Abstract

This document contains the detailed SWIFT scenarios as well as the first version of the SWIFT use cases. The scenarios are grouped around two main categories and the first one focuses on a Telco environment, the other one on a university setting, which could be seen as a large institution, incorporating network, service and identity provider, while at the same time interoperating with third parties.

Based on these scenarios a set of use cases has been identified and categorized. Finally a business model has been developed.

The objective of this document is to guide, on the one hand, the architecture and the technical work in the WPs, in particular WP3 and WP4; on the other hands, it serves as a platform to obtain feedback from participating companies’ business units, as well as from external contractors.
Disclaimer

This document contains material, which is the copyright of certain SWIFT consortium parties, and may not be reproduced or copied without permission.

In case of Public (PU):
All SWIFT consortium parties have agreed to full publication of this document.

In case of Restricted to Programme (PP):
All SWIFT consortium parties have agreed to make this document available on request to other framework programme participants.

In case of Restricted to Group (RE):
All SWIFT consortium parties have agreed to full publication of this document. However this document is written for being used by <organisation / other project / company etc.> as <a contribution to standardisation / material for consideration in product development etc.>.

In case of Consortium confidential (CO):
The information contained in this document is the proprietary confidential information of the SWIFT consortium and may not be disclosed except in accordance with the consortium agreement.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the SWIFT consortium as a whole, nor a certain party of the SWIFT consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

Imprint

Secure Widespread Identities for Federated Telecommunications

SWIFT
WP 5 – Scenarios and Evaluation
Swift Scenarios, Use Cases and Business Models
Mario Lischka, NEC
Juergen Jaehnert, USTUTT

Copyright notice

© 2008 Participants in project SWIFT

Optionally list of organisations jointly holding the Copyright on this document
Executive summary

The SWIFT project envisioned the creation of a new identity management solution space from the perspective of an identity centred approach. In WP5 we worked on different scenarios to demonstrate the usage of a user centric identity management. As a single scenario would be too complex for a demonstration the scenario was split into scenes featuring specific aspects. These scenes are then generalized and presented as use cases. Based on the scenarios initial business models for the SWIFT project have been developed.

The document at hand presents two scenarios which are illustrating this approach from a high-level view. Each scenario contains a set of scenes showing different use cases arranged within a day of some users. The first scenario focuses on customers of a Telco operator in their private and professional environment. It is used to present the ubiquitous and privacy-enabled access to the digital world of complex future technology and services in an easy and seamless way. The second scenario is hosted in a university environment as an example of a large institution acting as a network. It features identity and service provider for various types of users. The latter also includes some interaction with a Telco operator and third party services. Depending on the context different attributes of an identity are shown to the service providers.

Out of these scenarios a set of use cases has been identified, each one focusing on a specific aspect. These uses cases have been grouped into five different categories. They are covering the Authentication and Authorization of the users and their Identity Management as well as the Access to services and the related Accounting and Logging.

Based on the scenario and a market analysis the business model of the SWIFT project has been developed, exploiting the identity management framework from a Telco perspective. The business model identify the relevant roles in the scenarios. The service and money flows in the scenarios are illustrated.

The scenarios and use cases presented in this report should be another foundation stone of the SWIFT interim architecture.
## List of authors

<table>
<thead>
<tr>
<th>Company</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dracotic</td>
<td>Elena M. Torroglosa Garcia</td>
</tr>
<tr>
<td>DT</td>
<td>Gerd Foth</td>
</tr>
<tr>
<td></td>
<td>Peter Scholta</td>
</tr>
<tr>
<td></td>
<td>Wolfgang Steigerwald</td>
</tr>
<tr>
<td>Fraunhofer SIT</td>
<td>Ronald Marx</td>
</tr>
<tr>
<td></td>
<td>Dirk Scheuermann</td>
</tr>
<tr>
<td>NEC</td>
<td>Mario Lischka</td>
</tr>
<tr>
<td></td>
<td>Andreas Pashalidis</td>
</tr>
<tr>
<td>PTIN</td>
<td>Ricardo Azevedo Pereira</td>
</tr>
<tr>
<td></td>
<td>Pedro Nuno Santos</td>
</tr>
<tr>
<td>UMU</td>
<td>Antonio F. Gómez Skarmeta</td>
</tr>
<tr>
<td></td>
<td>Manuel Sanchez Cuenca</td>
</tr>
<tr>
<td>USTUTT</td>
<td>Marc Barisch</td>
</tr>
<tr>
<td></td>
<td>David Lutz</td>
</tr>
</tbody>
</table>
# Table of Contents

Abbreviations ....................................................................................................................... 8
Definitions ............................................................................................................................... 9

1 Introduction ........................................................................................................................ 10
   1.1 Objective of this document .................................................................................. 10
   1.2 Structure of this document .................................................................................. 10

2 Scenario ............................................................................................................................. 11
   2.1 Telco Scenario ....................................................................................................... 11
      2.1.1 Actors and Roles ......................................................................................... 11
      2.1.2 Components and Interfaces ......................................................................... 12
      2.1.3 Prerequisites ............................................................................................... 13
      2.1.4 Scenario Description .................................................................................... 14
   2.2 University Scenario ............................................................................................... 17
      2.2.1 Actors and Roles ......................................................................................... 17
      2.2.2 Components and Interfaces ......................................................................... 18
      2.2.3 Prerequisites ............................................................................................... 22
      2.2.4 Scenario Description .................................................................................... 26

3 Use Cases .......................................................................................................................... 30
   3.1 Authentication ......................................................................................................... 30
      3.1.1 Face to Face User Identification .................................................................. 30
      3.1.2 Online User Identification ............................................................................ 31
      3.1.3 Basic Authentication .................................................................................... 32
      3.1.4 Group-affiliation-based authentication .......................................................... 32
      3.1.5 Network Authentication .............................................................................. 33
      3.1.6 Authentication Context Exchange ................................................................. 34
      3.1.7 3rd Party Authentication .............................................................................. 34
      3.1.8 Re-Authentication in Foreign Networks .......................................................... 35
      3.1.9 Service Authentication .................................................................................. 36
   3.2 Authorization ............................................................................................................ 36
      3.2.1 Authorization by Policy ................................................................................ 36
      3.2.2 Re-Authentication for Authorization ............................................................... 37
      3.2.3 Authorization by Attribute Verification .......................................................... 38
      3.2.4 Deduction of Access Policies ........................................................................ 39
   3.3 Identity Management ................................................................................................. 39
      3.3.1 Creation of a virtual identity for service usage ............................................... 39
      3.3.2 Selection of a virtual identity for service usage .............................................. 40
      3.3.3 Implicit Identity selection ............................................................................. 41
      3.3.4 Selection of Roles ........................................................................................ 41
      3.3.5 Setting up and modifying end-user profiles and policies .................................. 42
      3.3.6 Delegation of usage rights .......................................................................... 43
      3.3.7 VID change ................................................................................................. 43
      3.3.8 Session handover ........................................................................................ 44
      3.3.9 Pseudomized Communication .................................................................... 45
      3.3.10 End-user registration at Identity Aggregator .................................................. 45
      3.3.11 End-user registration at the Attribute Provider ............................................. 46
      3.3.12 Multi-Layer Single Sign On ........................................................................ 47
      3.3.13 Reverse Multi-Layer Single Sign On .............................................................. 47
      3.3.14 Anonymous Attribute Transfer ................................................................... 48
      3.3.15 Provision of Community Services ................................................................. 49
      3.3.16 Event based policy resolution ..................................................................... 50
   3.4 Accounting and Logging ............................................................................................ 50
      3.4.1 Basic Accounting ........................................................................................... 50
      3.4.2 Anonymous charging of service usage .......................................................... 51
      3.4.3 Changing of Service Quality and Charging ................................................... 52

© EU SWIFT Project No. 215832 participants
3.5 Access ............................................................................................................................................... 52
  3.5.1 IdP-initiated service access........................................................................................................ 52
  3.5.2 SP-initiated service access ....................................................................................................... 53
  3.5.3 Access to Composite Provider ............................................................................................... 53
  3.5.4 ID-supported network handover ............................................................................................. 54
4 Business Model ........................................................................................................................................ 55
  4.1 Business Eco System .................................................................................................................... 55
    4.1.1 Market Analysis .................................................................................................................. 55
    4.1.2 Target Group Analysis ....................................................................................................... 56
  4.2 Business Models from SWIFT Scenarios ..................................................................................... 57
    4.2.1 Business Model University Scenario ................................................................................ 59
    4.2.2 Business Model Telco Scenario ...................................................................................... 62
  4.3 Business opportunities .................................................................................................................. 65
Annex A Bibliography ............................................................................................................................. 67
List of Figures

Figure 1: Lecture Infrastructure ....................................................................................................................... 26
Figure 2: Identity and access management market volume [1] ........................................................................... 55
Figure 3: Identity and access management market CAGR [1] ........................................................................... 56
Figure 4 Symbols for Roles ............................................................................................................................. 58
Figure 5: Relationship between Roles ............................................................................................................. 58
Figure 6: Elements of the illustrations .............................................................................................................. 58
Figure 7: Actors and roles / Flow of money and service .................................................................................... 59
Figure 8: University scenario business ............................................................................................................. 60
Figure 9: University scenario Prof. Peter's business .......................................................................................... 61
Figure 10: University scenario book business ................................................................................................... 61
Figure 11: University scenario football business .............................................................................................. 62
Figure 12: Telco scenario John morning business ........................................................................................... 63
Figure 13: Telco scenario John office business ................................................................................................. 63
Figure 14: Telco scenario John afternoon business ......................................................................................... 64
Figure 15: Telco scenario Karin business in the morning .............................................................................. 64
Figure 16: Telco scenario Karin business daily activities ................................................................................ 65

List of Tables

Table 1: Internet usage (Source [2]) .................................................................................................................. 57
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>CoD</td>
<td>Content on Demand</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>FU</td>
<td>Foreign University</td>
</tr>
<tr>
<td>FUL</td>
<td>Foreign University Library</td>
</tr>
<tr>
<td>HU</td>
<td>Home University</td>
</tr>
<tr>
<td>IdM</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>ISIM</td>
<td>IMS Subscriber Identity Module</td>
</tr>
<tr>
<td>LoA</td>
<td>Level of Assurance</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>VID</td>
<td>Virtual Identity Identifier</td>
</tr>
</tbody>
</table>

Additionally some abbreviations are defined for the various roles presented in the next section.
Definitions

In activity 3.1 a set of basic roles has been identified for the further usage within the project. These roles are used within this document to classify the various actors.

- **Identity Aggregator (IdAgg)**
  The IdAgg is responsible for the management of user profiles, Virtual Identities, SSO mechanisms and statements, etc.

- **Authentication Provider (AuthNP)**
  An AuthNP provides methods to verify the user’s authenticity.

- **Attribute Provider (AttP)**
  An AttP manages information of the user in terms of attributes, which can be related to specific services or for general purpose.

- **Identity Provider (IdP)**
  The IdP combines the roles IdAgg, AuthNP, and AttP.

- **Accounting Provider (AcP)**
  An AcP performs accounting on a service used by an end user.

- **Charging Provider (CP)**
  The CP charges the user's service (including network services) subscriptions and usages.

