 3.13 implies that the decision maker opts for DO1 with the IdMSP's decision value of +4. The decision maker will not opt for DO2, however, because the IdMSP has a negative decision value of -4.

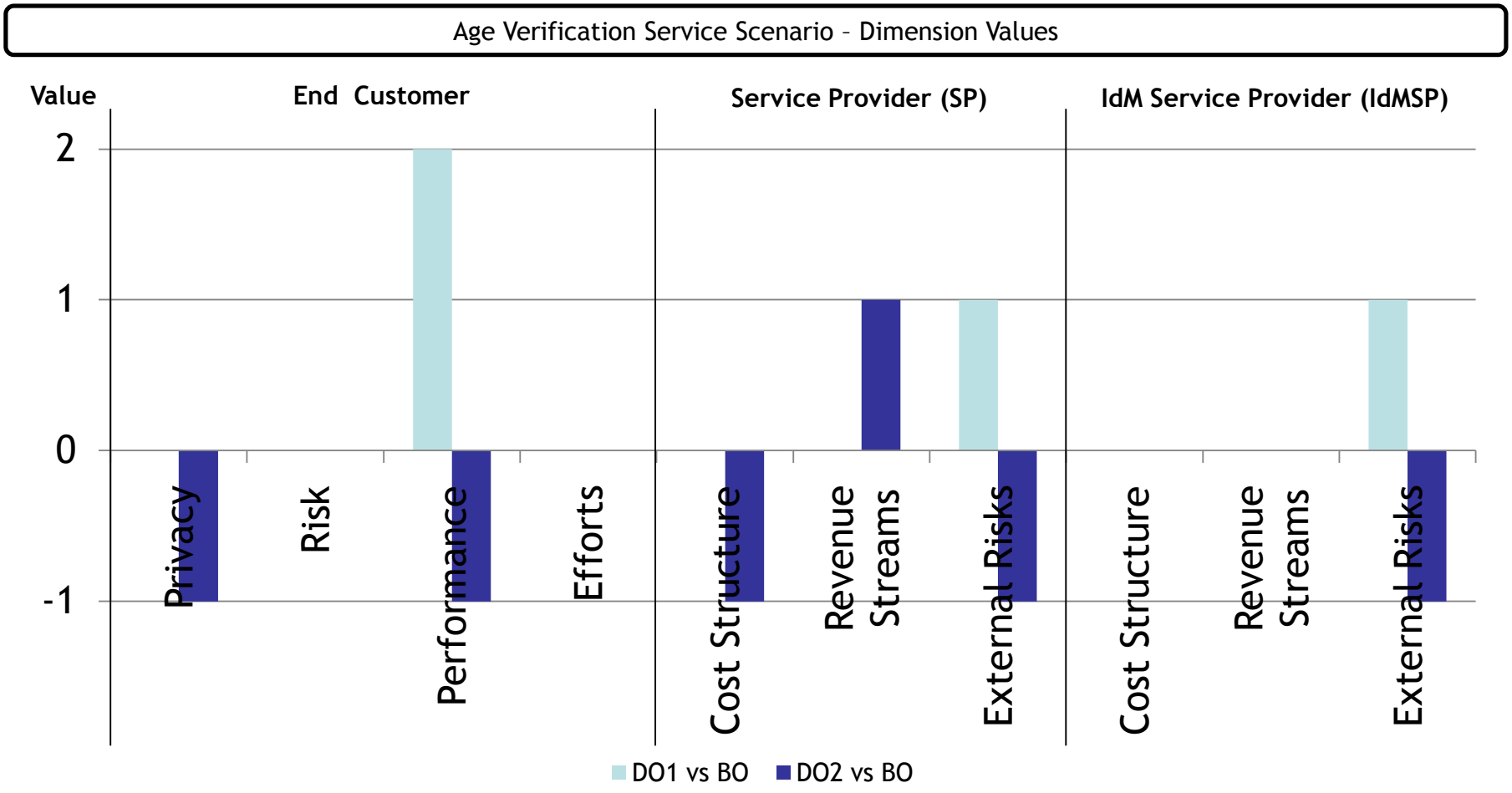

Figure 3.12: AgeVer - Visualization of Dimension Values

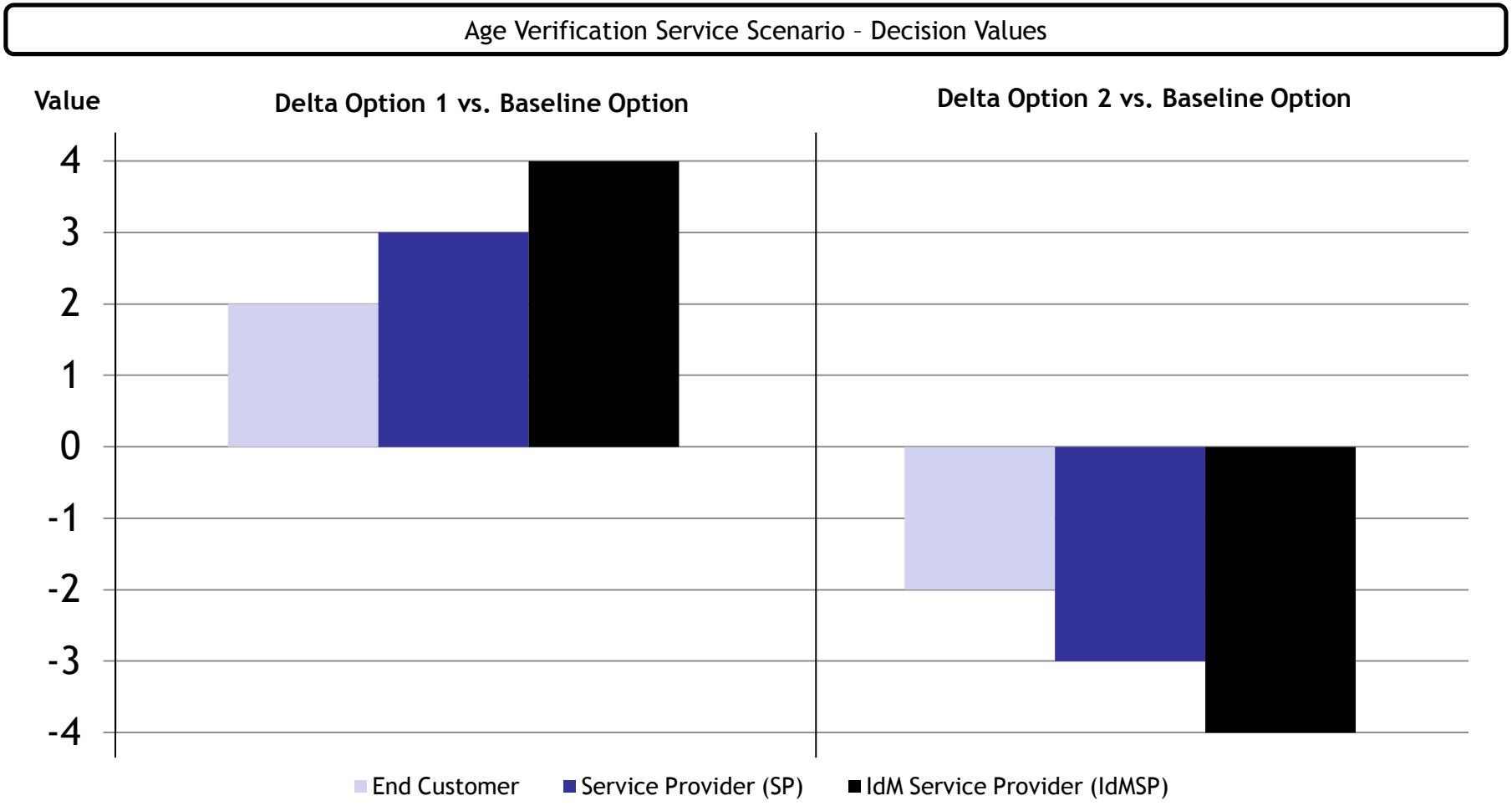

Figure 3.13: AgeVer - Visualization of Decision Values

Chapter 4

Application of the Method

The method presented in Section 3 can be applied to a variety of IdM services. Step 1 of the method requires the IdMSP to describe the BS and the DS'. In Section 3.3, a first IdM service scenario with its BS and DSs has been presented (age verification). To demonstrate the performance of the valuation method further, this chapter provides guided step-by-step executions on two additional IdM service scenarios: Authentication (sec. 4.1) and Privacy Policy Enforcement (sec. 4.2). For each step, the valuation result is presented in the form of figures. Additional explanations for some steps are provided in text form. We want to emphasize that the method is not deterministic, that is the results of our example execution represent *one* possible outcome. This is due to some steps' dependency on contextual factors, such as the operation environment, the decision maker's attitudes, or others. Nevertheless, we believe that these two examples will guide decision makers when using the method.

4.1 Evaluating the IdM Enabler "Authentication"

Authentication is an essential IdM function in online and offline scenarios. Due to its nature, implementations of authentication mechanisms have to be reliable and secure. Therefore, different authentication types exist for different scenarios. In the following, we present three possible authentication designs, the Baseline Option (BO) and two Delta Options (DO).

4.1.1 Step 1 – Description of Baseline Option and Delta Options

In this step, the decision maker has to design the service scenarios to be evaluated. We recommend doing this with established measures, such as UML diagrams. Especially sequence diagrams reveal valuable information on information flows between the stakeholders and also on required process steps. In the following, we present the Baseline Scenario (BS) and the two Delta Scenarios (DS) with such sequence diagrams.

4.1.1.1 Authentication Baseline Scenario

The BS illustrated in Figure 4.1 represents the most commonly used authentication scheme in online scenarios. Before a session starts, the end customer provides his username (pseudonym) together with the password to the service provider. The service provider then authenticates the

user. Though, the service is enabled by the user providing the authentication credentials (IdM data asset) and the service provider processing the authentication (IdM functional capability).

4.1.1.2 Authentication Delta Scenario 1

A more sophisticated authentication scheme is DS1, illustrated in Figure 4.2. The most known implementations of this multi-factor authentication scheme can be found in online banking scenarios (mobile TAN, smsTAN, mTAN). In DS1, the Telco is the trusted third-party IdMSP. In the first step, after the end customer requests the service, the service provider requests the Telco to forward an authentication code to the mobile phone of the end customer (1). The authentication code is generated randomly on the fly and is valid for a short time frame. After the end customer receives this authentication code (2), he presents this second authentication credential to the service provider (the first authentication step was providing a username and password combination to the service provider). This authentication scheme requires that the service provider and the Telco negotiate a commonly used identifier for the respective user in the initial registration phase. Here, the essential IdM data asset (mobile phone number of the end customer) comes from the Telco, the IdM functional capability is on the service provider's side (processing the authentication). This scheme follows Privacy by Design principles, since the phone number of the end customer is not shared with the service provider.

4.1.1.3 Authentication Delta Scenario 2

DS2 (Figure 4.3) is a generalised single sign-on scenario. The user has an (SSO-) account with the Telco. If he wants to consume a specific service, he authenticates to the Telco. The Telco then provides the user an authentication token, which the end customer then forwards to the service provider. In this scheme, the essential IdM functional capability (processing the authentication) is implemented and provided by the Telco.