- **Billing Provider (BP)**
  A BP is responsible for billing and clearing post-paid services to the subscriber.

- **Service Provider (SP)**
  A SP provides some kind of service to the end user. This role also includes the network service provider role as one special form.

- **End-user**
  The end-user makes use of the services provided by the IdM system (IdAgg, AuthNP, AttP) and the SP. It is possible to differentiate between the following sub-roles.

  - **IdM Subscriber**
    An IdM subscriber has at least one subscription with an IdAgg, an AuthNP, and an AttP. If the latter roles are combined in terms of an IdP then one subscription with an IdP is sufficient.

  - **(Service) Subscriber**
    The subscriber is a legal person that has a subscription with at least one service of an SP. Furthermore, he is also an IdM subscriber.

  - **(Service) Consumer**
    The consumer consumes a service of an SP. The service subscription (to the SP) is created by the subscriber. The subscriber also defines how a subscription will be used by the consumer. The consumer is also an IdM subscriber.
1 Introduction

This document contains the detailed SWIFT scenarios as well as the first version of the SWIFT use cases. The initial version of the scenarios has been part of the SWIFT interim report M501, but based on the discussion in the WP, as well as in the project as a whole, some refinements have been taking place. The scenarios are now grouped around two settings, the first one focusing on customers of a Telco operator, the second one on a university environment as an example of a large institution acting as a network, identity and service provider for various types of users. The latter also includes some interaction with a Telco operator and third party services.

A setup of use cases has been identified out of these scenarios. Each use case is focusing on a specific aspect which is presented in a well-defined schema. All of them are grouped into a set of categorises.

Based on the scenario and a market analysis the business model of the SWIFT project has been developed. Due to the expertise in the project this exploitation scenario has a Telco perspective.

1.1 Objective of this document

According to the project specification, this document will on the one hand be used to guide the architecture and in particular the technical work in WP3 and WP4, but also serves as a platform to obtain feedback from participating companies’ business units, as well as from external contractors.

Together with the interim reports of WP3 and WP 4 (M301 and M401 respectively), the scenarios and use cases, this report should be another foundation stone of the SWIFT interim architecture, whose core aspects are presented in D203 “First Draft of the Identity-driven Architecture and Identity Framework”.

1.2 Structure of this document

This document is comprised of three main sections each of them focusing on one aspect stated in the deliverable title. Nevertheless they are closely related. In section 2, we present the scenarios which should illustrate the needs of the users for a user centric solution of the identity management on the one hand and sketches the technology provided by the SWIFT project on the other hand. While these scenarios are embedded into two main story lines, the different aspects shown have been dispersed into use cases presented in section 3. As identity management in general is considered a future market which is discussed in section 4, we also discuss potential business models of the scenarios presented.
2 Scenario

In following subsections 2.1 and 2.2 we present two scenario settings the first one describing a pure Telco environment while the second one is suited in a university environment. Each of these scenarios first gives a general outline, after that the actors and roles are presented. Then an overview of the components and interfaces is given, followed by the prerequisites for the scenario as a whole. Finally, the scenario is described in detail, structured along the timeline of a day in the life of an end-user.

2.1 Telco Scenario

The Telco scenario describes a day in the life of Karin and John. The scenario is structured in different scenes and will show Karin and John in their jobs and private environment. The scenario is clearly user driven and user focused and is going to demonstrate how Karin and John – as users – will handle complex future technology and services easily and seamlessly. The scenario starts in the morning and continues through the day until an evening event. The SWIFT project takes this scenario as a basis in order to demonstrate the ubiquitous and privacy-enabled access to the digital world. It aims to show that users only have to handle a minimum number of service contracts. The different scenes in the scenario also consider identity privacy between services, and user control over data.

2.1.1 Actors and Roles

Consumer (Karin, John): The consumer is an entity to which a service is provided. The consumer may represent an individual entity (single consumer) or a group entity (e.g. a family) that has requested a service. The access to this service requires a valid identification and/or authorization. There may be different sorts of consumers with different access rights inside a group (e.g. limited access for children inside a family). Some sort of "super-users" may have special privileges like registering or deleting other consumers or modifying the access rights of consumers inside a certain group. In the given scenario we see Karin and John, who are different consumers and share some subscription contracts.

Subscriber (Karin, John): The service subscriber is the holder of a contract associated with one or more services and is responsible for the respective service payment. Subscriber and user can be one and the same but can also be represented by different entities. In particular, the subscriber may also play the role of a super-user as mentioned above. The subscriber can delegate a subset or even all of its access rights to another user but continues to be responsible for service payment. For example, a child could be a user of a specific content on demand (CoD) service, while access to which would be authorized and paid by its legal guardian (subscriber). In the Telco scenario Karin and John both play the role of service subscribers.

Home Telco operator: The home telco operator manages one or more access networks and their related components for performing authentication, authorization, accounting, and charging. The home telco operator also manages User identities and related information, providing them to other actors when necessary (according to the user’s privacy settings and regulatory demands). Additionally, he can also provide authentication assertions (conveying information about a successful authentication of a subject) to other actors. Overall, the home telco operator plays the role of the user/subscriber home network provider.

Foreign Telco operator: The foreign telco operator manages, just like the home telco operator, one or more access networks and their related components. It has an agreement with the home telco operator so that the subscribers and associated users of the home telco operator can use the foreign network for roaming purposes.

Enterprise operator: The enterprise operator manages the access and authentication to the enterprise intranet and the associated services. He has an agreement with different telco operators that ensure his privacy requirements of himself and those of his employees.

3rd Party Service Provider: The 3rd party service provider is in charge of providing the requested service to the user. Depending on the type of service requested, the service provider (SP) may require user
authentication and/or retrieval of certain User attributes from the user’s authentication and attribute provider. The 3rd party service providers in the telco scenario are:

- news service provider
- webmail service provider
- public transportation service provider
- media service provider

2.1.2 Components and Interfaces

This section introduces the components and interfaces that are employed in this scenario.

Karin’s PDA: Karin owns a private PDA, which she also uses for some company and society matters. Among the typical features such as making phone calls, accessing services on the Internet or her company’s intranet, reading e-mails etc., the PDA allows selecting and managing virtual identities (VIDs). Therefore, the PDA has to support the Identity Management (IdM) developed by SWIFT. By selecting different VIDs for different purposes Karin can control the personal information she reveals in her interactions with other SWIFT enabled services.

John’s PDA: John uses a PDA that his company gave to him. John stores business as well as private contacts on his device. John’s PDA has similar features as Karin’s PDA. In particular, it is also SWIFT enabled, i.e. it allows selecting and managing VIDs to use these with other SWIFT enabled services.

Car Hi-fi Multimedia System: The car hi-fi multimedia system is capable to play music from a media library. The media library is provided by a media service provider in the internet. The multimedia system provides a screen that enables the user to select music titles. Since the car is company owned, the connection to the internet is provided and paid for by the company.

Home Telco operator: The home telco operator offers services like telephony, broadcasting, or e-mail services. For this scenario, the home telco operator has to provide for an access network, a transport network (backbone), a middleware for accessing services, and a system for managing the user’s virtual identities and related attributes (identity management) developed in the SWIFT project.

Media Service Provider: The media service provider provides personal media libraries for its users and facilitates access to an online music store where the user can buy new music titles or albums.

Private Online Media Library: The online media library is hosted by the media service provider. Access to the library is restricted to a predefined set of users, in this case Karin and John.

Deep-freezer: Can read RFID signal from the food inside it. Has an interface to the facility management component (see below).

Webmail Service Provider: The webmail service provider hosts e-mail accounts accessible via the internet. Karin has an e-mail account at this provider where she received personal e-mail messages.

Facility Management: The facility management system of Karin’s and John’s apartment interconnects all electronic devices that are permanently located within the apartment. This includes TV, hi-fi multimedia system, household appliances and also the electronic heating control system. The facility management can supervise the current status of each device is capable of switching devices on or off if this is requested by the user.

Family White Board: Family members can leave messages on the family white board for other family members. The can also be done remotely, e.g. by using a mobile phone and transmitting the message by Bluetooth, SMS, MMS etc.

Personal Video Recorder (PVR): The PVR features remote programming so privileged users can program it via their mobile device, desktop computer and so forth.
Desktop Computer: The desktop computer in this scenario is connected to the company’s intranet and is capable of receiving remote commands to start-up its boot sequence. Furthermore, it can preload applications and settings depending on the user who is going to use the computer.

Meeting Room Management: The meeting room management is able to make room reservations on the fly. Additionally, sensors in the rooms can determine the participants in the meeting and adapt the environment within the meeting room to their preferences.

Restaurant Payment Services: After visiting a restaurant the guest can use the restaurant’s payment services to pay his bill. This service provides for different types of payment including anonymous payment.

Restaurant’s Menu Service: If a guest is not able to speak or understand the language the menu card is written in he can use the restaurant’s menu service to receive a translated version of the menu. This service also enables a guest to define preferences. So every time the guest enters a restaurant that offers this service the menu is translated and presented to the guest in the predefined language.

Event Organization Environment: The event organizing environment provides a set of tools to organize events, e.g. for a society. It offers the ability to specify the name of the event and of the organization team, specifying the members of the organization team and their reachability. Furthermore, the members can send invitation to firms for subscription to the event based on the companies’ profiles and to set up of a network based event calendar with all important dates.

Public Transportation Service Provider: Among others the public transportation service provider sells tickets for the public transportation corporation. People can order different types of tickets, e.g. for a single ride, or for a whole month. Bought tickets are sent electronically to the user’s preferred device.

Public Transportation Service Provider wireless network: The wireless network is a special service of the public transportation service provider. The network may be used for ticket validation.

Public Transportation Services Access Control: The access control facilities ensure that only people who have a valid ticket can use the public transportation services. Thus, when a passenger passes access control his (electronic) ticket is validated. Therefore, the passenger’s device presents the ticket either by transferring it wirelessly or by presenting it visually on screen. The access control facilities check if the ticket is valid and grant or deny access, accordingly.

Company Intranet Services: As mentioned earlier, desktop computers allow for remote control. Company intranet service might be a remote controlling entity; managing the users’ workspace, his preferences, calendar etc.

Restaurant Query and Reservation System: Users who are searching for a restaurant can use the restaurant query to find one and the built-in reservation service to book a table.

Main Station’s Lounge Network: The lounge network offers passengers that are waiting in the main station’s lounge to pass the time online. The network also feature service-bound access, i.e. the service will pay for the network access charges. Upon access request, these charges are negotiated in background between the lounge network and the service provider transparent for the user.

Cinema Reservation System: The cinema reservation system is an online shop for cinema tickets that provides electronic cinema tickets.

Cinema Admission Control System: The admission control system in the cinema can validate the electronic tickets issued by the cinema reservation system and will grant access as soon as a valid ticket is presented.

2.1.3 Prerequisites

This section provides an overview of the prerequisites of each of the scenario’s components in brief. Lots of actions must have been done, before the scenario ideas could work, and these actions are described here using bullet points.
Users

- John has a subscription with the home telco operator.
- He needs means for handling access rights delegation and for controlling the services being used.
- He has a subscription with a network operator for accessing the network.
- Furthermore, he already delegated its access rights to Karin.

Telco operator

- Support for SWIFT IdM Framework.
- Identity federation with other IdPs.

Enterprise operator

- The enterprise operator must also support the identity management system provided by the Home Telco operator.

3rd Party SP

- The 3rd party service provider must support the home telco operator’s identity management system.
- Additionally, it has to maintain service profile for each user and provide means for a user to personalize each service.

2.1.4 Scenario Description

The scenario describes a day in the life of John and Karin. John, the family father, is the subscriber of the services of his home telco operator’s services, like telephony, broadcasting, or e-mail services. John works as a sales man and is very technician. His wife Karin, as a user of the services subscribed by John, was granted access to these by John. Karin is a working woman. Her life is well-balanced between her job as a designer and her family. In addition to this, she is very active in different societies and from time to time she takes over the tasks of organizing social events for her society. She is a subscriber and user of a media service provider. John is an additional user and Karin granted the rights to use the online library of her media.

2.1.4.1 Karin’s day

Breakfast

Karin’s day begins with the planning of the meals for the next three days along with the preparation of the required shopping list. While discussing with John what to buy, she checks the latest recipes of her online cooking community. Karin knows that John’s and her own preferences regarding food items are taken into consideration including John’s allergy against fruit acid. Karin gets an updated version of her shopping list after a short check with the content of the deep-freezer based on collected RFID signals from the foodstuffs. The list is automatically adjusted with the latest offers of her preferred food discounters.

After reading the latest online news with her laptop Karin starts her webmail service to check her emails. While browsing her inbox, she gets personalized advertisement email with information based on her published news profile. In it, she finds the surprising information that the audio book version of her favourite author’s latest book has just been published.

Way to work

Karin drives with her company car to work. To better take advantage of her time in-between home and work, she decides to listen to an audio book from her private online media library. The car hi-fi multimedia system presents the list of her already purchased audio books (a service of her media service provider), but Karin can’t find anything really interesting. She then remembers the notice she got in her email about the recently released audio book from her favourite author. She navigates to the online media shop of her media service provider and buys the audio book. While commuting to work she enjoys the audio session. When Karin
arrives at her workplace, she leaves the car and continues to hear the audio book seamlessly on her PDA via a foreign telco operator.

**Facility remote control**

On the way to work Karin gets a warning to verify her home energy consumption due to abnormally high values considering no one is home. Karin finds out that John has forgotten to shut down the TV entertainment system. As John is already in a meeting, the facility management system wants her permission to do this now. Karin agrees and leaves a reminder to John on the family white board to better shut the TV off before he leaves home. She takes advantage of the opportunity and sets her PVR to record her favourite TV, because she and John have planed to be in the cinema at this time.

**At work**

When Karin arrives at her business premises, her PDA recognized that she has arrived at work and automatically starts the “welcome” process that has been specified by Karin at an earlier time. Hence, her PDA starts her business presence service and sets her status to ”available”. Furthermore, the PDA notifies to the company's time recording that Karin as arrived. Finally, the PDA starts Karin's computer at her desk including all necessary application, so she won't have to wait when she arrives in her office. Her PDA receives new and updated meeting information automatically.

As she arrives at her office, she finishes polishing a presentation that she will give the day after. She notes that she has a couple of open issues she would like to resolve with her boss and a colleague. Both of them will attend the meeting. Shortly afterwards, she is notified that they are both available for a 30-minute talk. An unscheduled meeting is automatically arranged in the boardroom on-the-fly for the three of them. As they enter the room, the environment is adapted to the group settings: air-conditioning is set to an acceptable temperature, the projector is switched on, curtains are rolled down, resources including the presentation under discussion are uploaded on the company server and their access is restricted. The group settings are derived from the individual preferences of the attendees. The boardroom is tagged as ‘not available’ for a time slot of 30 minutes.

**Lunch**

Karin goes to lunch with some of her colleagues. She notices that her restaurant balance account is nearly empty. She recharges her account, without revealing any personal financial information, with the help of the payment service provided by her telco operator, amount which will be charged along with her monthly telephone bill.

When entering the restaurant, Karin and her foreign colleagues anonymously solicit an electronic version of the menu on their PDAs. The menu is received in the preferred language to each colleague and her.

**After Work**

Today, Karin has to leave her work earlier because of the organization of a social event of her society. The organization is in a very early stage and Karin has to set up at first the event organization environment. For this she gets different project tools from her telco operator:

1. Name of the event and of the organization team (association with temporary identifier like telephone number, email address etc.)
2. Members of the organization team and the reachability of them
3. Invitation to firms for subscription to the event based on the companies profiles
4. Set up of an network based event calendar with all important dates

She schedules a telephone conference with the organization team to the next day. Every member gets the message and agrees to the network calendar. Karin knows that only one push on the conference button is enough to begin the audio conference at the agreed time very quickly.
Evening Event
The organization of the social event takes more time than Karin thought. She informs John via SMS that she has been delayed at work and will be 15 minutes late, and suggests that the meeting point with John be changed to the front of the cinema, to which John agrees. She arrives at the cinema where John is already waiting for her. Quickly Karin changes her availability to “Don’t bother me” and every communication, except emergency calls is routed to her messaging box. She then enjoys a beautiful evening with John.

2.1.4.2 John’s day

Breakfast
In the morning Karin and John are eating breakfast. John is reading the latest news using his business PDA. This online news service was composed and personalized taking into account his interests stored in his user profile within the home telco operator. While doing so they talked about the shopping list because Karin was planning the meals for the next few days. Karin receives a pleasant surprise when John invites her to the cinema later in the evening. They both look forward to the movie and all the things that belong to it like popcorn and soft drinks. Karin then leaves for work, Meanwhile John watches a few minutes of the morning news on the TV entertainment system, updates his podcasts and starts listening to them while on his way to work.

Way to work
John decides to use public transportation in order to get to his workplace. His monthly pass has however, already expired and he needs a new one. Therefore, at the train station, he buys it online from the Public Transportation Service Provider wireless network using his business PDA. He gets an electronic ticket for his usual routes on his preferred device and gains access to the public transportation services.

At work
At work John performs the role of a sales person. As such, and in order to access his company intranet, he authenticates himself as a sales person and later on loads his personal work profile preferences (personalized workspace, facilities, calendar etc.). John uses his mobile device for managing both company related as well as private contacts. When he arrives at work the device switches automatically to “working” mode, so all personal communications are automatically redirected to his personal message box. John is however expecting a very important call from his financial advisor, so he changes his current work profile communication settings in order for this call to be put straight through to him, bypassing the "working" mode. However, the message of his home’s facility management system does not reach him. Instead of leaving a message the facility management system redirects its request to Karin.

Lunch
John agrees to have lunch with some business partners in half an hour. When searching for a restaurant John includes the preferences of all participants and accepts a location based search. The service finds a great Mexican restaurant not far from his workplace and John reserves a table for a group of six people. The service informs each participant about the reservation through various mediums (instant message, e-mail, etc.), dependent on the availability of each. During the meal John receives his important call from his financial advisor, which is not blocked as other “non business calls” due to the setting he made earlier this morning. Since it was a business lunch John pays the bill as an employee of his company with his business mobile phone, without revealing any personal details.

After Work
After work John's train is delayed and he has to wait in the main station’s Lounge. John specifies that he wants to use his online media service. Following this desire, the “Lounge Network” (the local network provider) and his media service provider negotiate in the background about the payment method and basic access rights. They conclude that media service provider can cover the fees related to the network access (service bound access). After that John is informed about the access conditions to the media service, to which he agrees, and is granted access. He starts to browse his private media collection and discovers that a new audio book has been bought by Karin. He is curious about the audio book’s theme and decides to listen to a small free excerpt of said audio book. He later decides to hear the whole audio book during his way home. That’s no problem because the audio book is already bought by Karin. But when he clicks on the link to the audio book his current access provider “Lounge Network” blocks the access, as media streaming is not included in the negotiated access covered by media service provider. Thus “Lounge Network” ask John if he wants to pay the add-on fee of 1 Euro for the next hour (for improved access conditions and QoS). The extended access is granted to him as he accepts the add-on fee, which is billed to his media service provider. After a 30 minute delay, the train finally arrives at the main station and John begins his journey home. John enjoys the audio book without any interruption throughout the whole journey.

Evening Event

On the way home John buys the online cinema tickets for the evening with Karin. He gets bonus points for presenting his customer loyalty card number and after accepting the payment method (credit card) John receives the tickets on his mobile (2D Barcode).

John and Karin are brought into contact in front of the cinema. While entering the cinema and checking the tickets no private data will be divulged. Based on the cinema date entry in the calendar (network based) all communication channels of the mobile devices of John and Karin will automatically redirect to their respective message boxes. Now they can enjoy the movie - and the popcorn.

2.2 University Scenario

The university scenario shows a day at the Foreign University including two professors Peter and Paul (the later at the Home University (HU) and three students Harry, Fiona, and Tom. Each of the students is bound to a different identity aggregator and is doing several things during the day. Sometimes the students act on their own and sometimes they interact together. This section provides at first an overview of the day of all participants whilst the next subsections describe the day of the characters in detail.

The day starts for all the students and one of the professors at 08:00 with the lecture on communication networks. Afterwards, the students are using the Foreign University (FU) E-Learning platform for communication while the professor does some administrative work. Whilst the three students work in the afternoon alone, they met together in the evening again for viewing a football match.

2.2.1 Actors and Roles

Home University: Harry’s home university (HU) hosts study relevant data and account information; therefore, it is responsible for authenticating its students. It is allowed to collect and to distribute the students’ data based on their policies to other institutions participating in the same trust-federation, because HU plays also the role of an identity aggregator. The HU hosts further for all students studying there a small amount of money for paying purposes within the European academic federation.

Foreign University: The Foreign University (FU) offers services like network access to all students studying there. Roaming students, who belong to a university participating in the same trust-federation, may have the same rights as students belonging to the FU regarding some services, e.g., network access. Other services, e.g., virtual labs, are protected with stronger policies. The consumption of audio data, e.g., is restricted to those students studying the accordant subject. As the HU, FU also acts as identity aggregator and is responsible for the authentication and attribute provisioning of its students.
**Foreign University Library:** The Foreign University Library (FUL) is a special institution of the FU. It allows all students studying at FU to borrow books, if they can authenticate themselves. Foreign students have to pay a small fee when borrowing books.

**Foreign University Cafeteria:** The cafeteria of FU provides lunch information which is sent directly to the customer’s terminal when they enter the building and have their preferences set in such kind that the receiving of lunch information messages is allowed.

**Professor Paul:** Professor Paul is the Bologna coordinator at HU and therefore responsible for checking the courses, the HU students are taking at foreign universities. He is informed by Peter that Harry is visiting Peter’s lecture and Paul needs to check Peter’s lecture documents.

**Professor Peter:** Professor Peter is a professor for computer science at FU. He uses the FU E-Learning platform to support his lecture. During his day at the university he holds a lecture, contacts some tutors and does correction of the student’s homework.

**Student Harry:** Harry studies computer science at HU, but he decided to study one semester abroad at FU. Since FU and HU are both members of the European Academic Federation, students often chose to study one semester at a foreign university, because they don’t have to do any hard administrative paperwork. The usage of SWIFT supporting applications allows the participants of the academic federation an easy exchange of relevant data between the universities. Therefore, Harry is able to use the FU facilities with his HU account.