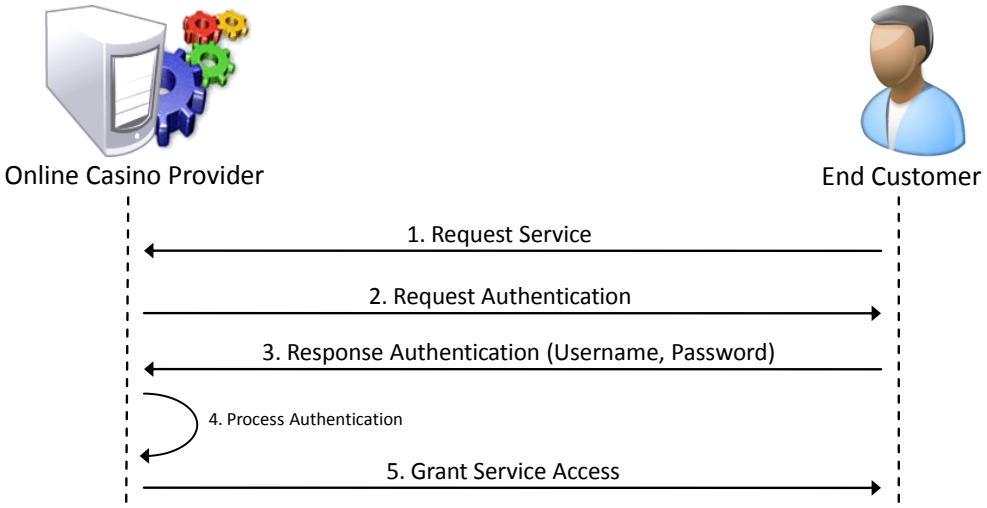

Figure 4.1: Auth – Baseline Scenario

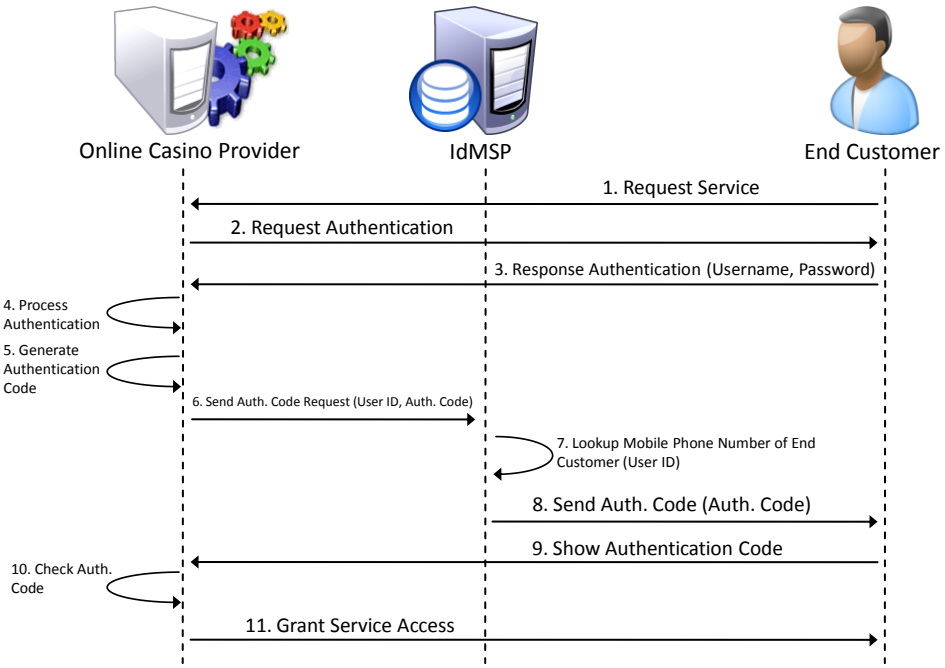

Figure 4.2: Auth - Delta Scenario 1

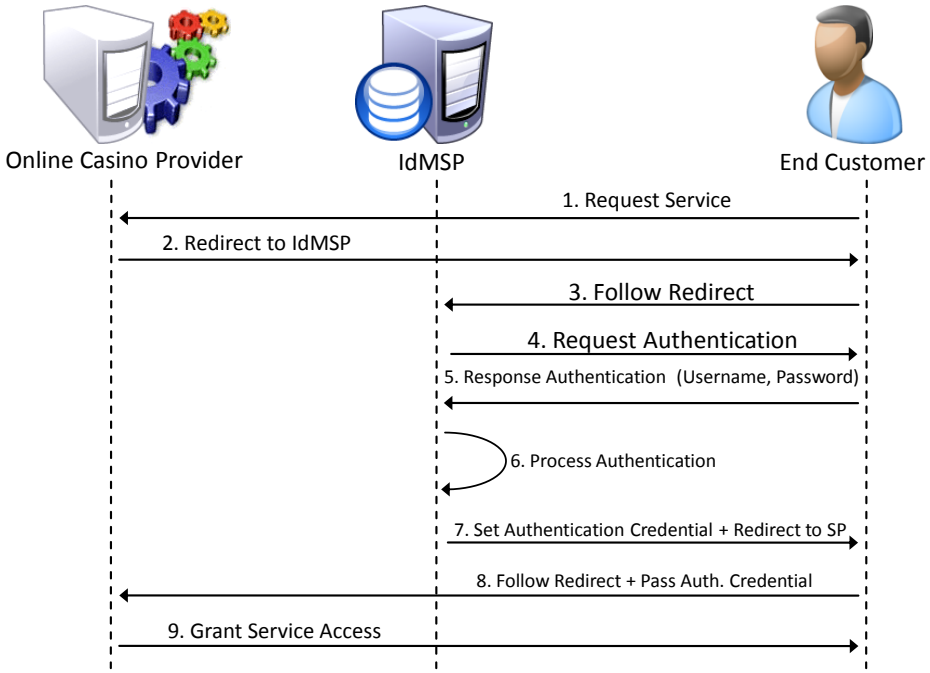

Figure 4.3: Auth - Delta Scenario 2

4.1.2 Step 2 - Identification of each Stakeholder's Costs and Benefits

Figure 4.4 shows the results of step 1 for DS1; Figure 4.5 shows the results of step 1 for DS2.

4.1.2.1 Delta Scenario 1

Table 4.1 provides for some selected cost and benefit items details on the reasoning behind the valuation.

Table 4.1: Identification of Costs and Benefits.

Valuation Item (Stakeholder/Dimension)	Description
Less Data Minimization by additional required data (EC/Privacy)	In this scenario, the end customer additionally provides his phone number to the IdMSP. Without this information, DS1 is not realizable. Thus, we have less data minimization for the end customer.
Less anonymity by additional party involved (EC/Privacy)	Compared to the BS, there is one more actor involved to the authentication process (the IdMSP). Thus, the IdMSP knows when the end customer uses a specific service. This decreases the anonymity level.
Less unlinkability by additional party involved (EC/Privacy)	Through the additional party (IdMSP) involved to the authentication, an "attacker" could link a service provider account with the phone number of the user.
Less undetectability by required data (EC/Privacy)	Through the additionally required data item "phone number", which is used to send the end customer the authentication code, an "attacker" can learn that this data item exists. In the BS, the phone number is not being processed.
Less unobservability by additional process step (EC/Privacy)	The authentication in DS1 consists of two main process steps. Thus, there are more process steps compared to the BS which increases the risk of observation.
Equal pseudonymity (EC/Privacy)	The end customer remains pseudonym.
Lower risk of identity thefts (EC/Risks)	Identity theft requires an attacker to compromise both, the password of the user and the mobile phone. In the BS, compromising the password is sufficient for identity theft.
Higher transaction duration by additional process step (EC/Performance)	Compared to the BS, the authentication process takes more time, since the end customer has to wait for the authentication code and provide it to the service provider.
Higher efforts by additional registration process (EC/Efforts)	In order to use this authentication service, the end customer has to register for it with the IdMSP. This is an additional registration step compared to the BS, where registration is only needed with the service provider.
Higher implementation and operation efforts by additional processes (SP/Cost Structure)	The service provider has to implement additional processes, such as authentication code generation and the interface to the IdMSP to request forwarding of the code to the end customer. Further, the authentication code verification has to be implemented.
Higher revenues by additional end customers and stronger lock-in effects (SP/Revenue Streams)	The provision of advanced authentication mechanisms strengthens lock-in effects, which in turn potentially lead to additional revenues.
Lower risk by using up-to-date technology (SP/External Risks)	Exploiting the capabilities of mobile phones to provide secure authentication obviates the risk of using outdated or insecure services.

Higher implementation and operation efforts by additional processes (IdMSP/Cost Structure)	The IdMSP has to implement new services and processes (e.g. an authentication code forwarding interface for service providers).
Higher revenues by additional distribution channel (IdMSP/Revenue Streams)	Through the new key partner (SP), the IdMSP has new distribution channels to promote its services.
Higher risk of being compliant by offering advanced security technologies (IdMSP/External Risks)	The IdMSP is now involved to the authentication process and therefore is responsible for being compliant with laws (e.g. data protection laws).
Lower risk by better customer image (IdMSP/External Risks)	With providing a secure and innovative authentication service, the IdMSP can improve its customer image.

4.1.2.2 Delta Scenario 2

Table 4.2 provides for some selected cost and benefit items details on the reasoning behind the valuation.

Table 4.2: Identification of Costs and Benefits.

Valuation Item (Stakeholder/Dimension)	Description
Higher Data Minimization by less required data (EC/Privacy)	Since the IdMSP acts as single sign-on provider, the end customer does not require registration with the service providers. Thus, the end customer does not need to provide personal data for registration.
Higher risk of identity thefts by multiple usage of credentials (EC/Risks)	This is due to the nature of SSO systems. If an attacker compromises the authentication credentials of the end customer, he has access to all services where these credential are used.
Higher usability by SSO functionalities (EC/Performance)	With SSO, the end customer can authenticate to a number of services with providing authentication credentials only one time.
Less efforts by less SP registration processes (EC/Efforts)	When using SSO, the creation of accounts with each service provider is not necessary.
Lower implementation and operation efforts by outsourced authentication process (SP/Cost Structure)	The whole authentication process is not required, since it is “outsourced”.
Lower revenues by weaker lock-in effects (SP/Revenue Streams)	Since the creation of an end customer account with the service provider is not required, service providers cannot establish strong customer relationships. Thus, it is easier for end customers to change the service provider.
Less revenues by less information about end customers (SP/Revenue Streams)	Since the creation of an end customer account with the service provider is not required, service providers have less information about their end customers that can be monetized (e.g. through advertising).
Higher implementation and operation efforts by additional processes (IdMSP/Cost Structure)	The IdMSP has to implement new services and processes (authentication processes and the management of authentication credentials).

Higher revenues by additional distribution channel (IdMSP/Revenue Streams)	Through the new key partner (SP), the IdMSP has new distribution channels to promote its services.
Higher revenues by additional information about end customers (IdMSP/Revenue Streams)	The IdMSP get new information about end customers (e.g. about services they use)
Higher risk by providing wrong technologies (IdMSP/External Risks)	The risk of providing the wrong SSO protocols, etc.
Higher risk of being compliant by offering advanced security technologies (IdMSP/External Risks)	The IdMSP is now involved to the authentication process and therefore is responsible for being compliant with laws (e.g. data protection laws)
Lower risk by better customer image (IdMSP/External Risks)	With providing a user-friendly and innovative authentication service, the IdMSP can improve its customer image.

Authentication Service Scenario - Delta Option 1 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
- − Less data minimization by additional required data
- − Less anonymity by additional party (IdMSP) involved
- − Less unlinkability by additional party (IdMSP) involved
- − Less undetectability by additional required data
- − Less unobservability by additional process step
- ● Equal pseudonymity

Risks
- − Higher risk of unavailability of service by more required infrastructure
- − Higher risk of data misuse by additional party (IdMSP)
- − Higher risk of service failure by additional process and communication errors
- − Higher risk of efforts by additional implementation and correction of transactions
- ● Equal acceptance risks
- + Lower financial risk by more secure service
- + Lower risk of frauds by more secure service
- + Lower risk of identity thefts by additional authentication token

Performance
- − Less potential for international usage by additional required mobile connection
- − Higher transaction duration by additional process steps
- − Less usability by additional processes
- ● Equal 24/7 usage
- ● Equal SP acceptance
- + More possibilities to abort transaction by additional process steps
- + More possibilities to inspect transactions by additional logs
- + More possibilities for bonus programs by additional party (IdMSP)
- + More control over authentication process by additional parameters

Efforts
- − Higher efforts by additional required hardware (mobile)
- − Higher efforts by additional registration process (IdMSP)
- − Higher efforts by additional usage fees (IdMSP)
- − Higher effort by additional registration fee (IdMSP)
- − Higher efforts by higher transaction duration
- ● Equal software efforts

Service Provider (SP)

Key Partners
- + Lower customer efforts by additional key partner (IdMSP's end customer base)

Key Activities
- − Higher implementation and operation efforts by additional processes

Key Resources
- − Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
- + Higher revenues by additional end customers and stronger lock-in effects

Distribution Channels
- + Higher revenues by additional distribution channel (IdMSP)

Customer Segments
- ● Equal revenues

Technological Change
- + Lower risk by using additional up-to-date and end customer friendly technology (mobile phone)

Customer Demand
- + Lower risk by additional end customer satisfaction (security needs)

Legal Environment
- + Lower risk of being compliant by using advanced security technologies

Social Environment
- + Lower risk by better end customer image (security)

Competitive Forces
- + Lower risk of competitors by additional value added service

IdM Service Provider (IdMSP)

Key Partners
- + Lower customer efforts by additional key partner (SP's customer base)

Key Activities
- − Higher implementation and operation efforts by additional processes

Key Resources
- − Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
- + Higher revenues by additional customers and stronger lock-in effects

Distribution Channels
- + Higher revenues by additional distribution channel (SP)

Customer Segments
- + Higher revenues by additional information about customers

Technological Change
- + Lower risk by providing up-to-date and customer friendly technologies

Customer Demand
- + Lower risk by additional customer satisfaction (security needs)

Legal Environment
- − Higher risk of being compliant by offering advanced security technologies

Social Environment
- + Lower risk by better customer image (innovative)

Competitive Forces
- + Lower risk of competitors by additional value added service (security)

Figure 4.4: Auth - Identification of Costs and Benefits (DO1 vs. BO)

Authentication Service Scenario - Delta Option 2 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
+ Higher data minimization by less required data
+ Higher anonymity by less required registration processes
− Less unlinkability by single point of knowledge
− Less undetectability by additional required data
− Less unobservability by additional process step
+ Higher pseudonymity by less required accounts at SP

Risks
− Higher risk of unavailability of service by more required infrastructure
+ Lower risk of data misuse by less required data
− Higher risk of service failure by additional process and communication errors
● Equal risk of efforts
● Equal acceptance risk
− Higher financial risk by lower security
− Higher risk of frauds by lower security
− Higher risk of identity thefts by multiple usage of credentials

Performance
● Equal for international usage
● Equal transaction duration
+ Higher usability by SSO functionalities
● Equal 24/7 usage
− Less SP acceptance by less control and less end customer data
● Equal possibilities to abort transaction
+ More possibilities to inspect transactions by central log
− Less possibilities for bonus programs by more end customer privacy
● Equal control about authentication process

Efforts
● Equal efforts for hardware
+ Less effort by less SP registration processes
● Equal usage fees
● Equal registration fees
+ Lower efforts by lower transaction durations
● Equal efforts for software

Service Provider (SP)

Key Partners
+ Lower customer efforts by additional key partner (IdMSP's end customer base)

Key Activities
+ Lower implementation and operation efforts by outsourced authentication processes

Key Resources
+ Lower implementation and operation efforts by less required hardware and software

Customer Relationships
− Lower revenues by weaker lock-in effects (no end customer account required at SP)

Distribution Channels
+ Higher revenues by additional distribution channel (IdMSP)

Customer Segments
− Lower revenues by less information about end customers and weaker relationship to the end customers

Technological Change
− Higher risk of selecting wrong technologies (IdMSP)

Customer Demand
+ Lower risk by additional satisfaction of end customers usability needs

Legal Environment
+ Lower risk of being compliant by outsourcing authentication processes of being compliant

Social Environment
+ Lower risk by better end customer image (usability)

Competitive Forces
+ Lower risk of competitors by value added service

IdM Service Provider (IdMSP)

Key Partners
+ Lower customer efforts by additional key partner (SP's customer base)

Key Activities
− Higher implementation and operation efforts by additional processes

Key Resources
− Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
+ Higher revenues by additional customers and stronger lock-in effects

Distribution Channels
+ Higher revenues by additional distribution channel (SP)

Customer Segments
+ Higher revenues by additional information about customers

Technological Change
− Higher risk by providing wrong technologies

Customer Demand
+ Lower risk by additional customer satisfaction (usability and privacy needs)

Legal Environment
− Higher risk of being compliant by offering privacy and usability technologies

Social Environment
+ Lower risk by better customer image (openness)

Competitive Forces
+ Lower risk of competitors by additional value added service (usability)

Figure 4.5: Auth - Identification of Costs and Benefits (DO2 vs. BO)

4.1.3 Step 3 – Selection of Key Costs and Benefits

In step 3, the decision maker has to reduce the set of costs and benefits to a subset of key costs and key benefits for each stakeholder. The IdMSP excludes all costs and benefits he does not consider relevant for its decision making. Figure 4.6 and Figure 4.7 show the result of step 3. In our case, we followed the strategy to exclude all costs and benefits which were valuated equally in both, DO1 vs. BO and DO2 vs. BO. In other words, costs and benefits that are neither dominant in DO1 nor in DO2 were excluded. Non-key costs and benefits are greyed out in the figures.