**Student Fiona:** Fiona is a student of computer science at FU. She has chosen FU to host her data, thus, FU acts as identity aggregator and is responsible for the authentication and attribute provisioning of her. She uses SWIFT, since the benefits of this framework make her day at the university easier than before.

**Student Tom:** Tom is, like Fiona, a student at FU that studies computer science. But in difference to her, he has chosen his telco operator to act as identity aggregator. His study related Attributes are still stored at FU, however. He uses SWIFT to combine the benefits of his Telco identity aggregator with the attribute providing component at FU.

**Telco Operator:** The telco operator is a common operator that offers identity aggregator functions as a new service to its customers. This simplifies its own authentication and authorization process, but empowers the operator also to offer more services that some of its competitors.

**Bookstore:** The bookstore is an online book store at FU. It allows the access from the FU network to offer books to the students studying there. Since it supports SWIFT, students does not need to have an account at the bookstore, they could use their university account for accessing it.

**Football Stream Service Provider:** The football stream service provider offers live streams of the most important European matches. Since it does not want to generate an account for every customer, it uses the SWIFT framework to make use of accounts the customers already have. To convince its customers to use payment by telco bill, which makes the charging very easy for the service provider, it offers a small discount to all telco customers that agree to pay using their telco account.

**Conference Service Provider:** The conference service is a service provider that acts as a composite service provider. It receives requests for many different kinds of services, such as flight ticket booking, hotel search, printer jobs, etc. After receiving a request, it collects the demanded services from other service providers and offers the access to the found services to the requestor in a specific interface.

### 2.2.2 Components and Interfaces

This section provides an overview about all components and especially all devices used within the scenario. At first, each player of the scenario is mentioned together with a listing of the devices, he/she is using. Afterwards, the capabilities of each component are explained in detail. The assignment of components/interfaces to the player’s in the scenario is done in the following way:

**User Devices:** Each player is equipped with a set of personal devices which are used for accessing the various services in detail:
• Professor Peter uses a SWIFT enabled laptop and a SWIFT enabled smartphone.
• Professor Paul uses only a SWIFT enabled computer terminal.
• Student Harry uses a SWIFT enabled laptop and a SWIFT enabled smartphone.
• Student Fiona uses a SWIFT enabled laptop, a SWIFT enabled smartphone and a SWIFT enabled home entertainment system.
• Student Harry uses a SWIFT enabled laptop and a SWIFT enabled smartphone.

Home University: Under the umbrella of the Home University a lot of different components with even more interfaces exist. At first, the HU acts as identity aggregator, this means that it must have every interface related to that. Furthermore, HU is responsible for the authentication and attribute provisioning of its students. Although it is not necessary to have all those functions bundled within one entity, in this scenario it is assumed for simplicity. Neither the key elements of the scenario nor the SWIFT architecture have to be changed for having each component in one independent entity. Since HU deals with the student’s data and even releases them, it needs an interface for the students to manage their data. The fact that HU acts also as the student’s payment provider requires both, a payment provider (PP) interface as well as an account hosting function.

Foreign University: Within this scenario, FU plays the role of a service provider and offers several services to the students that study there and, further more, is responsible for the authentication and attribute provisioning of its students and acts as identity aggregator. The services that are used by the students are the wireless network access and the access to the several functions provided by the FU’s E-Learning platform. But since FU is also an identity aggregator and offers further authentication and attribute provisioning, it has to establish all related functions of this aspect, too.

Book Store: FU offers a Books store, where students get small discounts when they are studying at FU. Therefore, it needs a service provider Interface, which checks the consumer’s authentication and requests some attributes of him from his identity aggregator.

Foreign University Library: The FUL acts as another service provider in the scenario. Although the students need network access at the FUL, too, it is assumed that the FU’s network covers also the FUL. The service, the FUL offers, is the borrowing of books, with no cost for local students but with a small fee for roaming ones. Therefore, the FUL needs a payment-enabled borrowing terminal. Since the status of the student is important for the handling at the FUL, the FUL’s policy decision point needs attributes about the consumer. These attributes will be collected by contracting the students’ identity aggregator as in the network access case before.

Foreign University Cafeteria: The cafeteria at FU offers a service for all people standing in the queue and waiting to be served. To avoid long time choosing of the different provided meals, the cafeteria sends automatically the daily menu options to all entering persons who have accepted the delivery of such a message.

Telco Operator: Within this scenario, the telco operator plays only the role of an identity aggregator and is, furthermore, responsible for providing some attributes of its customers. Therefore, the only functions that have to be enabled there are those related to the identity aggregator and Attribute Provider role.

Live Match Service Provider: The football stream service provider offers services related to football match streams to its customers. However, since it acts as a service provider, only those functions related to the provisioning of services must be realized.

Conference Service Provider: Since the conference service provider acts as a composite service provider, it needs firstly a full service provider interface that supports authentication and authorization as well as payment and, secondly, it has to be able to contact other service providers like a common consumer.

The next subsections describe the needed components of the scenario actors in detail.
2.2.2.1 Laptop

The laptop is SWIFT enabled, i.e., it contains the SWIFT federation and identity management application. Furthermore, it is able to store SWIFT SSO statements, it uses the common technology to connect to wireless LANs, it supports handover, etc. In general, the laptop supports each of the SWIFT requirements mentioned in the accordant SWIFT documents.

2.2.2.2 Smartphone

The smartphone has the same abilities as the student’s laptop and is equipped with the same applications. It supports WLAN communication in addition to 3GSM networks.

2.2.2.3 Computer Terminal

A standard computer terminal (e.g., a PC) is used and equipped with SWIFT enabled software. It is used by Professor Paul for accessing data at FU.

2.2.2.4 Home Entertainment System

The Home Entertainment System is compatible to the SWIFT framework, i.e., it supports the SWIFT identity management functions and provides information distribution as well as handover support. It is used by Fiona to watch a video stream.

2.2.2.5 Identity Aggregator

The identity aggregator (IdAgg) redirects the students or telco customers based on the requests to their authentication provider or it collects their attributes from all their Attribute Providers. It is the main source for all the students’ or customers’ attributes.

2.2.2.6 Authentication Provider

The authentication provider hosts the students’ or telco customers’ credentials, e.g., username and password, certificate information, etc. The students / customers will be redirected from their IdAgg to their authentication provider to which they submit their credentials. If the submitted credentials match the stored information, the students / customers are seen to be authenticated and the SWIFT SSO statement is sent to them.

2.2.2.7 Attribute Provider

The Attribute Provider at the universities hosts some of the students’ attributes, e.g., the study branch or the student’s grade, while the Attribute Provider at the telco may host other data, such as credit card information. Whenever the students’ / telco customers’ attributes are required for authorization, their IdAgg requests the attributes from the accordant Attribute Provider.
2.2.2.8 Payment Provider

The payment provider offers payment services in the federation in that manner as the authentication provider offers authentication services. The students could have a small amount at an account at the PP, which is located at HU. This amount could be paid using the federation infrastructure, architecture and even its language, e.g., SAML. In this scenario the PP is used to pay the fee for roaming students at FUL.

2.2.2.9 Network Provider

The network provider component is established at FU, since one of the services, it offers to the student, is wireless network access. To find out, whether the access seeking person is a student, the person’s IdAgg is contacted with request for attributes. Only if one of the attributes proves that the person is a student, access is granted. Therefore, the network access point must be SWIFT enabled and should contain a policy enforcement component. A second network provider may be established by the telco operator and used, if the students leave the area covered by the FU’s WLAN.

2.2.2.10 E-Learning Platform

Another service of FU is the E-Learning platform, which is offered to all students studying there. It is composed of several virtual classrooms as well as audio data of passed lectures. Students who have missed a lecture could listen to the audio record taken of that session. But access to the audio streams is restricted to those students studying the accordant subject. Therefore, among the audio delivering service a policy decision point has to be established that handles the access control to the resource.

2.2.2.11 Book Store Service Provider

The information needed for the book buying is of the same kind used for every authorization plus payment information. The book store service provider needs only to know, if the person is a student of a specific subject, to what address to deliver the book later on and how the consumer wants to pay. Therefore, a common SP interface plus payment support is needed.

2.2.2.12 Borrowing Service Provider

The information needed for the borrowing process is of the same kind used for every authorization. FUL needs only to know, if the person is a student and to which university he belongs. Therefore, a common SP interface is needed. In addition to that, the FUL’s books and the borrowing terminals have to be enabled to support automatically borrowing using SWIFT technology.

2.2.2.13 Lunch Information Service Provider

The lunch information service provider at the FU’s cafeteria provides information about the daily menu options by sending a short message to all the people entering the building who have allowed the receiving of such messages. However, if those people allow the transmission of some attributes, too, the lunch information SP offers the menus with recommendations.
2.2.2.14 Live Match Service Provider

The information needed for the match stream buying is of the same kind used for every authorization. The provider needs to know if the customer belongs to a telco operator and what are the supported payment processes. Therefore, a common payment enabled SP interface is required.

2.2.2.15 Service Bundling Interface

The conference service provider needs an interface to bundle services, because of acting as a composite service provider. The interface is able to collect complex requests, to split them up into several small service requests and to contact then other service providers. Access to the required services is then offered to the requestor in the same interface.

2.2.2.16 Federation Payment Interface

The fact, that the FUL needs sometimes payment to grant access to its services, distinguishes it from many other SPs in the academic world, where only the authorization by attributes is foreseen. To handle the consumer’s payment, an interface for contacting the consumer’s payment provider should be established.

2.2.3 Prerequisites

This section provides an overview of the prerequisites of each of the scenario’s components in brief. Lots of actions must have been done, before the scenario ideas could work, and these actions are described here using bullet points. But not only the required actions, the needed abilities and behaviours are mentioned, too.

Federation:
- Federation is set up with an existing trust relationship
- Federation supports SWIFT framework

Home University:
- Federation contract with the European Academic Federation
- Support for SWIFT framework
- Attribute provider ability
- Identity aggregator ability
- Authentication provider ability
- Payment provider ability
- Some people’s VIDs are assigned to the group “Bologna Coordinators”

Foreign University:
- Federation Contract with the European Academic Federation
- Support for SWIFT framework
- Attribute provider ability
- Identity aggregator ability
• Authentication provider ability
• Offers lecture in computer science (by Professor Peter)
• Established a network accessible for all students and all professors at FU
• Offers an E-Learning platform with audio streams of passed and ongoing lectures

Professor Peter:
• Has a SWIFT enabled laptop
• FU authenticates him
• FU provides his attributes
• Has an account at the identity aggregator at FU
• He is a Professor for computer science at FU
• Uses the FU E-Learning platform to support his lecture

Professor Paul:
• Has a SWIFT enabled PC
• HU authenticates him
• HU provides his attributes
• Has an account at the identity aggregator at HU
• Is Bologna coordinator at HU

Harry:
• Has a SWIFT enabled laptop and smartphone
• HU authenticates him
• HU (most of his data) and FU (information regarding his one semester study there) provide his data
• Has an account at the Identity Aggregator at HU
• Has moved to FU
• Has a small amount of money at his HU account

Fiona:
• Has a SWIFT enabled laptop and smartphone
• FU authenticates her
• FU provides her attributes
• Has an account at the identity aggregator at FU
• Has a SWIFT enabled home entertainment system

Tom:
• Has a SWIFT enabled laptop and smartphone
• FU authenticates him
• FU (most of his data) and his telco operator (information regarding his customer relation to the telco operator) provides his attributes
• Has an account at the identity aggregator at the telco operator
• Is a tutor for Prof. Peter’s lecture in the computer science department of FU

Book Store:
• Offers books to students at FU campus
• SWIFT enabled applications

Foreign University Library:
• Contract with FU regarding book-borrowing
• SWIFT enabled terminals
• RFID secured books
• Small fee for all students not belonging to FU

Foreign University cafeteria:
• SWIFT enabled applications
• Ability to filter the daily menu options related to the received preferences
• Ability to send information wireless to the devices of entering people, if they accept the delivery of such messages

Conference Service:
• Offers composed services for conference participants
• SWIFT enabled applications
• Ability to contact several service providers to build a composite package of the services

Telco Operator:
• Federation contract with the European Academic Federation
• Support for SWIFT framework
• Attribute provider ability
• Identity aggregator ability
• Allows its customers to use the operator’s network
• Charges its customers for payment required actions in its network
• May charge its customers for consumption of 3rd party services

Live Match Service Provider:
• Offers football match live stream to its customers
• SWIFT enabled applications
• Ability to charge the customers either directly or indirectly via their telco operator bill.
2.2.4 Scenario Description

In the following paragraphs the actions of the five scenario players are explained in detail to show exactly the interactions with the SWIFT framework and the benefits that can be offered by it.

08:00

At 8:00, Prof. Peter holds a lecture on communication networks, which is visited by Harry, Fiona and Tom. All the four want to be connected with the university’s E-Learning Platform, thus, everyone opens his or her laptop and connects to the university’s Wireless Network. The network access control is configured to allow access only to persons affiliated to the university, e.g., professors, students and roaming students. After the professor and the students have entered their login credentials (Peter and Fiona the one from FU, Harry from HU and Tom from his telco operator), the network access control discovers automatically the identity aggregator from the credentials and receives from them the information, that each of them is affiliated to the university. Therefore, it grants access to the network.

During the initial login to the FU’s network, the players chose their VIDs, i.e., the virtual identity that should be used when being visible on the network as well as on later used applications. This step is important, since several attributes are assigned to a VID, so, the choice of a VID influences the privacy. Fiona and Harry use their normal student VID, but Tom, who is a tutor, chooses that VID that marks him as tutor. Peter, however, uses the VID that marks him as a professor for computer science.

Now, having network access, they try to access to the E-Learning Platform. Although the virtual classroom, they use for the lecture, requires authorization credentials, since only students and professors of computer science are allowed to access, the four can access the classroom directly. The request for their study subject and the authorization is done invisible to them.

After all students and the professor are connected to the university’s E-Learning platform, Peter starts his lecture and the students follow his talk with support from the platform. This step is shown in Figure 1: Lecture Infrastructure.

![Figure 1: Lecture Infrastructure](image-url)
10:00
At the end of the lecture, Prof. Peter mentions, that he has finished a new book about networking. Students of him will get a discount at the local bookstore confirming that they are taking the course, e.g., by allowing their identity aggregator to release the corresponding attribute. Fiona, who is interested in this book, accesses her identity aggregator and changes her privacy policy.

Before Peter closes the lecture finally, he sends new documents for the E-Learning platform to all tutors of his lecture. Tom, who is automatically detected by the platform, receives the documents to be uploaded this afternoon to his virtual classroom on the platform.

Prof. Peter returns to his office and takes care of some formal issues. Because he knows that there are sometimes problems in the accreditation of courses visited by roaming students, he requests the name of the accordant home university from all students on the E-Learning platform. Since Harry has not allowed his identity aggregator to release this attribute, he is now informed by a small message, that someone from FU is requesting this attribute. Harry, who has heard Prof. Peter’s announcement that information about roaming students may be required, allows the release. After Prof. Peter has received the information that someone from HU is visiting his course, he delegates the right to access the documents about his lecture on the FU E-Learning platform to the group Bologna-Coordinators at HU for three days and sends a message to HU informing about the roaming student. At HU, Professor Paul, who is the Bologna-Coordinator of the university and already logged in into the HU platform, receives Prof. Peter’s message. By using the delegated right of accessing Peter’s documents, he is able to browse through all lecture relevant information at FU. Paul examines the documents and decides that Peter’s lecture fulfils the requirements of an HU lecture.

12:00
Prof. Peter, who has a lot to do in the afternoon, decides to have lunch early and visits at 12:00 the university’s cafeteria. When he enters the building, his smartphone, which is still connected to the FU network, sends on requested his SSO token to the Lunch Information SP at the cafeteria. Peter has configured the policy at his identity aggregator to release the attribute that informs about his milk intolerance. Thus, the lunch information SP recommends only those menu options that are free of milk or prepared with only less milk.

Harry, Fiona and Tom are not hungry and meet again on the E-Learning platform, because they want to do homework together. Although they were meanwhile disconnected from the platform, their login is still valid and they do not have the need to login again. Tom uses his tutor privilege to open a virtual classroom for them and after a while Harry and Fiona joined him in the room. The three take advantage of the several benefits the virtual room offers and they finish their work right before they become hungry.

14:00
While the three students have lunch at the university’s cafeteria, Prof. Peter is back for work. Since he has turned off his laptop during lunch, he logs into the university’s network again and connects to the E-Learning platform. He wants to correct the homework the students of his lecture have uploaded and accesses the stored homework documents. Having access to those documents is a right that is bound to the VID of a FU professor. To avoid disadvantages of bad homework, all documents are stored under pseudonyms, Peter cannot resolve. However, he corrects them and leaves the E-Learning platform.

16:00
At 16:00, each of the four main players is doing some work on his or her own.

Peter visits an online conference service, which offers strong support to participants of academic conferences. Since Peter has to visit a conference in the next week to present his new results on a poster, he chooses the service to buy some components of his trip. He logs into the service platform using his professor VID, because he gets discounts as university member. At the conference platform, Peter enters the details of
the conference and uploads the file containing the poster information. The conference service, however, contacts in turn several other service providers to build the offered service to Peter. It searches for the best flight ticket on travel service providers, contacts hotel information portals and looks for print offices near Peter’s location. When all good services are discovered, the composite service provider offers each service in the requestor interface to Peter, who can now, in turn, access those service providers.

After his friends Tom and Fiona have left the virtual classroom, Harry stays in because he realizes that he has already missed one lecture of Peter. Therefore, he accesses the audio stream provider of FU E-Learning platform. Since he is a student of computer science, he has the right to listen to all computer science lectures. Harry finds the one he has missed from Peter and starts listening at his laptop. During listening to the stream, Harry finds out that he has to borrow one of the books Peter has mentioned during the lecture. Since he does not want the audio stream being stopped, he starts his smartphone and handovers the session from his laptop to it. After plugging in his earphones, Harry walks over the FU campus to the FUL, which means, that a network handover took place between different WLAN cells invisible to him. When he arrives at the FUL, he stops the audio stream, looks for the book and brings it to one of the borrowing terminals at FUL, after he has found the needed book. The book borrowing process is SWIFT enabled, which means that the terminal requests a connection to Harry’s smartphone. Harry allows the connection by entering his PIN and the smartphone sends Harry’s authentication information to the terminal. The terminal recognizes Harry as HU student and since only FU students are allowed to borrow books without paying a small fee, it requests Harry to pay the small fee, every roaming student has to pay. Harry chooses federation payment, and the terminal contacts his identity aggregator to start the payment. Harry initializes the payment by entering his Payment PIN and his identity aggregator sends the payment information to the terminal. After having checked the correctness of the received payment statement, the borrowing terminal allows Harry to borrow the book and disables the RFID alarm of the book. When leaving the FUL, Harry starts the audio stream again and continues to listen to the missed lecture audio data.

Fiona decides to use the time without her friends to buy the book, Peter has mentioned during his lecture. Thus, she contacts the online book store available at FU. Since she is still logged into the FU network and her authentication is valid, she accesses the store without the need for logging in again. The online bookstore detects her home address (part of her VID attributes) and the right to use the lecture discount. Therefore, the online book shop offers to send the bought book to her address and to charge her credit card account – a configuration entry from a former session with her. Fiona accepts the charging approach and closes the transaction.

Tom, on the other hand, logs into the FU E-Learning platform using the tutor VID again, since he needs more rights than a common student has. He changes some documents and uploads the new material from Professor Peter to the platform. Furthermore, Tom looks into a question pool and answers questions from other students, but this time, due to preferences and privacy settings, his name won’t be available for the students. Tom is given a pseudonym that he is automatically using when giving his answers.

18:00
At 18:00, while Peter is already at home, Tom closes his laptop and leaves the university. During shutdown of the laptop, his authentication information are transmitted to his smartphone, therefore, he is still authenticated. He realizes that a very important football match takes place in the evening. He is a very enthusiastic football fan and wants to view the match with Harry and Fiona. So, he starts an audio conference application on his smartphone and invites Harry and Fiona for a SIP call conference. Tom and Fiona, both still logged in, too, receive the message containing the conference invitation and agree. When they start the audio conference, Tom asks them, whether they would like to view the match with him. He offers to buy the live stream from a service provider and Fiona points to her home entertainment system, which could be used for viewing the match. However, the three agree on meeting together at Fiona’s room to watch the match on her home entertainment system at 20:00.

20:00
While Harry and Fiona have met already at Fiona’s place, Tom is late. Since he is extremely interested in the match, he accesses the service provider with his smartphone and starts the stream. But this time, Tom wants to use another VID, because his tutor-VID carries a lot of private information, he does not want to submit to
the service provider, now. Therefore, Tom restarts the login, logs into the network after having chosen a more anonymous VID (Telco-Customer-VID). The service provider recognizes him as a telco operator customer and offers a discount, if he agrees on paying the service with his telco bill. Tom agrees and the service provider detects automatically, that Tom’s End Device is not able to handle the full live video stream. Therefore, the service provider starts only an audio stream and Tom walks hurried to Fiona’s room. When he arrives there, he transfers the stream from his mobile smartphone to Fiona’s wired home entertainment system. The service provider detects the change of devices and starts the video stream. Since the new device does not belong to Tom, the service provider asks, if a cost sharing between the involved persons is wanted. Fiona and Tom confirm the request, thus, her credit card and his telco account is charged after the match has ended.
3  Use Cases

This chapter discusses the functionality of a generic IdM & AAA infrastructure by means of a collection of small and self-consistent sets of interactions. By doing this, it provides a basic toolkit of interactions that a generic IdM & AAA infrastructure has to support.

A use case has the following characteristics:

- It describes concrete functionality, which has a specific initiation and that terminates with a definite result.
- It has at least one actor that uses the business functionality.
- It does not describe any details of (possible) implementations (of that use case).

Each use case is structured as follows:

- **Summary**
  Short description of the use case’s functionality

- **Examples**
  Description of the use case examples, if available.

- **Actors**
  List of all actors involved.

- **Preconditions**
  List of prerequisites which have to be fulfilled in order to launch the use case’s sequences.

- **Results**
  List of conditions, which have to be fulfilled after the sequence of interactions terminates.

- **Errors**
  Description of possible error situations, if available.

- **Alternatives**
  Description of alternative sequences of interactions, if available.