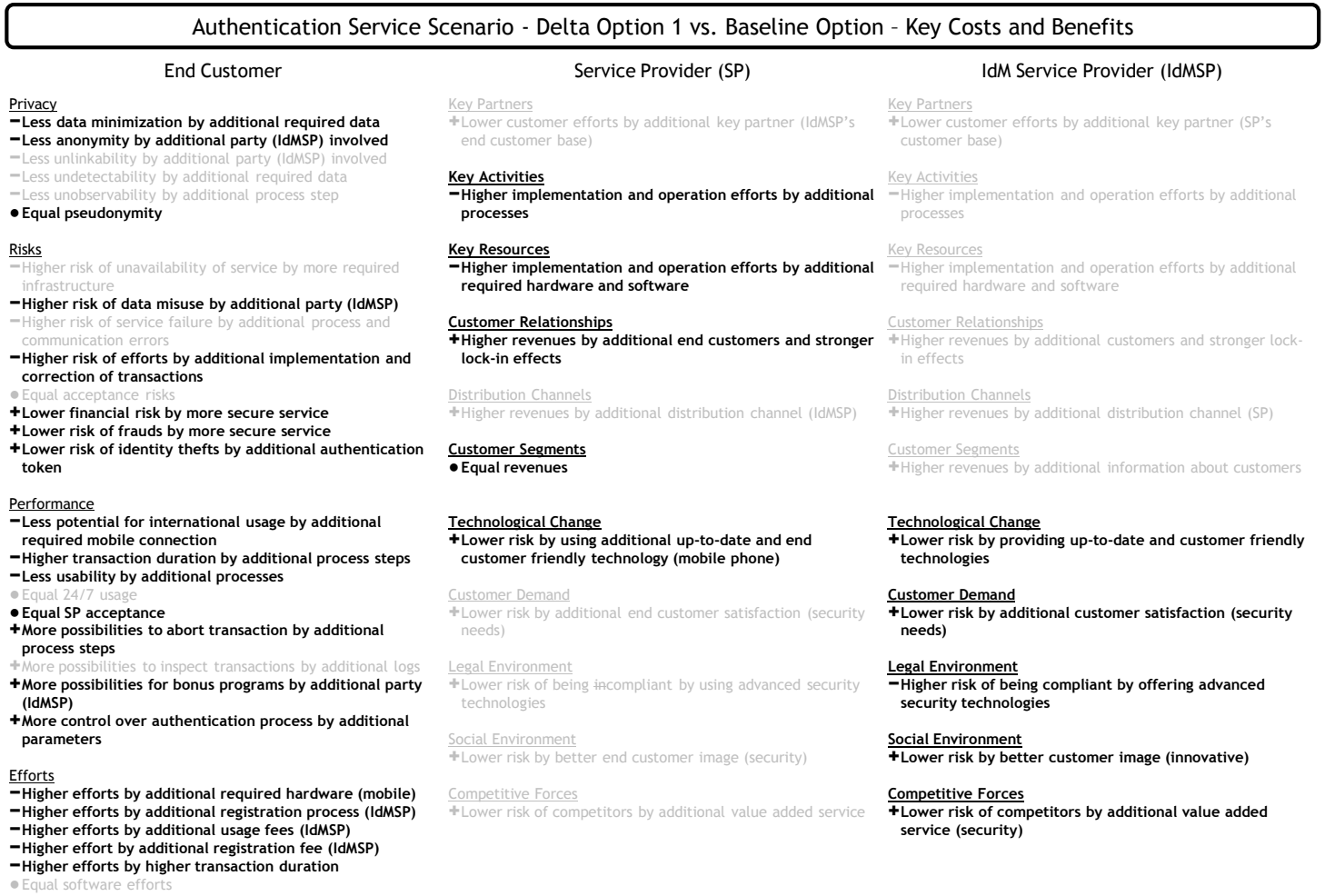

Figure 4.6: Auth - Selection of Key Costs and Benefits (DO1 vs. BO).

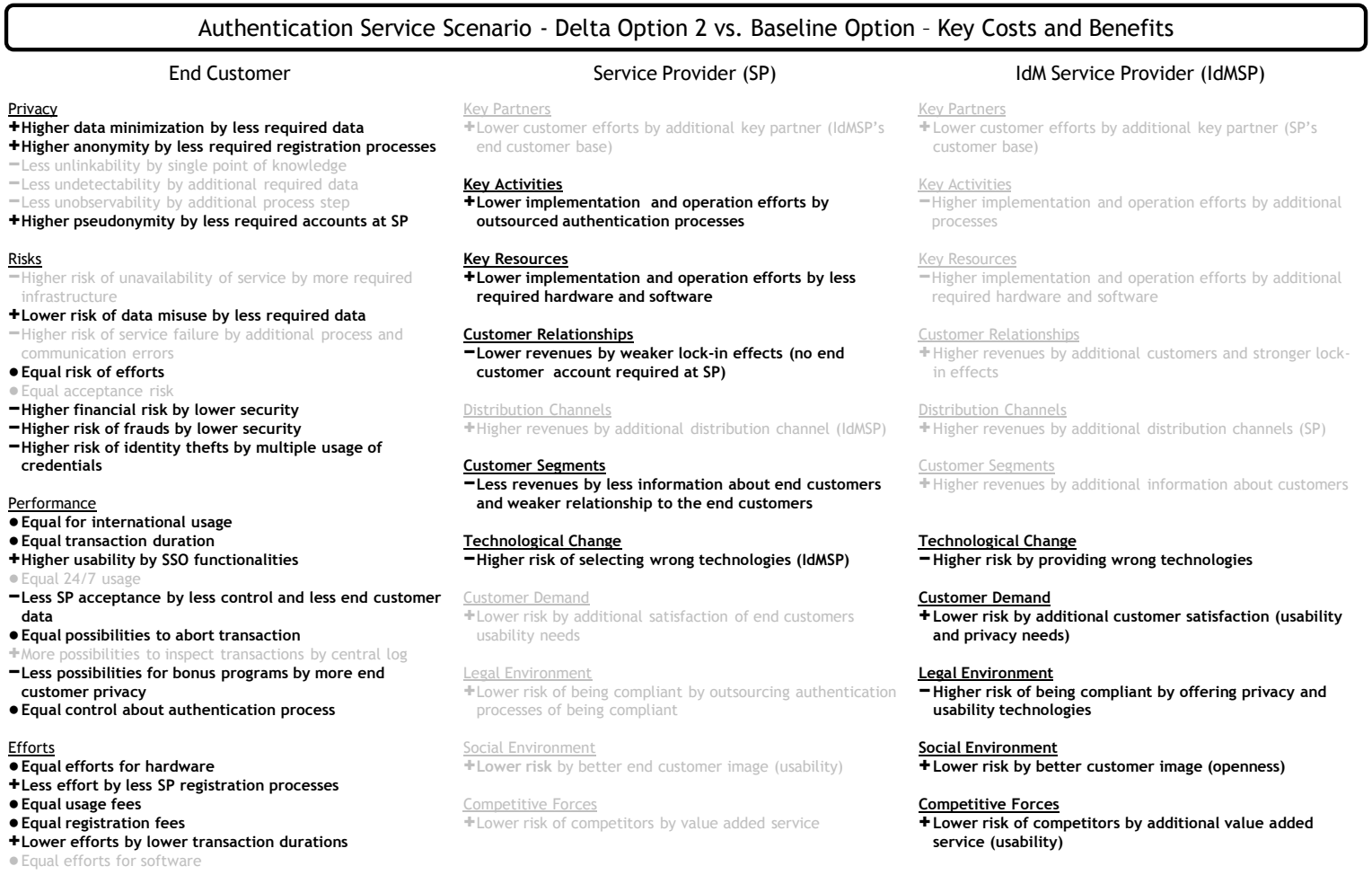

Figure 4.7: Auth - Selection of Key Costs and Benefits (DO2 vs. BO).

4.1.4 Step 4 – Clustering and Mapping of Key Costs and Benefits

The key costs and benefits identified for each stakeholder in a DO have to be mapped to the IdMSP by cause-effect chains. In this way, interdependencies between costs and benefits of each stakeholder can be modelled. Therefore, the costs and benefits of each stakeholder have to be clustered. In our case, all end customer and service provider cost-benefits dimensions are clustered into the decision value “Service Adoption”. The IdMSP’s cost-benefit dimensions are clustered into the decision value “Value Proposition”. Furthermore, the end customer’s decision value “Service Adoption” is mapped to the service provider’s decision value “Service Adoption”, which in turn is mapped to IdMSP’s decision value “Value Proposition”.

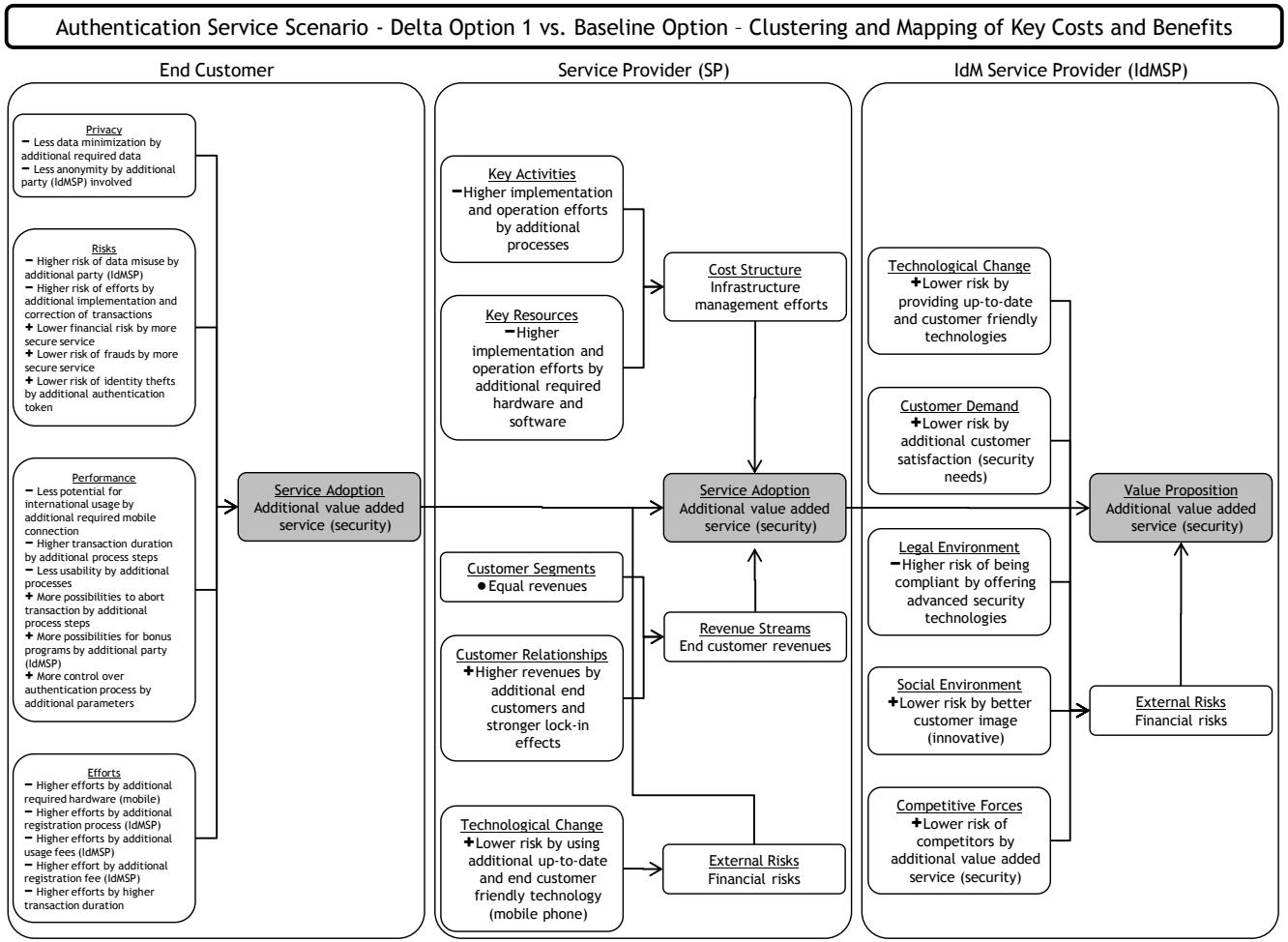

Figure 4.8: Auth - Clustering and Mapping of Key Costs and Benefits (DO1 vs. BO)

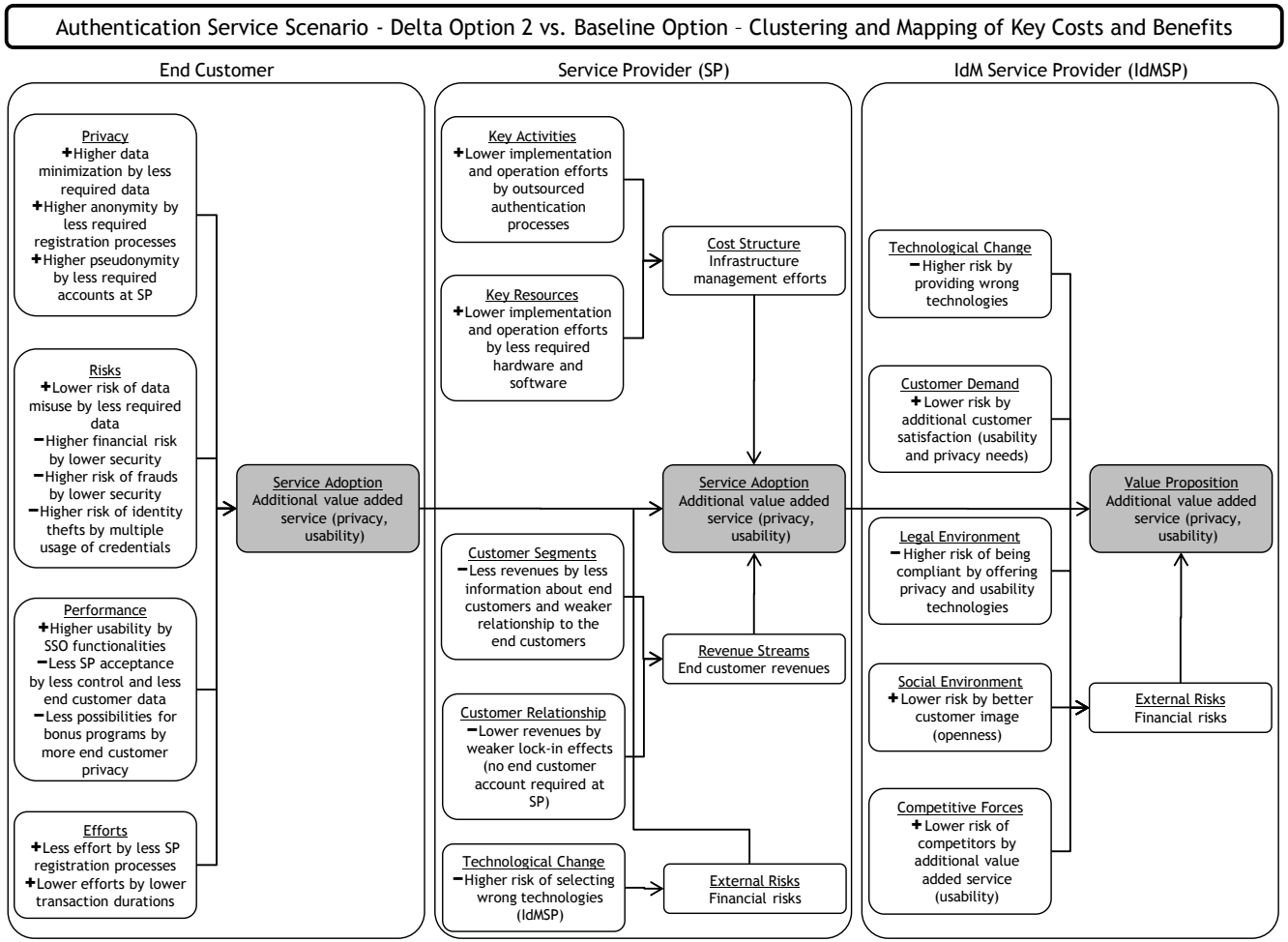

Figure 4.9: Auth - Clustering and Mapping of Key Costs and Benefits (DO2 vs. BO)

4.1.5 Step 5 – Assessment and Aggregation of Clustered Costs and Benefits

Based on the results of Step 4, the IdMSP now assesses the intensity of each dimension influencing effect by using the abstract value classes negative (-), equal (●), and positive (+). Figure 4.10 and Figure 4.11 illustrate the results of our example execution of step 5. In DO1 vs. BO, the total value of the end customer's decision value "Service Adoption" is ***-6,*** the total value of the service provider's decision value "Service Adoption" is ***-6***, the total value of the IdMSP's decision value "External Risks" is ***+3,*** and thus the total value of the IdMSP's decision value "Value Proposition" is ***-3.*** Furthermore, the figures show the sums of each stakeholder's cost-benefit dimensions (e.g. the "Privacy" cost-benefit dimension of the end customer has a total value of ***-2***).

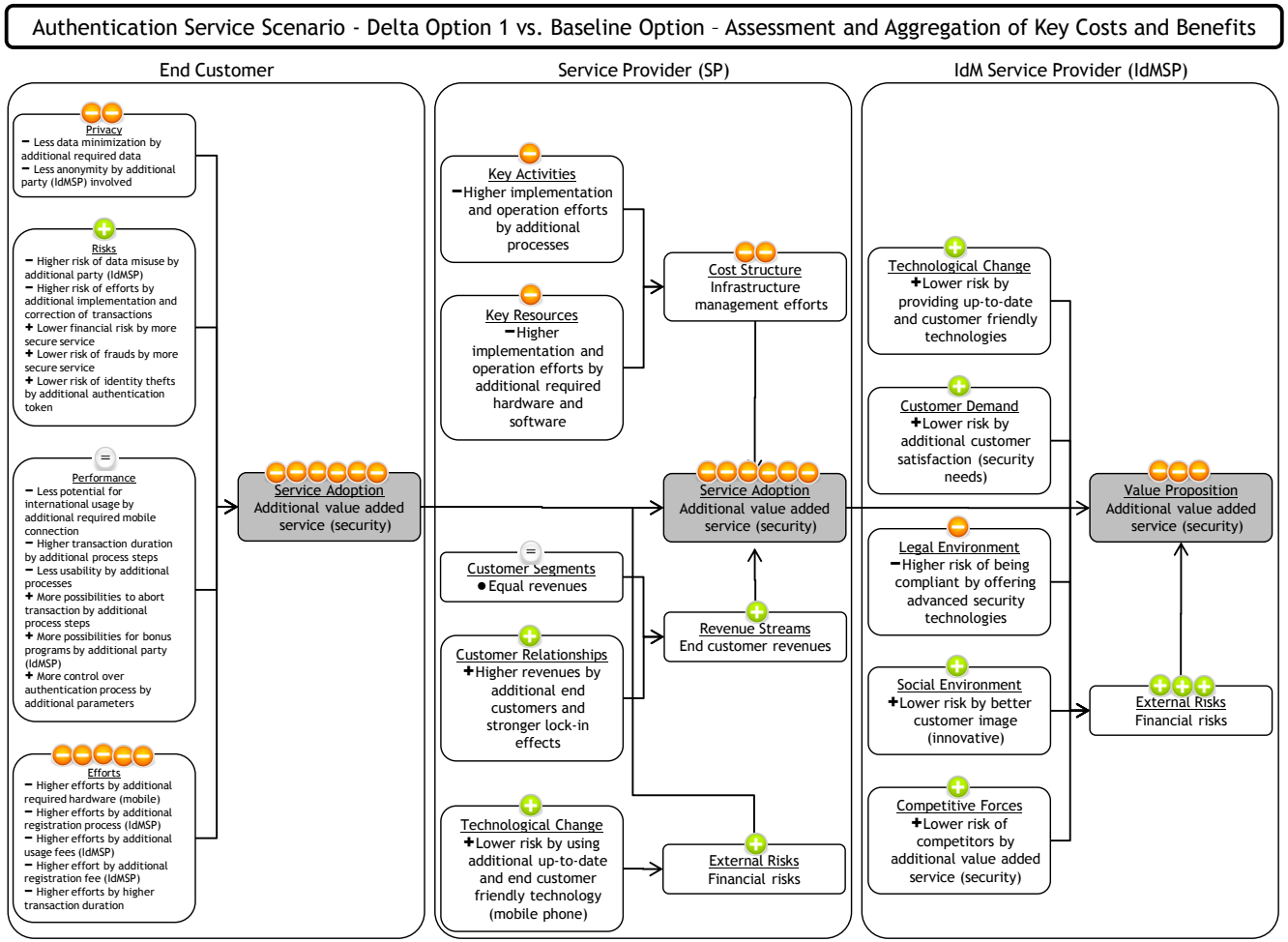

Figure 4.10: Auth - Assessment and Aggregation of Key Costs and Benefits (DO1 vs. BS)

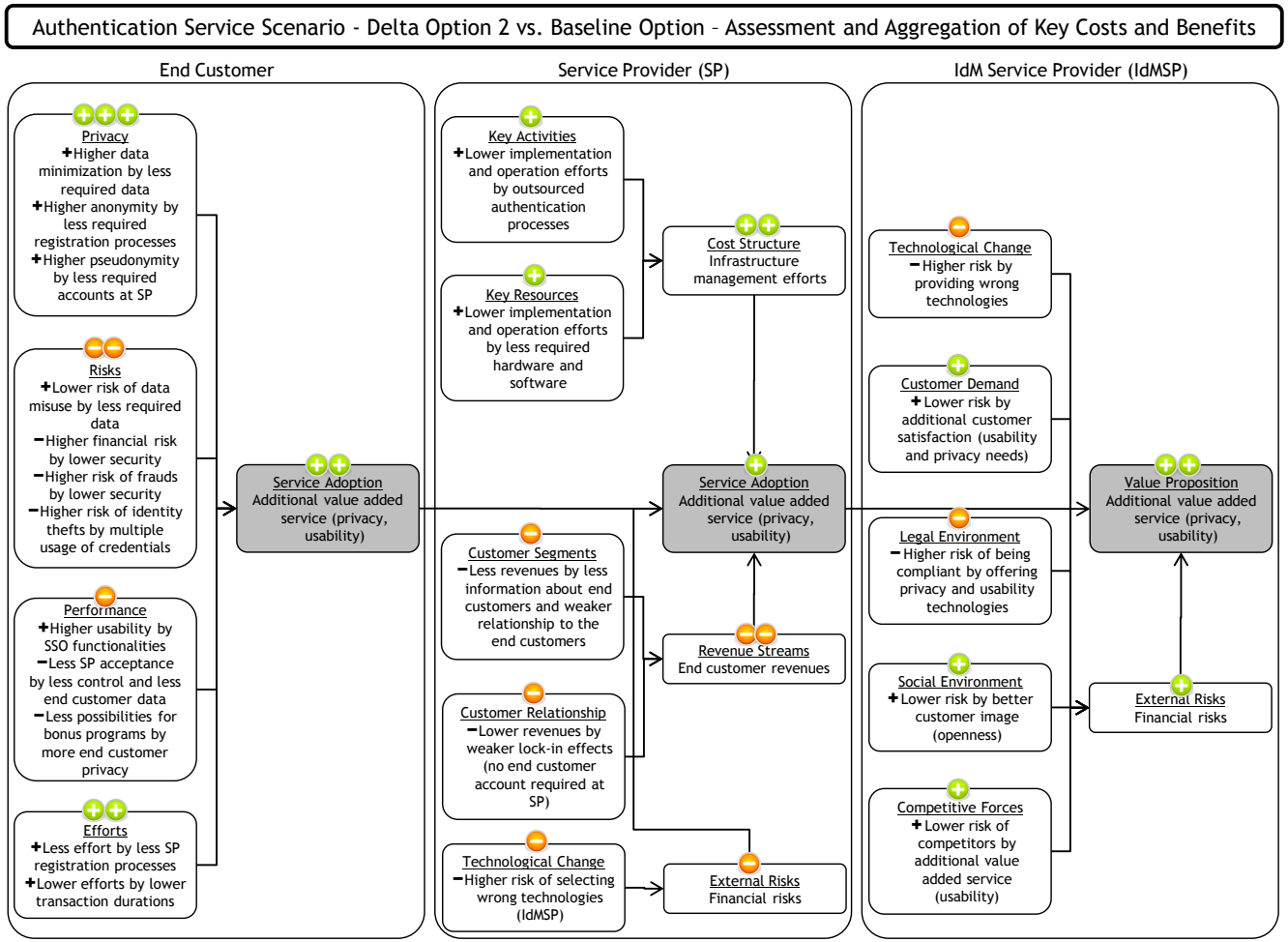

Figure 4.11: Auth - Assessment and Aggregation of Key Costs and Benefits (DO2 vs. BO)

4.1.6 Step 6 – Visualization of Aggregated Costs and Benefits

In step 6, the aggregated costs and benefits of both valuations (DO1 vs. BO and DO2 vs. BO) will be visualised in order to further simplify complex decision situations to support the IdMSP. Figure 4.12 visualizes the results of step 5. This side-by-side visualization of both results (DO1 vs. BO and DO2 vs. BO) allows direct comparison between the two scenarios. Figure 4.13 visualizes the resulting decision values for both DOs. Based on our valuation, DS2 would be the dominant scenario, thus the decision maker would chose DO2.

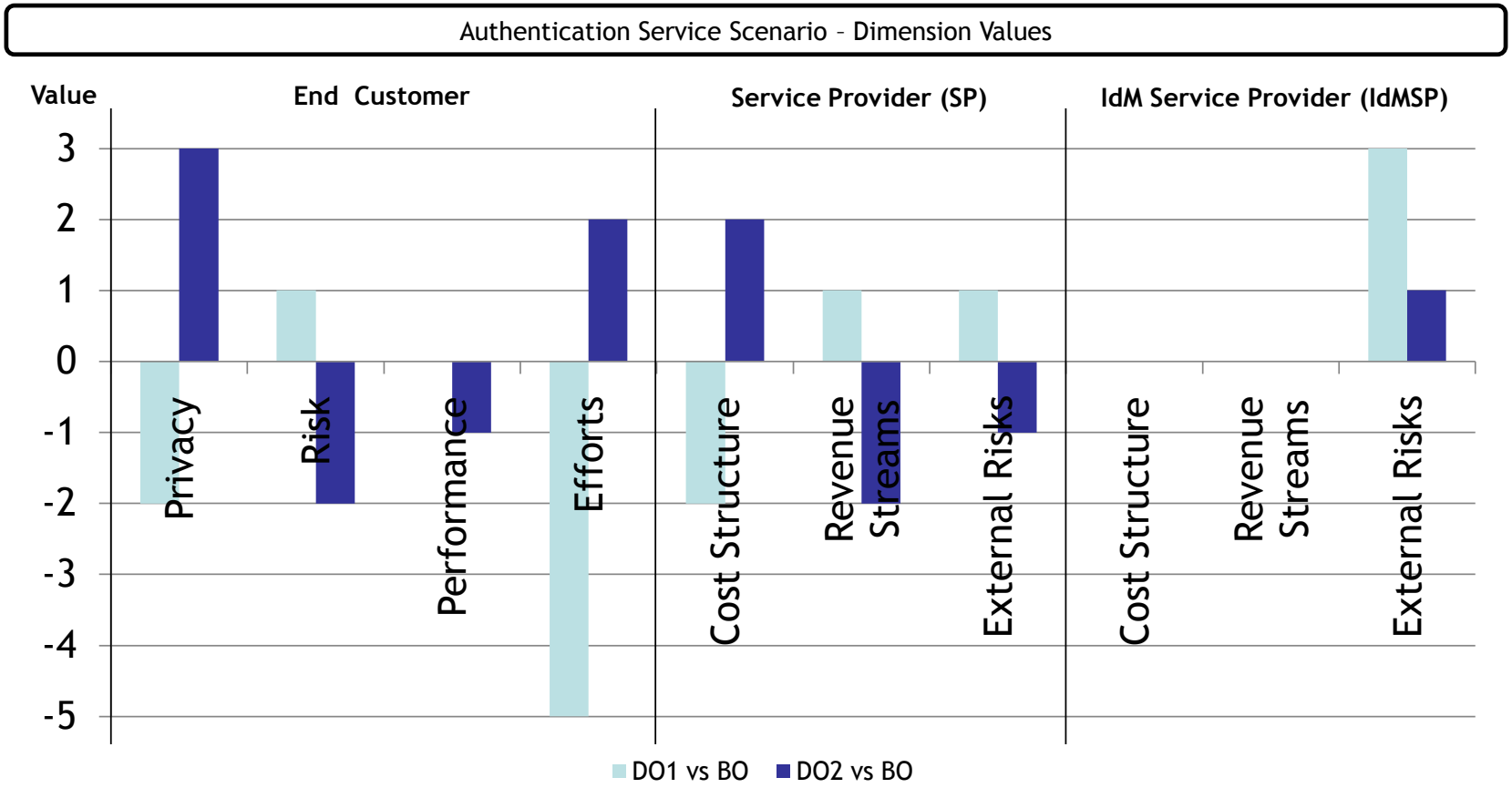

Figure 4.12: Auth - Visualisation of Dimension Values (DO1 vs. BO and DO2 vs. BO)