- **Remarks**
  Additional comments, if available.

The actors appearing in the following use cases are in general those described in the Definitions on page 9. But in derivation to this it is sometimes not necessary to distinguish between the exact role an end-user is playing, thus we just refer to “end-user”. Similar service provider or network provider are just using other entities in the same way, then the term “provider” is used for both of them.

The use cases are grouped in four categories to provide a more structured overview, independent of their relations regarding preconditions or usage in the scenario in section 2.

### 3.1  Authentication

#### 3.1.1  Face to Face User Identification

**Summary**

The end-user can identify himself to the service provider if he visits an office of the service provider and proves his identity.
Examples
An end-user wants to get network access, so the end-user visits an office of the service provider. Signs the contract and proves his identity through his Identity Card which is issued by the government.

Actors
• End-user
• Service provider
• Identity issuer\(^1\)

Preconditions
None

Results
The end-user is identified, gets his authentication credentials and he may has a contract.

Errors
None

Alternatives
Online user Identification (3.1.2)

Remarks
How valuable the identification is depends on the reputation of the identity issuer.

3.1.2 Online User Identification

Summary
The end-user can identify himself to the service provider and prove his identity online without the need to visit an office of the service provider.

Examples
An end-user wants to get network access so the end-user enters an online platform for registration. The end-user owns an appropriate certificate to prove his identity data (that would also appear on an identity card). He signs the contract with an electronic signature.

Actors
• End-user
• Service provider
• Identity issuer

Preconditions
A valid authentication credential from a trusted authority

Results
The end-user is identified, gets his authentication credentials and may have a contract.

Errors
None

\(^1\) This Identity Issuer might be outside the scope, or network of the SWIFT enabled services. A traditional example is a governmental institution like ID card or driving license. Other examples could be credit cards containing photos of the legitimate user.
3.1.3 Basic Authentication

Summary
The end-user authenticates with the authentication provider in order to access a service or resource of a service provider. The end-user proves its identity by providing authentication credentials to the authentication provider.

Examples
None

Actors
• End-user
• Authentication provider
• Service provider

Preconditions
• The end-user owns valid authentication credentials of the authentication provider.
• The end-user is not already authenticated with the authentication provider.

Results
The end-user is authenticated with the authentication provider and is able to access the service provider.

Errors
The authentication process fails due to invalid authentication credentials.

Alternatives
None

Remarks
None

3.1.4 Group-affiliation-based authentication

Summary
The rights for access to a resource or service might also be granted due to the end-user affiliation to a certain group of users. For that purpose it is sufficient for the end-user to show credibly (e.g. by presenting an appropriate and valid token) that he is a member of this specific group.

Examples
E-learning material is provided for a group of students attending a certain lecture. For getting access to the material, the student just needs to prove to be an attendant of this lecture.

Actors
• End-user
• Service provider
• Authentication provider

**Preconditions**
End-user is member of a specific group, and can somehow prove it.

**Results**
End-user is authenticated as a member of this group because he owns valid credentials to prove being a group member.

**Errors**
Credentials are invalid, (e.g. because they are issued for another end-user or because they are expired) so the end-user could not be recognized as belonging to the group.

**Alternatives**
Individual authentication with an attribute which shows the group membership

**Remarks**
Could be converted to an alternative of the basic authentication

### 3.1.5 Network Authentication

**Summary**
The device of an end-user authenticates with the authentication provider of a network access provider in order to establish a network connection.

**Examples**
Authentication methods of mainstream standards such as SIM-Card-Authentication within GSM/GPRS/UMTS networks, EAP (Extensible Authentication Protocol) within WLAN or RADIUS, Diameter, LDAP and Kerberos within fixed line networks are examples of this use case.

**Actors**
- Device
- Service provider
- Authentication provider

**Preconditions**
- The required authentication credentials are valid and “known” to the device (by means of pre-configured).

**Results**
The network connection is established successfully.

**Errors**
The authentication fails due to insufficient authentication credentials.

**Alternatives**
None

**Remarks**
None
3.1.6 Authentication Context Exchange

Summary
The process of authentication creates an authentication context within the authentication provider, which describes the circumstances of the authentication (e.g. authentication method, authentication quality, timestamp of authentication, etc.). The authentication context can be exchanged by request of other providers between the authentication provider and the providers (e.g. service providers, network providers, or other authorization provider).

Examples
Single Sign On within a circle of trust based on the exchange and evaluation of authentication contexts is an example of this use case.

Actors
- Authentication provider
- Provider/other authorization provider

Preconditions
- The end-user is already authenticated with the authentication provider.
- The authentication provider has already created the authentication context.

Results
The provider is able to access the authentication context created by an authentication provider. The provider is able to judge any further end-user’s interaction by evaluation of the authentication context.

Errors
The end-user disallowed the exchange of its authentication context.

Alternatives
Re-Authentication with the provider or other authorization provider (3.1.8)

Remarks
None

3.1.7 3rd Party Authentication

Summary
The provider uses the authentication provider of another 3rd party domain in order to execute some or all authentication request within its own domain. Therefore all incoming authentication requests of users are forwarded to the 3rd party domain’s authentication provider.

Examples
The usage of authentication providers, which provide specialized authentication methods (e.g. voice recognition), is an example of the use case.

Actors
- End-user
- Provider
- Authentication provider
- (3rd Party) authentication provider

Preconditions
• The provider’s and the 3rd party authentication provider’s domains have a trusted relationship between each other.

**Results**
The end-user’s authentication request is successfully forwarded to and accomplished by the 3rd Party authentication provider.

**Errors**
The redirection of the authentication request fails due to absence of a valid trust relationship between the provider and the 3rd party authentication provider.

**Alternatives**
None

**Remarks**
None

### 3.1.8 Re-Authentication in Foreign Networks

**Summary**
The enhancement of an existing service session results in a request for re-authentication. The end-user has to re-authenticate with the authentication provider of the service provider of the existing session or with the authentication provider of a new service provider, which enhances the existing service session with new capabilities. The reason for re-authentication may be either that the new service provider stems from a foreign authentication domain or that Single Sign On (SSO) is not available for other reasons.

**Examples**
A typical example of re-authentication can be found in the current heterogeneous networks environment within the domain of a network provider. When the end-user moves from one into another access network of different type (e.g. from GSM/UMTS into WLAN), her/his device needs to re-authenticate to the networks even though it stays in the domain of a network operator.

**Actors**
- End-user
- Authentication provider (of domain A and B)
- Service provider (of domain A and B)

**Preconditions**
- The end-user is already authenticated with the authentication provider of domain A.
- The end-user uses already the service provider of domain A.
- The end-user owns the appropriate authentication credential for the required re-authentication with the authentication provider of domain B.

**Results**
The re-authentication of the end-user with the authentication provider of domain B was successful and the end-user uses the services of both domains A and B within a shared session.

**Errors**
The re-authentication with the authentication provider of domain B fails due to insufficiency of the authentication credentials.

**Alternatives**
None

Remarks
Through the involvement of different service providers complicated accounting and charging actions may occur.

3.1.9 Service Authentication

Summary
The service provider authenticates itself to the end-user by means of the presentation of authentication credentials.

Examples
The establishment of a secure SSL web connection based on X.509 SSL server-certificates of the service provider is an example of the use case.

Actors
- End-user
- Authentication provider
- Service provider

Preconditions
- Service provider owns an authentication credential of the authentication provider or is able to get one on-the-fly.
- The end-user has to be able to evaluate the authentication credentials presented by the service provider.

Results
The end-user has authenticated the service provider.

Errors
The authentication of the service provider fails due to insufficient authentication credentials.
The authentication of the service provider fails since the end-user is not able to evaluate the authentication credentials.

Alternatives
None

Remarks
None

3.2 Authorization

3.2.1 Authorization by Policy

Summary
The end-user wants to use a service of a service provider that is access restricted by policies. The access to the service is granted only by the authorization entity of the service provider, when specific policies of the service provider and the end-user are satisfied by means of end-user’s attributes are fitting to policies’ specific rules.
Examples
The end-user gets only access to the foreign network when the attribute exchange is possible, allowed by the end-user and expressed through the end-user’s network policies.

Ongoing check of credit balance during an existing service session is an example of an authorization decision with complex policies. When the balance drops under some specific threshold value, the authorization decision for the running session may change and access to the service may be denied by the authorization provider.

Actors
- End-user
- Authorization provider
- Attribute provider
- Service provider

Preconditions
Some policies have to be specified and known and the specific entities.

Results
The end-user is allowed to access the service provider’s services.

Errors
The authorization provider can not decide on the authorization request, because of conflicting policies, a deadlock in the inference process, or is unable to get attributes required to evaluate some policies.

Alternatives
None

Remarks
Policies can be distributed, i.e. there may be policies of the service provider and policies of the end-user. Therefore, a “negotiation concept” is needed, which is able to resolve conflicts within a set of distributed policies.

3.2.2 Re-Authentication for Authorization

Summary
The end-user chooses a service of a service provider, which is not included within the existing usage contract and may cause extra charges to the end-user. The service provider’s authorization provider requests a re-authentication of the end-user by its authentication provider in order to avoid accidentally usage or unauthorized usage of the service. The re-authentication acts as a kind of acknowledgment, which authorizes the end-user to use the service.

Examples
The end-user is already logged on to the network but the library service needs a special verification so the end-user is re-authenticated.

Actors
- End-user
- Authorization provider
- Authentication provider
- Service provider
Preconditions

- The end-user is already authenticated and authorized to use the services of the service provider.
- The end-user owns the appropriate authentication credential for the required re-authentication, if a different authentication than before is required.

Results

The end-user is allowed to access the service provider’s additional services.

Errors

The re-authentication fails and access to the additional service is denied.

Alternatives

None

Remarks

The re-authentication is not required to be stronger or of better quality than the first authentication.

3.2.3 Authorization by Attribute Verification

Summary

The end-user wants to use a service of a service provider that is access restricted. The service provider’s authorization provider requires specific attributes of the end-user in order to decide on the authorization request. The attributes are provided by an Attribute provider of the end-user. Afterwards, they are evaluated by the authorization provider according to specified business rules.

Examples

The authorization provider grants access to the service when the end-user attributes proves the end-user is member of a certain end-user group.

The evaluation of the end-user’s age considering the corresponding attribute is an example of the use case.

Actors

- End-user
- Authorization provider
- Attribute provider
- Service provider

Preconditions

- The authorization provider is able to access all attributes required for the authorization decision.

Results

The end-user is allowed to access the service provider’s services.

Errors

The authorization provider denies access to the service, because at least one attribute does not satisfy the policy rule.

Alternatives

In case of negative authorization decision, the authorization provider may have the flexibility either to use an additional Attribute provider or to request another attribute. This depends on the actual business rules of the authorization provider.

Remarks
3.2.4 Deduction of Access Policies

Summary
An end-user requests access to a specific resource, the local policy decision point could not decide on the request, instead it sends out another policy request - which may contain different subject, resource and action information - to a second policy decision point. Depending on the result of the second PDP the first PDP access or denies the request of the end-user.

The first PDP may send out more than one request, either parallel or sequential. The second PDP may as well send out deduction requests on its own.