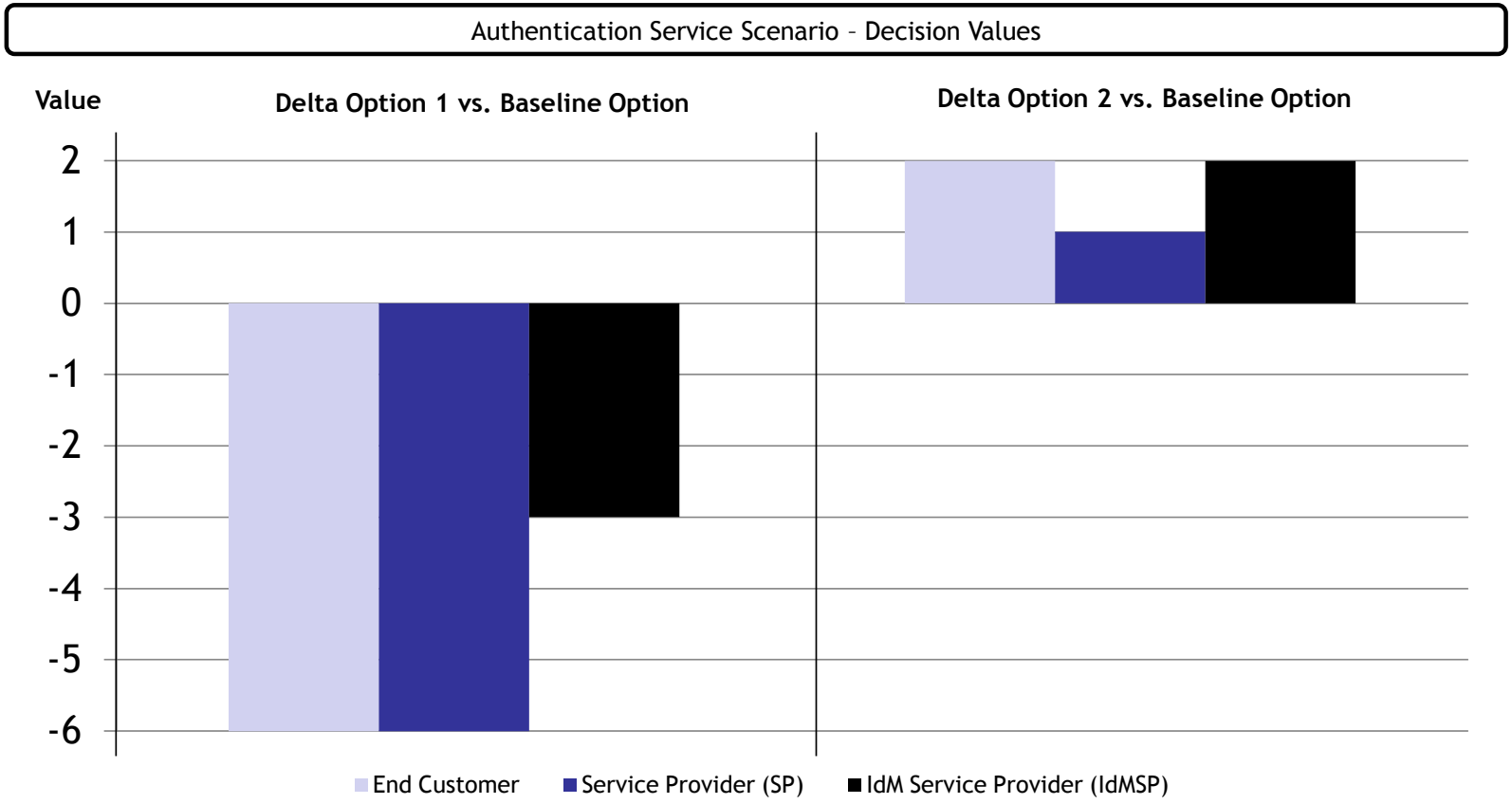

Figure 4.13: Auth - Visualisation of Decision Values (DO1 vs. DO2)

4.2 Evaluating the IdM Enabler "Privacy Policy Enforcement"

Privacy policies are an essential instrument for the end customers to express their privacy preferences. Policy enforcement mechanisms ensure that these policies are followed. This section presents three different types of policy enforcement implementations.

4.2.1 Step 1 – Description of Baseline Option and Delta Options

4.2.1.1 Privacy Policy Enforcement Baseline Scenario

Figure 4.14 illustrates the most common approach for a user to control the flow of personal data. There is no actual configuration of privacy policies and no dedicated process for enforcing policies. The end customer selectively provides the data that he wants to share with the service provider. Obviously, this approach is not very flexible and scalable, but still the state of the art.

4.2.1.2 Privacy Policy Enforcement Delta Scenario 1

In DS1 (Figure 4.15), the user provides his personal data together with a privacy policy (data handling policy) to the service provider. The SP handles the provided data as specified in the privacy policy. This variant is applicable to scenarios where the service provider is a potential provider of identity data to third parties.

4.2.1.3 Privacy Policy Enforcement Delta Scenario 2

Figure 4.16 illustrates a policy enforcement design derived from PrimeLife results of different work packages. There is a dedicated Policy engine at the Telco's side where the end customer can create and configure (or upload) his individual privacy policy (1). When a service provider requests personal data from the end customer, the policy enforcement point (PEP) checks this request against the user's privacy policy. In case of a mismatch, the end customer is informed about this (e.g., push notification to his mobile phone, 2). He then can decide whether to provide the data anyhow or to insist on his policy configuration (3). In the first case, the policy filtered data is provided to the service provider (4). In this option, both the IdM data assets (personal data) and the IdM functional capability is provided by the Telco.

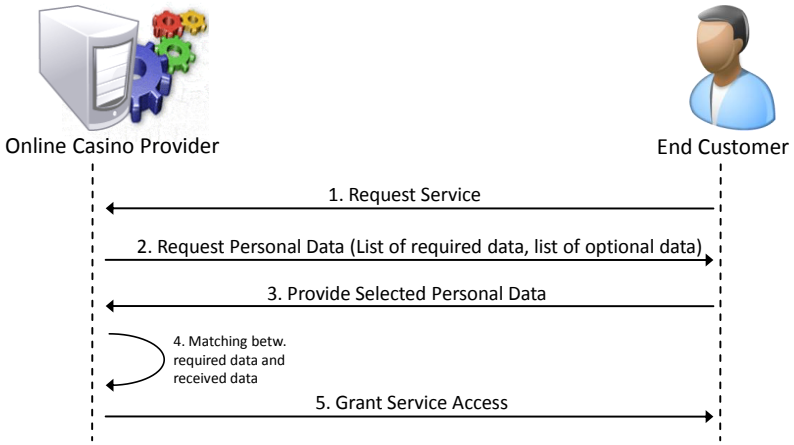

Figure 4.14: PPE - Baseline Scenario

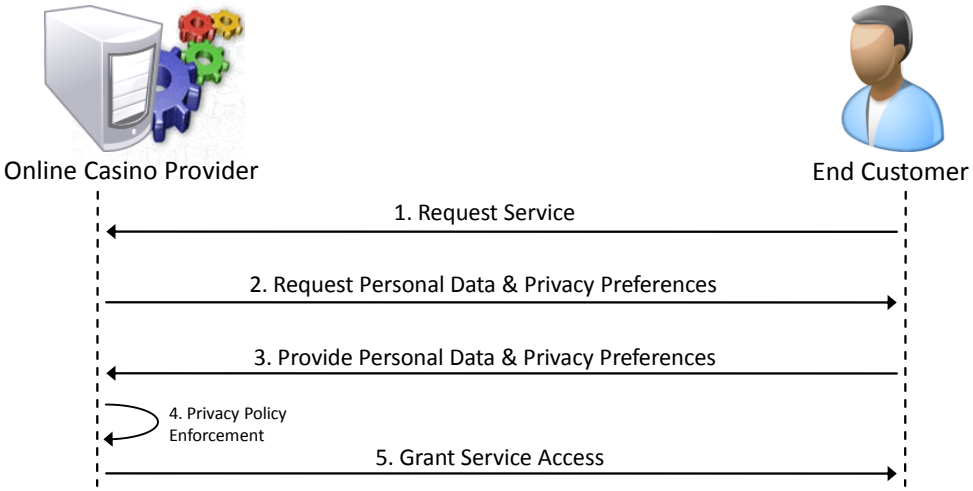

Figure 4.15: PPE - Delta Scenario 1

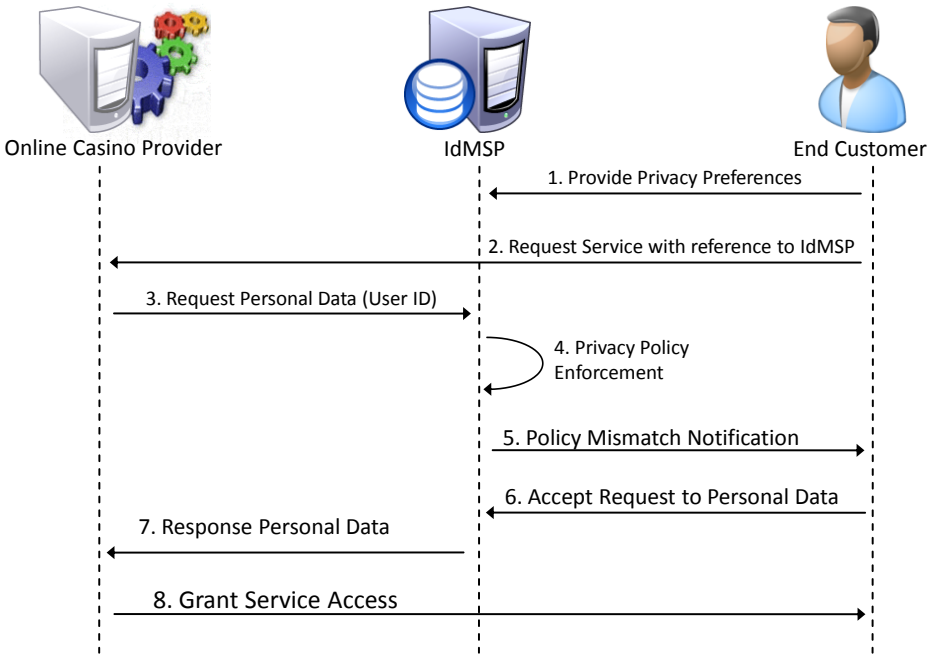

Figure 4.16: PPE - Delta Scenario 2

4.2.2 Step 2 – Identification of each Stakeholder's Costs and Benefits

4.2.2.1 Delta Scenario 1

Table 4.3: PPE - Selected Costs and Benefits (DO1 vs. BO)

Evaluation Item (Stakeholder/Dimension)	Description
Higher Risk of unavailability of service by more required infrastructure (EC/Risks)	In this scenario, an additional infrastructure component – the privacy policy enforcement engine – is required. Thus, the risk of unavailability is increased.
Lower risk of data misuse (EC/Risks)	By providing a privacy policy enforcement engine, the SP obligates itself to respect the users' privacy preferences. This decreases the risk of data misuse.
More possibilities to abort transactions by additional policies (EC/Performance)	The usage of privacy policies provide the user the possibility to define data handling rules that allow the abortion of transactions after personal data has been provided.
Higher implementation and operation efforts by additional processes (SP/Cost Structure)	The service provider has to implement and maintain additional processes – the privacy policy enforcement engine.
Higher revenues by additional end customers and more privacy-friendly services (SP/Revenue Streams)	The provision of advanced privacy policy mechanisms could attract new end customers, which in turn potentially lead to additional revenues.
Higher revenues by additional information about end customers (SP/Revenue Streams)	Through the provision of advanced and transparent privacy policy mechanisms, customers could be ready to provide more information for advertisement purposes.

4.2.2.2 Delta Scenario 2

Table 4.4: PPE Selected Costs and Benefits (DO2 vs. BO)

Valuation Item (Stakeholder/Dimension)	Description
Less anonymity by additional party involved (EC/Privacy)	With the IdMSP, there exist an additional party that is involved in the transactions between the user and the SP. This decreases the anonymity level of the user.
Higher risk of unavailability of service by additional required infrastructure (EC/Risks)	Through the involvement of an additional party (the IdMSP) the transactions become more complex. This increases the risk of unavailability of the service.
Lower risk of data misuse by additional enforcement of IdMSP (EC/Risks)	The dedicated third-party privacy policy enforcement, supports the user in protecting his privacy. This decreases the risk of data misuse.
Higher transaction duration by additional process steps (EC/Performance)	The additional privacy policy enforcement is time consuming. In the worst case, the user has to be informed about a policy mismatch. The user then would have to confirm or abort the transaction with his mobile phone.
More possibilities to inspect transactions by IdMSP (EC/Performance)	IdMSP privacy policy enforcement transaction logs could be provided to the user.