Examples
An end-user wants to access an internal web service via an arbitrary device registered at a public access point of his company. It is assumed that the policies related to this end-user account allow an access to the web service. In order to access the service, the firewall between the public access point and the server has to be opened for his device. We assume that a policy is specifying the access of the end-user to a web service, and another is used for deducing the access of the end-user’s terminal through a firewall to a dedicated server.

Actors
• End-user
• Provider
• 1st Authorization provider
• 2nd Authorization provider

Preconditions
• Policies specified and available at 1st and 2nd authorization provider
• Trust relation ship between authorization provider to exchange decisions
• Secure communication channel between authorization providers

Results
Decision given to the provider

Errors
Circular or non determination in the recursive calls of the authorization providers.

Alternatives

Remarks

3.3 Identity Management

3.3.1 Creation of a virtual identity for service usage

Summary
A user can create a virtual identity, or user profile, based on its current existing digital identities in an identity aggregator. This process includes the definition of which identities are going to be aggregated, which attributes from each identity are included, the definition of specific privacy policies and the selected authentication provider for the virtual identity. Once the virtual identity is created, the user can use a virtual identifier or VID to reference it.

Examples
A user wants to create a new virtual identity for making blog entries pseudonymous, revealing as less personal information as possible. From the blog provider (service provider) he knows that it is sufficient to present a valid e-mail address. Therefore, he creates a virtual identity with a pseudonym and his e-mail address attribute, which has already been confirmed by an attribute provider.

Actors
• User
• Identity aggregator

Preconditions
• The user is registered at an identity aggregator.
• The user knows which claims/attributes are necessary for the intended application of the new virtual identity.
• Necessary attributes issued by an Attribute Provider are present.

Results
User has created a new virtual identity that can be used with SWIFT-enabled services.

Errors
None

Alternatives
None

Remarks
None

3.3.2 Selection of a virtual identity for service usage

Summary
The end-user could utilize different virtual (or digital) identity for each service usage, even with the same service provider. This allows for increased privacy and prevents usage pattern data collection. To use a service an end-user first contacts the service provider anonymously and "asks" the service which attributes will be necessary for access. Afterwards, the end-user selects an appropriate virtual identity or creates a new one. The exact procedure for selecting a virtual identity depends on the implementation of the identity aggregator.

Examples
A web service contains a logging of VIDs having accessed this service, but users do not want to appear with their VIDs as more or less frequent users of this web service.

Actors
• End-user
• Service provider
• Identity aggregator
Preconditions
The end-user has at least one VID established at the identity aggregator

Results
When accessing services the end-user appears with the selected virtual identity.

Errors
None

Alternatives
None

Remarks
None

3.3.3 Implicit Identity selection

Summary
The identity provider can use implicitly a virtual identity of the end-user for a certain service provider. This can be done by policies or by tracing end-user behaviour.

Examples
An end-user surfs anonymously in the web and wants to use an email account. The identity provider knows it’s in the morning and from the location information that the end-user is at home, so the identity credentials for a certain identity are used for that account.

Actors
• End-user
• Identity aggregator
• Service provider

Preconditions
• The end-user is authenticated to the identity aggregator.
• The identity provider has a policy for this situation.
• The service provider connects the identity provider and defines which service is required.

Results
The service usage is possible without further interaction and with the desired virtual identity.

Errors
No appropriate policy is available.

Alternatives
None

Remarks
None

3.3.4 Selection of Roles

Summary
The end-user is able to select specific (business) roles from a set of roles. The role definitions are provided by some kind of administrator who decides which roles are necessary in a given context. The selection of a specific role by the end-user controls reachability, access rights and attribute transfer of the end-user. The predefined role can be taken by several users.

Examples

The end-user is student and works for the university. Additionally to the normal role as “student”, the end-user is a tutor. Therefore the end-user selects the role as “tutor”, which gives him special rights.

Actors

- End-user
- Identity provider
- Service provider

Preconditions

- All abstract roles required for a specific context are stored in the identity provider.
- The end-user has a valid VID at the identity provider.
- The end-user is authenticated with the identity provider.
- The end-user was assigned to take specific roles by an administrator.

Results

- The end-user has selected one or more transferable roles.
- Reachability, access rights and attribute transfer are managed with respect to the selected roles.

Errors

None

Alternatives

None

Remarks

None

3.3.5 Setting up and modifying end-user profiles and policies

Summary

The SWIFT Framework allows the end-user to dynamically manage his profiles at any time via the identity aggregator. This includes modification of end-user privacy settings. All settings concerning the privacy of the end-user will have proper default values. Nevertheless, the end-user should be given the option to change these settings in order to grant services or other users to access parts of his profile. Users should have a simple mechanism to both set and realize the consequence of policies; even when these policies are set by an agent on behalf of the end-user.

Examples

A user wants to give access to some personal data to one specific service. By modifying the privacy settings in the identity aggregator he can deblock the access e.g. by adding this very service to the white list for certain personal information.

Actors

- End-user
- Identity aggregator
Preconditions
End-user is properly authenticated as the owner of the corresponding profile.

Results
Services may be used according to the newly set up resp. modified end-user profiles and policies.

Errors
End-user was not successfully recognized as eligible for setting up resp. modifying profiles and policies.

Alternatives
None

Remarks
None

3.3.6 Delegation of usage rights

Summary
If an end-user has the rights to use certain services, he may have the intention to also allow other users to use the same services. When delegating usage rights, the end-user exactly determines the corresponding usage policies.

Examples
Parents may allow their children to also use video on demand services, but under certain restrictions.

Actors
- End-user
- Other end-user (who receives the delegation)

Preconditions
- The end-user has successfully authenticated with the authentication provider and holds the appropriate usage rights for the corresponding services.
- An identifier of the end-user who receives the delegation is known.

Results
The other users now own the usage rights as intended by the original end-user under consideration of the specified usage policies.

Errors
End-user is not eligible to delegate rights to other users.

Alternatives
New users may be added to an end-user group and may be granted usage rights according to group-affiliation-based authentication.

Remarks
None

3.3.7 VID change

Summary
It should be possible for an end-user to use different VID according to the profile he wants use at every time. To do this, the end-user should be able to switch from one VID to another.

**Examples**

An example scenario for this use case would be a person who is surfing the net using a VID that gives permission to access to messaging services and comment on blogs. Suddenly, the end-user wishes to make a purchase and wants to make use of another of his VIDs that enables him to make charges to his credit card.

**Actors**

- End-user
- Identity aggregator

**Preconditions**

The end-user has been successfully authenticated toward the identity provider.

**Results**

The VID chosen by the end-user is now presented to a service provider on request.

**Errors**

None

**Alternatives**

Selection of a virtual identity for service usage.

**Remarks**

None

3.3.8 **Session handover**

**Summary**

Aim of a session handover is to move a running session (e.g. voice, video ...) to another device without interrupting the session. With a session handover the different characteristics of the target device have to be taken into account, like bandwidth, processing power, screen resolution etc. An end-user might initiate a session handover for various reasons including technical (better resolution), financial (cheaper rate), and convenience (easier handling) or just for being able to switch to another terminal for any reason.

**Examples**

An end-user is viewing a video on his home entertainment system and wants to continue viewing it on a mobile device when moving away.

**Actors**

- End-user
- Service provider

**Preconditions**

A session has already been established with some service provider.

**Results**

Session continues on the other device without interruption and without any additional authentication procedure to be performed.

**Errors**

End-user's authentication status gets lost during session transfer to other device.

**Alternatives**

Re-establishing the session using the other device.
3.3.9 Pseudomized Communication

Summary
Two users know each other only through a pseudonym. If Alice wants to contact Bob (e.g. by IMS/Sip) she enters the Bob pseudonym. A dedicated service resolves this pseudonym (without revealing it to Alice) through the identity aggregator. Additionally Alice real address is replaced by a pseudonym she wanted to use toward Bob.

The real identifiers of the communication peers are completely replaced by the pseudonyms in all messages send to the peer.

Examples
In a chat room the users don’t want to reveal there real identity but they want the possibility to address specific members.

Actors
- 2 users
- Service provider
- One or two Identity Aggregators

Preconditions
- Both users are logged on to a Service who supports Pseudonyms.

Results
The identifiers used in the communication process are replaced by pseudonyms.

Errors
One or both users have not enabled the usage of pseudonyms.

Alternatives
- Only one of the communication partners is hidden by a pseudonym.
- One of the communication partners is a service.

Remarks
None

3.3.10 End-user registration at Identity Aggregator

Summary
Before an end-user can create a virtual identity, or user profile, based on its current existing digital identities he must register at an identity aggregator. For this purpose the end-user must close a contract with the identity aggregator. Depending on the operator of the identity aggregator the registration may be included in other contracts with this operator.

Examples
The end-user has chosen his mobile phone operator to be his identity aggregator. If not already included in his mobile phone contract the end-user has to register by ratifying a contract which entails accepting terms and conditions.
3.3.11 End-user registration at the Attribute Provider

Summary
An end-user has to register with at least one attribute provider in order to use verified attributes or certified claims in an authentication process. The registration process entails an attribute-dependent procedure for verifying the specific claim.

Examples
An end-user intends to make shopping in various online-shops. In order to avoid entering his address in every shop’s registration system he registers at an attribute provider who is willing to verify his address and provide it as an attribute.

Actors
• End-user
• Attribute provider

Preconditions
None

Results
The attribute provider issues the requested attribute, either immediately as a certified token or later on demand.

Errors
If the attribute provider is unable to verify the claim issuing the attribute will fail.

Alternatives
None

Remarks
None
Under certain conditions, a stakeholder may play both the role of an identity aggregator and the role of an Attribute provider, i.e. the attribute service may be integrated. This gives the end-user the option to directly choose the Attribute provider as his identity aggregator for registration.

3.3.12 Multi-Layer Single Sign On

Summary

Each service provider usage requires prior establishment of a network connection between the device and the network provider. Therefore, the device authenticates with the authentication provider of the network provider’s identity provider. Afterwards, the end-user selects and uses a service of a service provider without any additional authentication with the service provider’s authentication provider.

Examples:

Internet service providers (ISPs) offer optional configurations, that the network authentication can be used for web authentication.

Mobile services can be used by an end-user with a mobile device without further authentication, because the mobile device has authenticated with the mobile network based on SIM or UICC cards.

Actors

- End-user
- Device
- Authentication provider (of network provider)
- Service provider

Preconditions

- The required authentication credentials are known to the end-user’s device.
- The service provider is able to re-use the end-user’s authentication with the network provider by means of sharing the same authentication provider or federation of Identities.

Results

The network connection is established and the service provider’s service can be used without any additional authentication.

Errors

The authentication fails due to invalid authentication credentials.

Alternatives

None

Remarks

In fact, this use case authenticates the device more than the end-user.

3.3.13 Reverse Multi-Layer Single Sign On

Summary

Established authentications on the service layer can be used for authentications with a network provider, when network changes are necessary. The end-user authenticates with a service provider’s authentication provider. For some reasons, the end-user’s device has to switch the underlying network connection. The access to the new network does not need any additional authentication with the new network provider’s authentication provider, because the authentication with the service provider’s authentication provider is reused.
Examples
End-user is on a campus that are roaming via wireless LAN without interruption of existing service session are examples for the use case.

Actors
- End-user
- Device
- Authentication provider (of the network provider)
- Service provider

Preconditions
- The network provider’s authentication provider is able to re-use the end-user’s authentication with the service provider by means of sharing the same authentication provider or federation of identities.