Higher efforts by additional registration process step (EC/Performance)	The usage of the IdMSP PPE service requires a registration.
Higher implementation and operation efforts by additional required software (SP/Cost Structure)	The service provider has to implement and maintain additional processes – an interface to the IdMSP PPE service.
Higher implementation and operation efforts by additional required software (IdMSP/Cost Structure)	The IdMSP has to implement and maintain additional processes – the PPE service and respective interfaces for service providers and end customers.
Higher revenues by additional customers and stronger lock-in effects (IdMSP/Revenue Streams)	The provision of advanced privacy mechanisms could potentially attract new end customers and strengthen customer retention.
Higher revenues by additional distribution channel (IdMSP/Revenue Streams)	Service providers that use the PPE service are potential distribution channels for the IdMSP to promote its services.
Higher revenues by additional information about customers (IdMSP/Revenue Streams)	Through the provision of advanced and transparent privacy policy mechanisms, customers could be ready to provide more information for advertisement purposes.
Higher risk of selecting and providing the wrong technology (IdMSP/Risks)	The risk of providing the wrong PPE protocols, etc.
Higher risk of being legally compliant by offering security technology (IdMSP/Risks)	Through the provision of privacy services, the IdMSP accountable for the users' personal data.

Policy Enforcement Service Scenario - Delta Option 1 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
- ● Equal data minimization
- ● Equal anonymity
- ● Equal unlinkability
- ● Equal undetectability
- ● Equal unobservability
- ● Equal pseudonymity

Risks
- − Higher risk of unavailability of service by more required infrastructure
- + Lower risk of data misuse by additional obligations of SP
- − Higher risk of service failure by additional process and communication errors
- − Higher risk of efforts by additional inspection and correction of transactions
- ● Equal acceptance risk
- ● Equal financial risk
- ● Equal risk of frauds
- ● Equal risks of identity thefts

Performance
- ● Equal international usage
- − Higher transaction duration by additional process steps
- − Less usability by additional processes
- ● Equal 24/7 usage
- − Less SP acceptance by additional processes
- + More possibilities to abort transactions by additional policies
- ● Equal possibilities to inspect transactions
- ● Equal possibilities for bonus programs
- + More control about data handling

Efforts
- ● Equal hardware
- − Higher efforts by additional registration process step
- ● Equal usage fees
- ● Equal registration fees
- − Higher efforts by higher transaction duration
- ● Equal software efforts

Service Provider (SP)

Key Partners
- ● Equal efforts

Key Activities
- − Higher implementation and operation efforts by additional processes

Key Resources
- − Higher implementation and operation efforts by additional required software

Customer Relationships
- + Higher revenues by more end customers and more privacy-friendly services

Distribution Channels
- ● Equal revenues

Customer Segments
- + Higher revenues by additional information about customers

Technological Change
- ● Equal risk

Customer Demand
- + Lower risk by additional satisfaction of end customers privacy control needs

Legal Environment
- + Lower risk of being compliant by offering end customers more privacy control

Social Environment
- + Lower risk by better end customer image

Competitive Forces
- + Lower risk of competitors by additional value added service

IdM Service Provider (IdMSP)

No IdMSP involved!

Figure 4.17: PPE - Identification of Costs and Benefits (DO1 vs. BO)

Policy Enforcement Service Scenario - Delta Option 2 vs. Baseline Option – Costs and Benefits

End Customer

Privacy
- ● Equal data minimization
- ● Less anonymity by additional party involved (IdMSP)
- ● Less unlinkability by single point of knowledge (IdMSP)
- ● Equal undetectability
- ● Equal unobservability
- ● Equal pseudonymity

Risks
- − Higher risk of unavailability of service by more required infrastructure
- + Lower risk of data misuse by additional enforcement of IdMSP
- − Higher risk of service failure by additional process and communication errors
- − Higher risk of efforts by additional inspection and correction of transactions
- ● Equal acceptance risk
- ● Equal financial risk
- ● Equal risk of frauds
- ● Equal risk of identity thefts

Performance
- ● Equal international usage
- − Higher transaction duration by additional process steps
- + More usability by predefined and IdMSP-enforced policies
- ● Equal 24/7 usage
- ● Equal SP acceptance
- ● More possibilities to abort transactions by additional policies
- + More possibilities to inspect transactions by IdMSP
- + More possibilities for bonus programs
- + More control about data handling

Efforts
- − Higher efforts by additional required hardware (mobile)
- − Higher efforts by additional registration process step
- ● Equal usage fees
- ● Equal registration fees
- − Higher efforts by higher transaction duration
- ● Equal software efforts

Service Provider (SP)

Key Partners
- + Less customer efforts by additional key partner (IdMSP)

Key Activities
- ● Equal efforts

Key Resources
- − Higher implementation and operation efforts by additional required software

Customer Relationships
- + Higher revenues by more end customers and more privacy-friendly and more usable services

Distribution Channels
- + Higher revenues by additional distribution channel (IdMSP)

Customer Segments
- + Equal revenues

Technological Change
- ● Equal risk

Customer Demand
- + Lower risk by additional satisfaction of end customers privacy control and usability needs

Legal Environment
- + Lower risk of being compliant by outsourcing privacy control to IdMSP

Social Environment
- + Lower risk by better end customer image

Competitive Forces
- + Lower risk of competitors by additional value added service

IdM Service Provider (IdMSP)

Key Partners
- + Less customer efforts by additional key partner (SP's customer base)

Key Activities
- − Higher implementation and operation efforts by additional processes

Key Resources
- − Higher implementation and operation efforts by additional required hardware and software

Customer Relationships
- + Higher revenues by additional customers and stronger lock-in effects

Distribution Channels
- + Higher revenues by additional distribution channel (SP)

Customer Segments
- + Higher revenues by additional information about customers

Technological Change
- − Higher risk by selecting and providing wrong technology

Customer Demand
- + Lower risk by additional satisfaction of customers privacy control and usability needs

Legal Environment
- − Higher risk of being compliant by offering security technology

Social Environment
- + Lower risk by better customer image

Competitive Forces
- + Lower risk of competitors by additional value added service

Figure 4.18: PPE - Identification of Costs and Benefits (DO2 vs. BO)

4.2.3 Step 3 – Selection of Key Costs and Benefits

In step 3, the decision maker has to reduce the set of costs and benefits to a subset of key costs and key benefits for each stakeholder. The IdMSP excludes all costs and benefits he does not consider relevant for its decision making. Figure 4.6 and Figure 4.7 show the result of step 3. In our case, we followed the strategy to exclude all costs and benefits which were valuated equally in both, DO1 vs. BO and DO2 vs. BO. In other words, costs and benefits that are neither dominant in DO1 nor in DO2 were excluded. Non-key costs and benefits are greyed out in the figures.

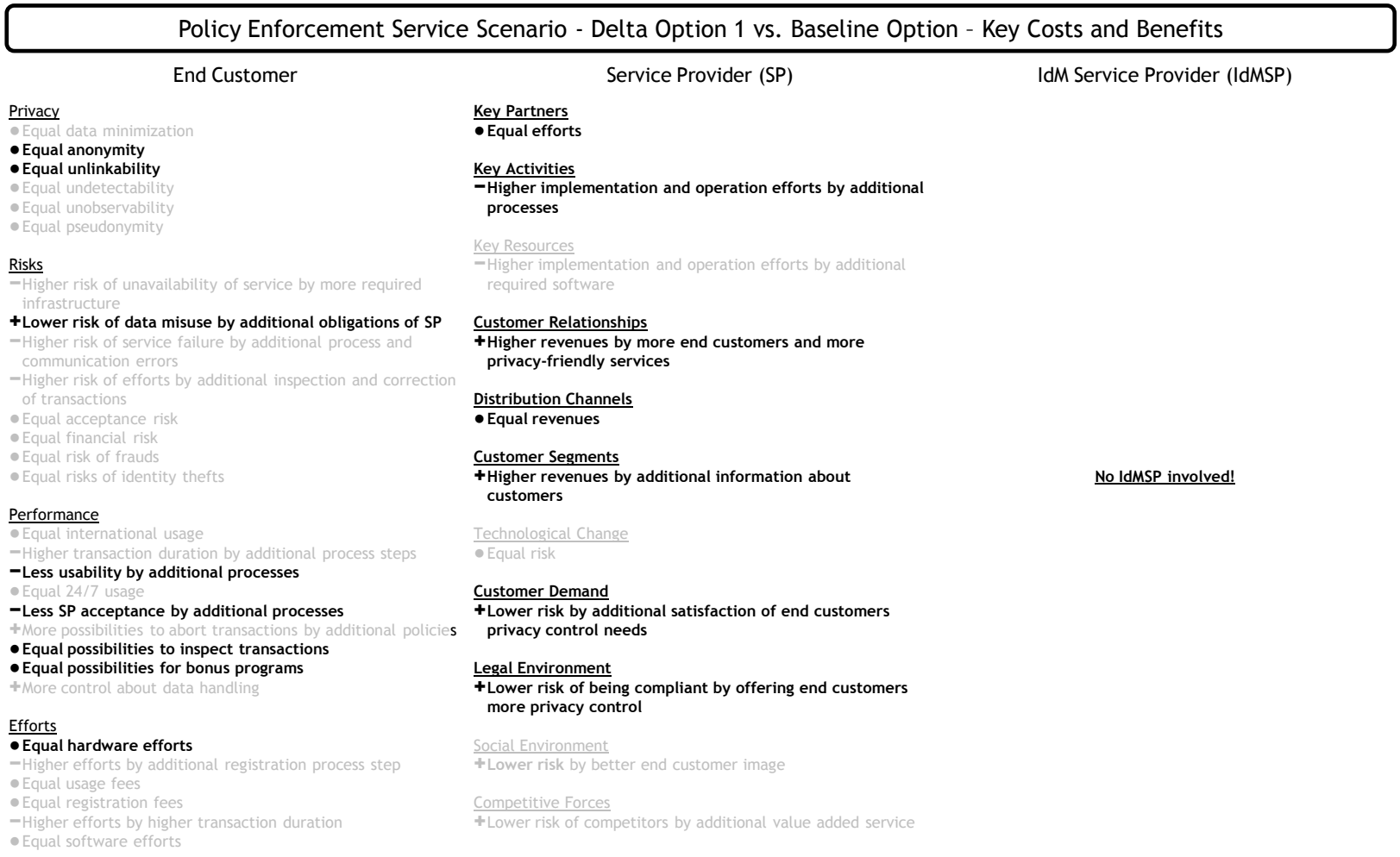

Figure 4.19: PPE - Selection of Key Costs and Benefits (DO1 vs. BO)

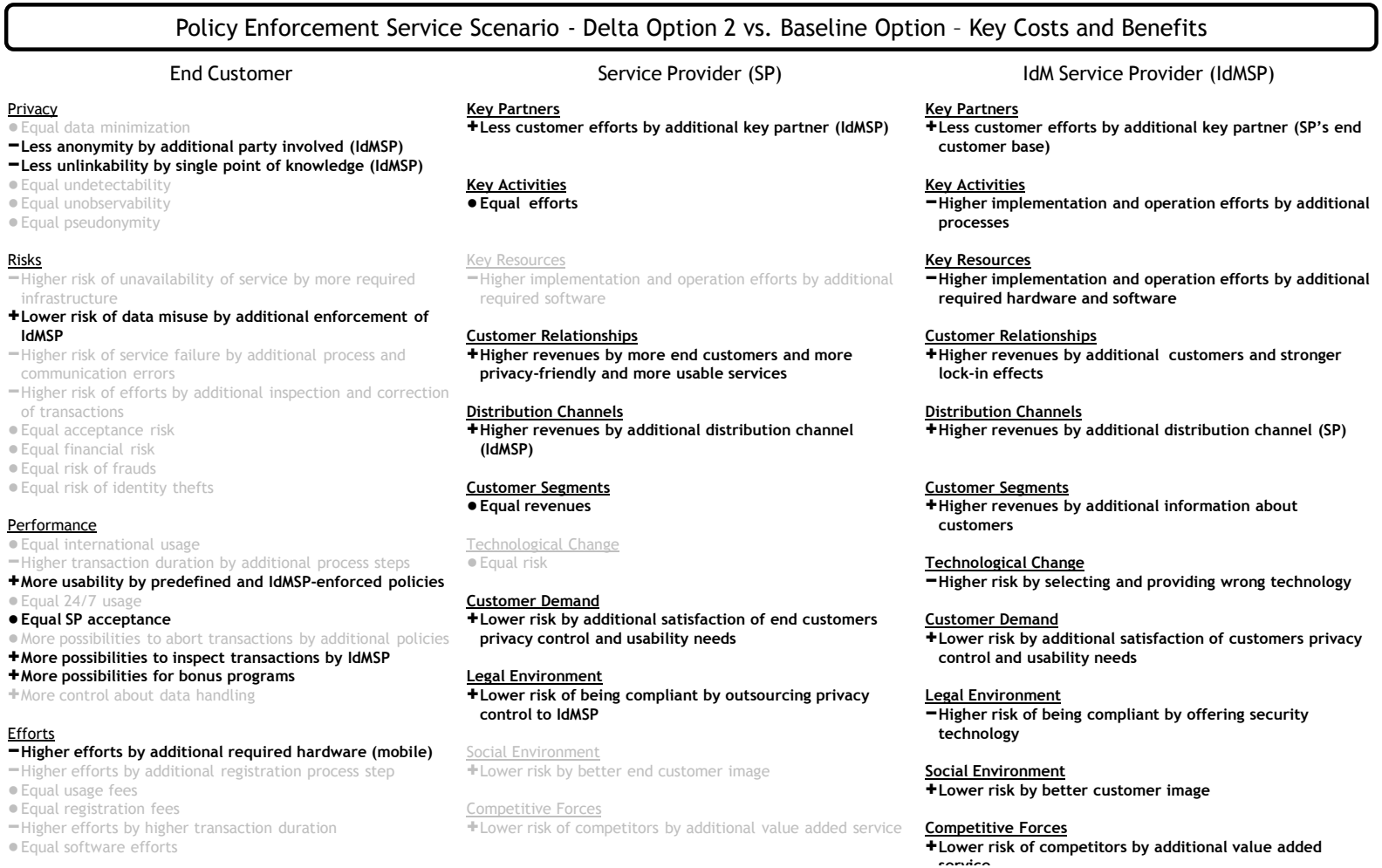

Figure 4.20: PPE - Selection of Key Costs and Benefits (DO2 vs. BO)

4.2.4 Step 4 – Mapping and Clustering of Key Costs and Benefits

The key costs and benefits identified for each stakeholder in a DO have to be mapped to the IdMSP by cause-effect chains. In this way, interdependencies between costs and benefits of each stakeholder can be modelled. Therefore, the costs and benefits of each stakeholder have to be clustered. In our case, all end customer and service provider cost-benefits dimensions are clustered into the decision value “Service Adoption”. The IdMSP’s cost-benefit dimensions are clustered into the decision value “Value Proposition”. Furthermore, the end customer’s decision value “Service Adoption” is mapped to the service provider’s decision value “Service Adoption”, which in turn is mapped to IdMSP’s decision value “Value Proposition”.

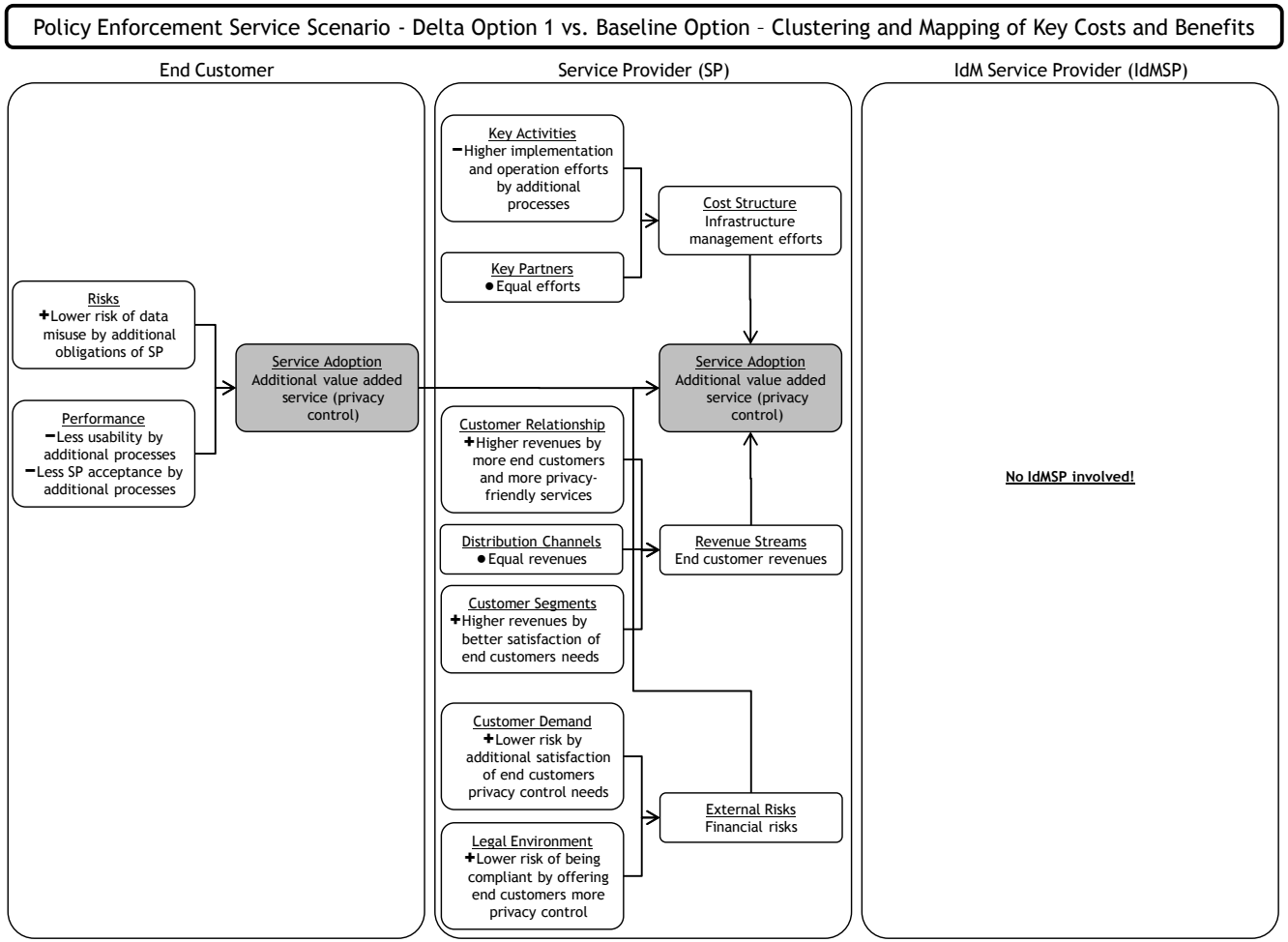

Figure 4.21: PPE - Clustering and Mapping of Key Costs and Benefits (DO1 vs. BO)

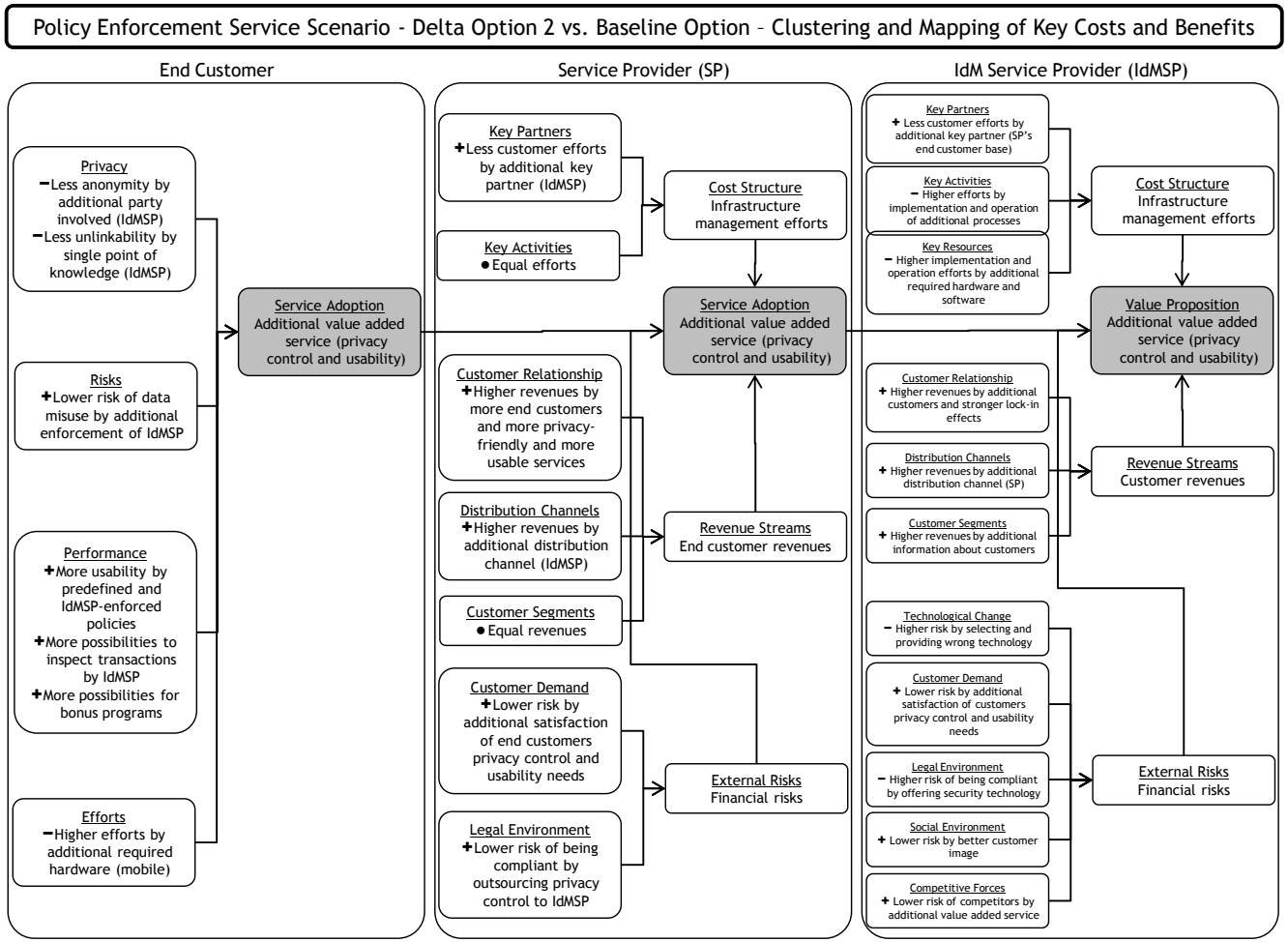

Figure 4.22: PPE - Clustering and Mapping of Key Costs and Benefits (DO2 vs. BO)

4.2.5 Step 5 – Assessment and Aggregation of Clustered Costs and Benefits

Based on the results of Step 4, the IdMSP now assesses the intensity of each dimension influencing effect by using the abstract value classes negative (-), equal (●), and positive (+). Figure 4.23 and Figure 4.24 illustrate the results of our example execution of step 5. In DO2 vs. BO, the total value of the end customer's decision value "Service Adoption" is ***+1,*** the total value of the service provider's decision value "Service Adoption" is ***+6***, the total value of the IdMSP's decision value "External Risks" is ***+1,*** the total value of the IdMSP's decision value "Cost Structure" is ***-1,*** the total value of the IdMSP's decision value "Revenue Streams" is ***+3,*** and thus the total value of the IdMSP's decision value "Value Proposition" is ***+9.*** Furthermore, the figures show the sums of each stakeholder's cost-benefit dimensions (e.g. the "Performance" cost-benefit dimension of the end customer has a total value of ***+3***).

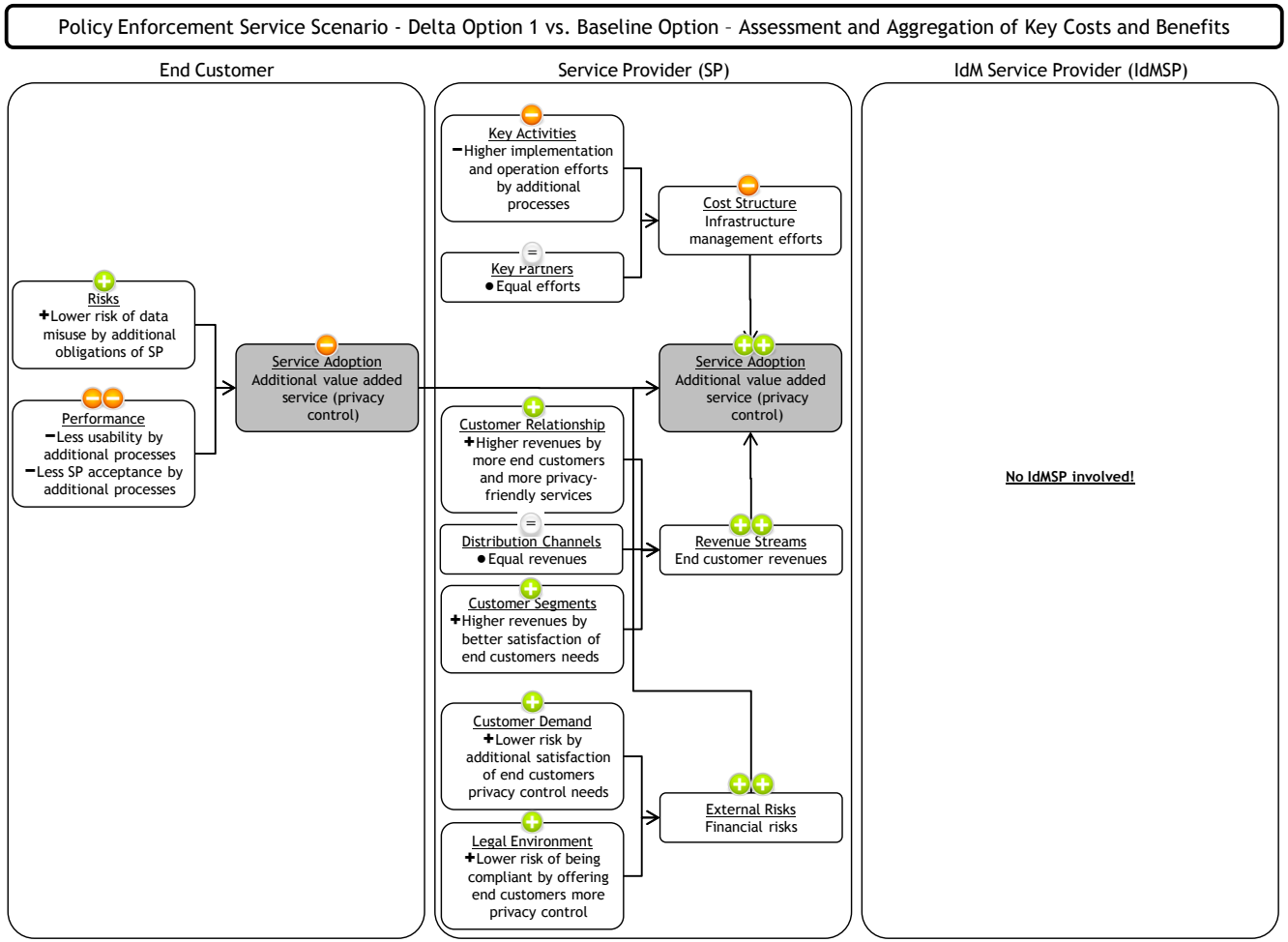

Figure 4.23: PPE - Assessment and Aggregation of Key Costs and Benefits (DO1 vs. BO)

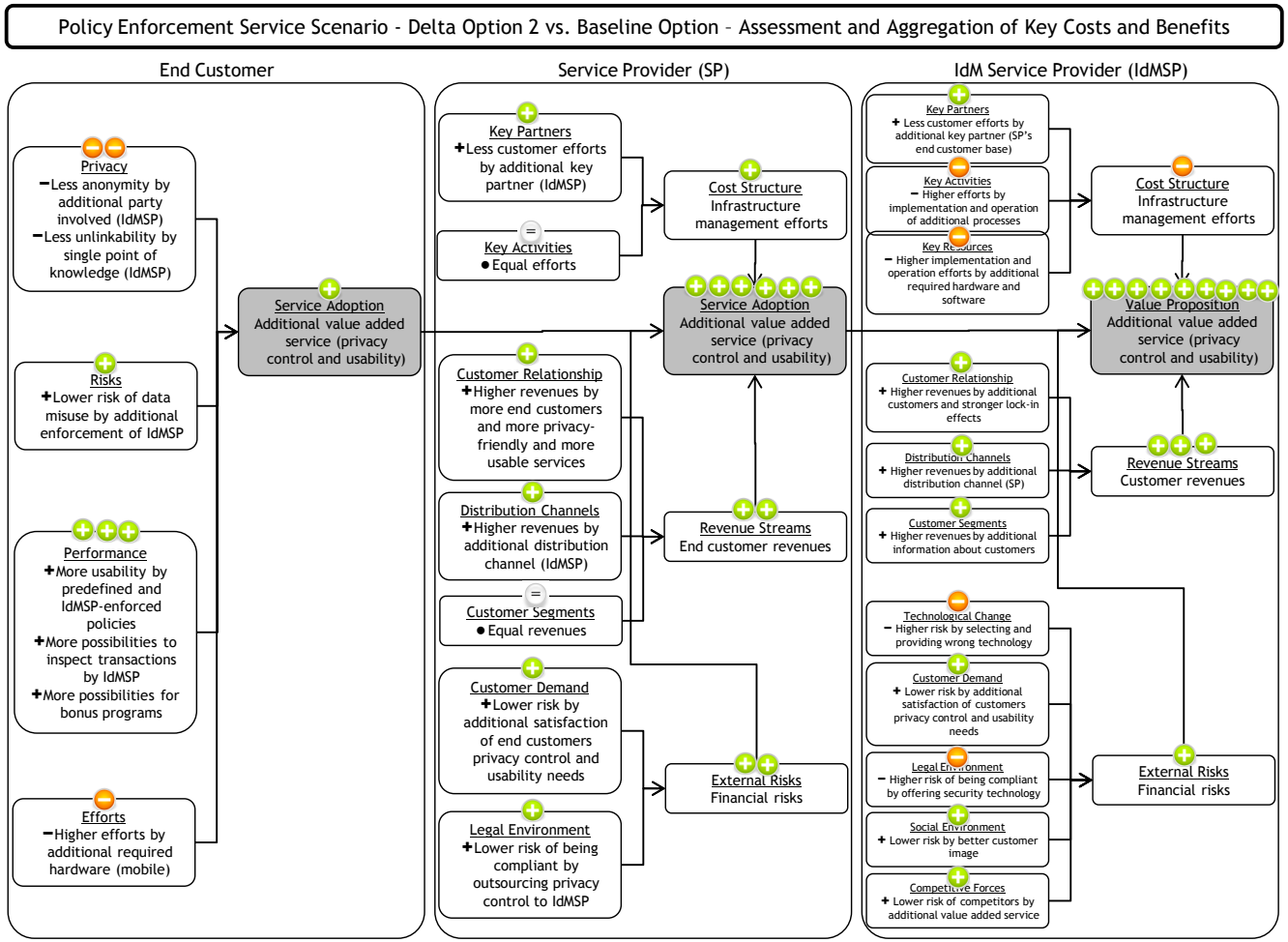

Figure 4.24: PPE - Assessment and Aggregation of Key Costs and Benefits (DO2 vs. BO)

4.2.6 Step 6 – Visualisation of Aggregated Costs and Benefits

In step 6, the aggregated costs and benefits of both valuations (DO1 vs. BO and DO2 vs. BO) will be visualised in order to further simplify complex decision situations to support the IdMSP. Figure 4.25 visualizes the results of step 5. This side-by-side visualization of both results (DO1 vs. BO and DO2 vs. BO) allows direct comparison between the two scenarios. Figure 4.26 visualizes the resulting decision values for both DOs. Based on our valuation, DS2 would be the dominant scenario, thus the decision maker would chose DO2.

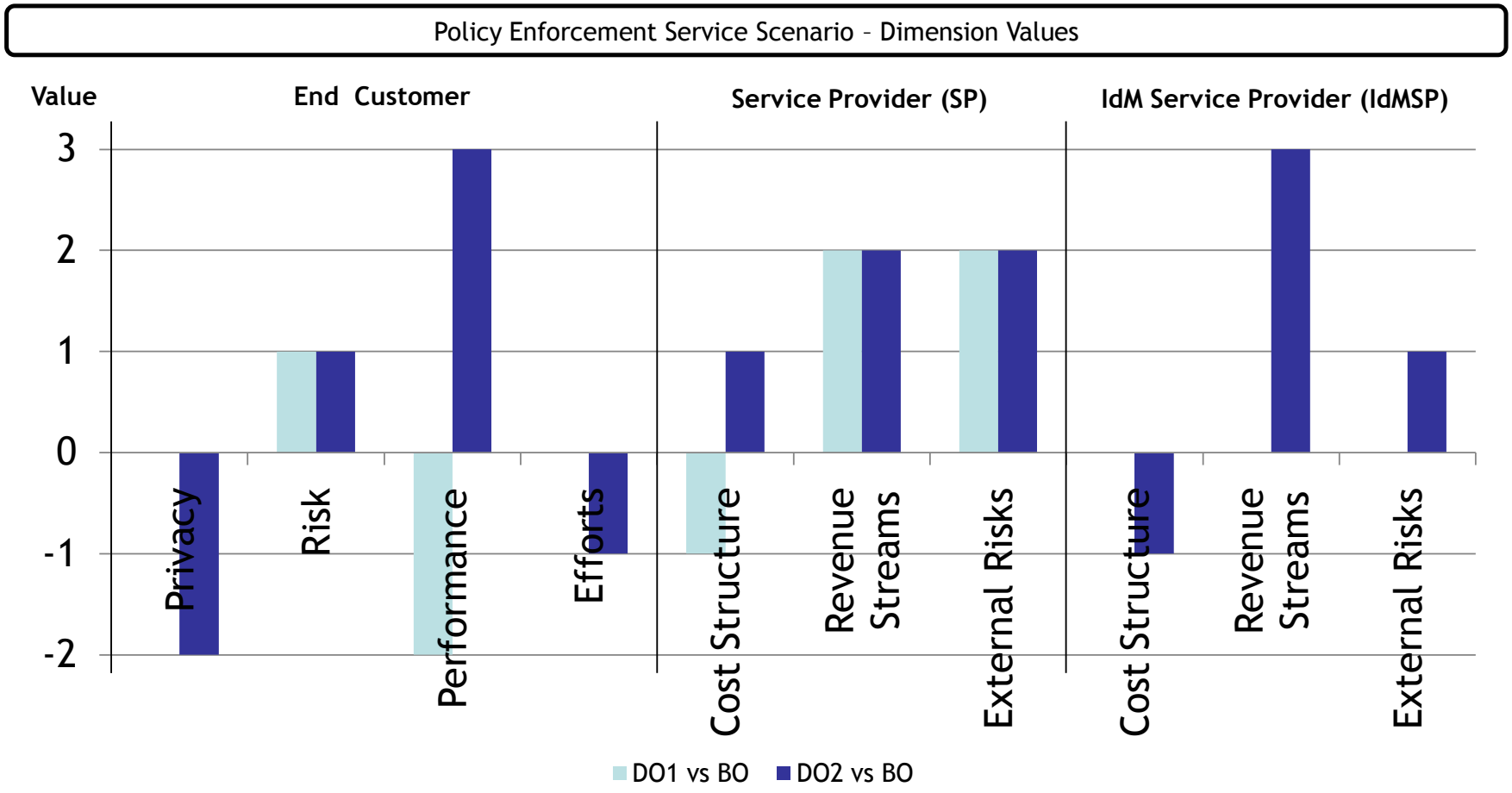

Figure 4.25: PPE - Visualisation of Dimension Values

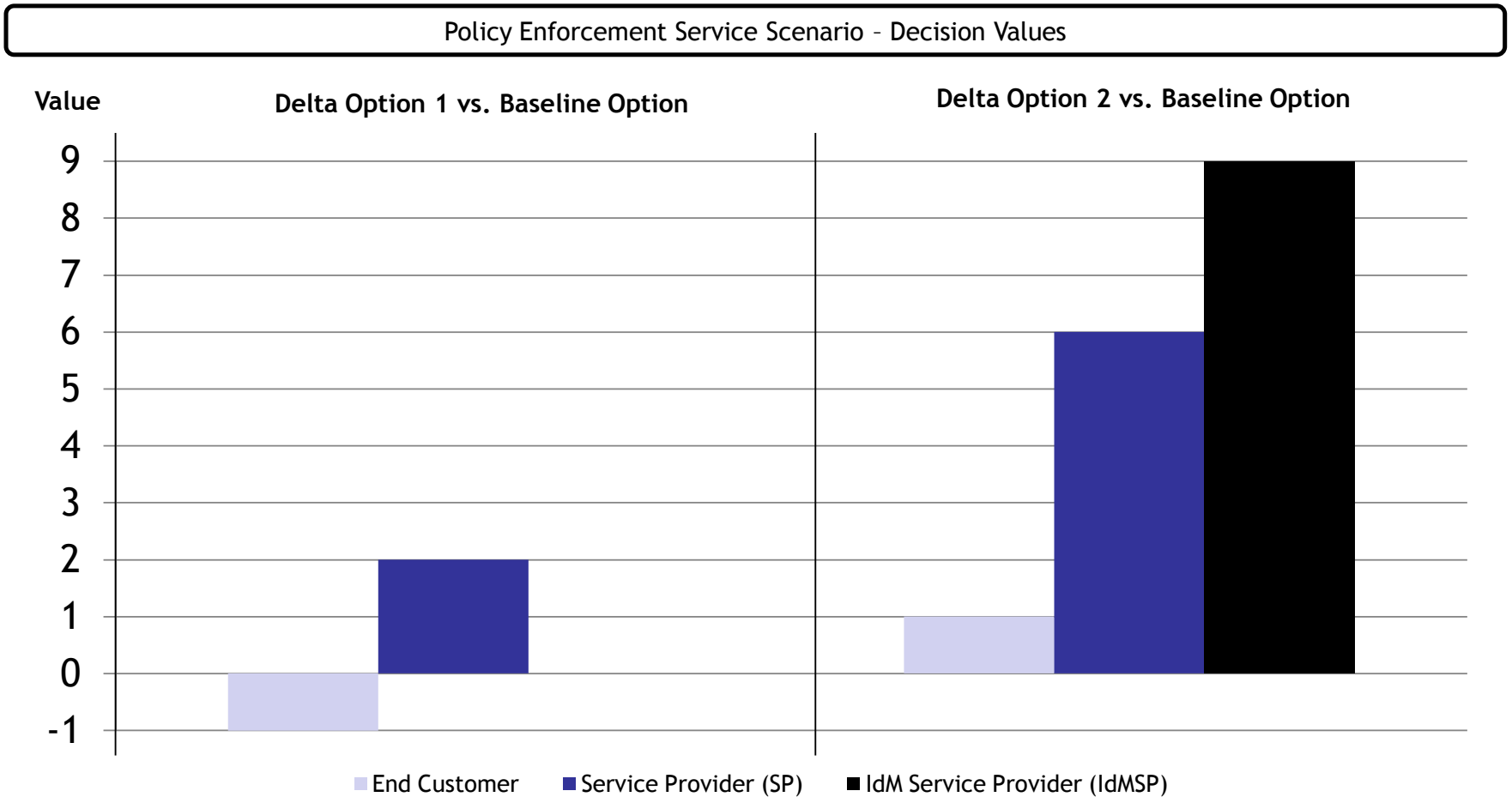

Figure 4.26: PPE - Visualisation of Decision Values

Chapter 5

Summary, Conclusion, and Outlook

The provision of identity management services is one potential direction of future business models of telcos. However, there is a lack of instruments that let telcos (or other potential IdM service providers) systematically assess the potential value of providing such identity services. Motivated by this gap, we have developed a method to evaluate privacy-enhancing IdM Services from the perspective of a telco acting as IdM Service Provider. Some of the six steps of the method are structured following established economic methods. The major goal of our approach is to develop a simple method with a good trade-off between quality of the method's results and the effort needed in carrying out the work. One essential component of the method is the IdM Enabler Concept that we introduced in this document. To test our valuation method, we applied it to several IdM service scenarios. The tests supported the need for a detailed and precise description of the scenarios.

The general benefits of our method:

- takes into account monetary as well as non-monetary costs and benefits.
- presents decision-relevant information in a simple and structured way without over-challenging the decision maker.
- integrates perspectives of different stakeholders, so that interdependencies can be evaluated.
- enables a stronger focus on (and integration of) privacy-effects on consumers as an essential factor for economic success.

The benefits related to processing of input:

- considers individual value perceptions of stakeholders to enable application field-specific valuations of IdM services
- considers interdependencies between costs and benefits by using cause-effect chains
- enables the aggregation of costs and benefits to a one dimensional decision factor
- offers a standardized and balanced valuation approach by using predetermined holistic value-systems for stakeholders
- offers a standardized procedure for a repeatedly occurring decision problem for a better comparison beyond company and department boundaries

The benefits related to organization of decision making:

- leads to an improved decision making basis and to a higher transparency of the decision making process.

- reduces intuitive (and consequently highly subjective) valuations, or rather, makes them at least more transparent for others.
- structures complex decision processes and simplifies a separation into transparent sub-aspects.
- enables a division of work and thereby a specialization on sub-problems.
- enables a parallelization of separate valuation- and decision-steps.
- provides a structured basis for discussions within a decision making group.
- considers impacts on the decision maker's individual goals and overall strategy.

To further develop the method, the following work is planned:

- intensive testing of the method on real world use-cases,
- further examination of the economic viability of privacy-enhancing telco-based IdM Services,
- enhancement of the method based on the basic model of normative decision theory,
- enhancement and improvement of each step by more sophisticated methods and concepts and for more intensive focus on privacy-related effects,
- simplification of the applicability by predefined and selectable components for each step of the approach (e.g. predefined and selectable costs and benefits, cause-effect chain elements),
- reducing possible errors caused by subjectivity of the decision maker.

References

[CL01] Camenisch, J. And Lysyanskaya, A. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 93-118, Springer Verlag 2001.

[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/

[PH2010] A. Pfitzmann and M. Hansen, "A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, Aug. 2010, v0.34.

[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