Results
A new network connection is established without any additional authentication or preconfigured authentication credentials in the end-user’s device for each new network. Service usage is not interrupted during the switching of networks.

Errors
None

Alternatives
None

Remarks
None

3.3.14 Anonymous Attribute Transfer

Summary
A frequently visited service provider requests specific attributes of an end-user in order to provide a personalized service without really knowing the end-user’s identity. The service provider uses an opaque handle in order to request the attributes instead of using the identity and receives the attributes if the end-user configured the service policies on his identity provider.

Examples
A service provider offering horoscopes within a Circle of Trust (CoT) requests the date of birth and the place of birth from the attribute provider hosting the end-user’s attribute with out knowing the real identity of the end-user.

Actors
- End-user
- Attribute provider
- Service provider
- Identity aggregator

Preconditions
- The end-user is authenticated with an identity aggregator.
- The attribute provider has access to the requested attributes.
• The end-user has provided an access control policy that allows access to the attributes without prompting the end-user.

Results
The service provider submits a personalized service to the end-user without knowing his real identity.

Errors
None

Alternatives
None

Remarks
None

3.3.15 Provision of Community Services

Summary
The identity provider provides community services to users and service providers. Users are able to set up and maintain their own groups of users with group based communication and group wide access to attributes of all users. Service providers are able to provide specialized services for groups of users.

Examples
Service providers offering group oriented games such as paper chase are examples of this use case. Groups of users forming a community about a common interest (e.g. cooking) with support for group based communication are other examples.

Actors
• end-user
• Identity provider
• Attribute provider
• Service provider

Preconditions
• The users of a group of users have identities on an identity provider.
• The users of a group of users have provided access control policies for their attribute provider that allows mutual group wide attribute access.

Results
The users and the service providers are using the identity provider’s services for groups of users.

Errors
None

Alternatives
None

Remarks
None
3.3.16 Event based policy resolution

Summary
A service provider or service agent triggers an event which is evaluated by the identity aggregator. Dependent on the policy of the end-user or group certain actions take place.

Examples
A facility management system detects an unusual event and sent this to the identity aggregator. Through the under laying policies the identity aggregator sends a message to a certain end-user from which he knows where he is and what kind of device he currently uses.

Actors
• End-user
• Identity aggregator
• Service/Agent

Preconditions
• The end-user is authenticated to his identity aggregator and has a valid VID.
• On the service/agent the address/name of the identity aggregator is configured.
• The identity aggregator has an appropriate policy.

Results
The end-user will be notified about the event.

Errors
None

Alternatives
None

Remarks
None

3.4 Accounting and Logging

3.4.1 Basic Accounting

Summary
The service provider transfers usage data stemming from the service usage of an end-user to an accounting provider.

Examples
A network service transfers usage data of the network to the accounting provider.

Actors
• End-user
• Service provider
• Accounting provider

Preconditions
• The end-user is entitled to use the service provider’s services.
• The service provider has a valid agreement with the accounting provider in order to aggregate usage data.

Results
The usage data was transferred to the accounting provider successfully.

Errors
Transmission of usage data from the service provider to the accounting provider is interrupted (e.g. due to network connection errors).

Alternatives
None

Remarks
None

3.4.2 Anonymous charging of service usage

Summary
After using one or more services an end-user will most likely be charged for it in case he has used commercial services. It is possible for an end-user to employ different digital identities with different services (and even with the same service). It is important that no one than the identity aggregator is able to link the different service utilisations. In order to charge for services the identity aggregator accumulates the different service fees and bills the end-user for them with a combined bill.

Examples
Different content on demand services are used for different purposes, but none of the service providers may get to know that the end-user also has a contract with another one.

Actors
• End-user
• Different service providers
• Different charging providers
• Identity aggregator

Preconditions
Metering functions worked properly for each individual service using the different digital identities.

Results
Identity aggregator owns a combined bill containing the fees for all really used services.

Errors
None

Alternatives
None

Remarks
None
3.4.3 Changing of Service Quality and Charging

Summary
If an end-user desires a higher or lower quality of service which is combined with a changing fee, mechanisms must exist to notify the service for higher service quality as well as the end-user for changing charging fee.

Examples
An end-user views a video stream on his TV set and wants to move the last part on his PDA because he has to leave. On the PDA he doesn’t need a high resolution so his device signals to the service provider to change to a lower resolution. The service provider signals to the end-user changed charging information.

Actors
- End-user
- Service provider

Preconditions
None

Results
The end-user gets the desired quality of service and the charging information.

Errors
None

Alternatives
None

Remarks
None

3.5 Access

3.5.1 IdP-initiated service access

Summary
A user can access his identity aggregator to authenticate himself with a VID. After the authentication, he can access the different services offered by means of the aggregator.

Examples
An identity aggregator can establish several agreements with different hotel booking services. Therefore, when the user access the identity aggregator, he can see a set of links that allow him to access directly the hotel booking web pages, without needing to identify again.

Actors
- Identity Aggregator
- End-user
- Service Provider

Preconditions
The user owns a User Profile, identified by means of a VID.
Results
The user gets access to the service

Errors
None

Alternatives
None

Remarks
The "basic authentication" use case is part of this use case.

3.5.2 SP-initiated service access

Summary
The user requests access to some service provider by means of its VID. Then, based on the VID, the SP redirects the user to its identity aggregator to be authenticated. After this process, he is redirected again to the service provider, where the requested service can be provided.

Examples
The user can access some hotel booking web page without previously being authenticated. Then, the service provider redirects the user to the identity aggregator to be authenticated. After the authentication is carried out, the user can make a reservation.

Actors
• End-user
• Service Provider
• Identity Aggregator.

Preconditions
The user owns a user profile, identified by means of a VID, which allows him to access to the specific service.

Results
The user gets access to the service.

Errors
None

Alternatives
None

Remarks
The "basic authentication" use case is part of this use case.

3.5.3 Access to Composite Provider

Summary
The end-user can access to a composite service provider, which is a special kind of provider that composes services from other service providers and offers end-users a unified interface to them.

Examples
An example scenario for this use case would be a financial composite service that summarizes services and financial information from different bank accounts.

**Actors**
- End-user
- Service provider acting as a composite provider
- Different service providers

**Preconditions**
None

**Results**
All services are accessible via one unique interface.

**Errors**
None

**Alternatives**
None

**Remarks**
None

### 3.5.4 ID-supported network handover

**Summary**
If the network operator of the source as well as target network allow for an ID-supported handover, the roaming end-user can use a digital identity to authenticate with the target network. After that, he is able to use the same services in the same way as after authentication with the source network.

**Examples**
An end-user moves with his car from one country to another and change thereby the network without interruption of the video stream for the children's entertain program.

**Actors**
- End-user
- 2 Network providers

**Preconditions**
Source and target network provider have a trusted relationship between each other.

**Results**
End-user is authenticated with the target network and is able to use the same services as in the source network.

**Errors**
Digital identity was not recognized correctly by the target network.

**Alternatives**
None

**Remarks**
None
4 Business Model

In this section the initial business models based on the scenarios described in section 2 are discussed.

In the next subsections, an analysis on the current market, possible target groups as well as different business models gained through the scenarios are discussed in detail.

4.1 Business Eco System

This section describes properties of the SWIFT project business ecosystem.

4.1.1 Market Analysis

Because of the growth in the legacy network markets is ebbing fast, the traditional network service providers must prepare growth plans that transform their offerings via the scope to offer converged solutions, to provide service in non-traditional sectors and to enter and win in emerging markets, whose profile is very different from more-mature regions.

One of these possibilities is to deploy and enlarge the identity and access management market.

Market data are given for "identity and access management" as a whole. According to the definition of [3] this is equivalent to the market for an

- Authentication Management and
- Identity and Attribute Management and
- Authorisation Management and Access/Usage Control and Monitoring

The market volume for identity and access management will rise from over 4.5 billion euro to more than 6.7 billion euro in 2012 (according to Gartner's market report for IT Services 2008: Gartner Telekom Dataquest, 2008,) as shown in Figure 2. This market is dominated by the USA with a market share of about 60% in 2008 with slow decline to about 58% in 2012 (expected market volume in America more than 4.5 billion € in 2012).

![Figure 2: Identity and access management market volume [1]](image-url)
While this market has a moderate growth of about 5% CAGR\(^2\) in North America and Western Europe (expected market volume in 2012 about 1.4 billion €) the CAGR in central Eastern Europe (expected market volume in 2012 about 38 million €) and Middle East Africa (expected market volume in 2012 about 46 million €) is more than double.

![Figure 3: Identity and access management market CAGR [1]](image)

With their extensive customer database, enlarged by the identity and attribute management, carriers could also generate revenue streams in creating adopted services or deliver relevant advertisement through their multiple channels (SMS, MMS, email, IPTV, …). Mobile advertisement market alone will be worth over 8 billion euro by 2011 [1].

4.1.2 Target Group Analysis

According to the SWIFT-scenarios there are four target groups to be named:

- End-user
- Network Operator / university
- Semi-public network operators (like universities)
- (3rd party) service provider

We will investigate the potential advantages of a SWIFT environment for each of these groups separately.

4.1.2.1 End-User

By 2008 there are about 1.5 billion Internet users, which may become possible SWIFT-users, steadily growing with about 20% CAGR in 2008. That means about 22% of the world's population is using the Internet with strong distinctions in the penetration, which varies from about 5% to more than 70% of the population as illustrated in Table 1. They all may benefit from SWIFT.

\(^2\) Compound Annual Growth Rate
### Table 1: Internet usage (Source [2])

<table>
<thead>
<tr>
<th>World Regions</th>
<th>Population (2008 Est.)</th>
<th>Internet Users, Jul 2008</th>
<th>% Population (Penetration)</th>
<th>Usage % of World</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>955,206,348</td>
<td>51,065,630</td>
<td>5.3 %</td>
<td>3.5 %</td>
</tr>
<tr>
<td>Asia</td>
<td>3,776,181,949</td>
<td>578,538,257</td>
<td>15.3 %</td>
<td>39.5 %</td>
</tr>
<tr>
<td>Europe</td>
<td>800,401,065</td>
<td>384,633,765</td>
<td>48.1 %</td>
<td>26.3 %</td>
</tr>
<tr>
<td>Middle East</td>
<td>197,090,443</td>
<td>41,939,200</td>
<td>21.3 %</td>
<td>2.9 %</td>
</tr>
<tr>
<td>North America</td>
<td>337,167,248</td>
<td>248,241,969</td>
<td>73.6 %</td>
<td>17.0 %</td>
</tr>
<tr>
<td>Latin America/Caribbean</td>
<td>576,091,673</td>
<td>139,009,209</td>
<td>24.1 %</td>
<td>9.5 %</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>33,981,562</td>
<td>20,204,331</td>
<td>59.5 %</td>
<td>1.4 %</td>
</tr>
<tr>
<td><strong>WORLD TOTAL</strong></td>
<td><strong>6,676,120,288</strong></td>
<td><strong>1,463,632,361</strong></td>
<td><strong>21.9 %</strong></td>
<td><strong>100.0 %</strong></td>
</tr>
</tbody>
</table>

Within Europe the internet user penetration varies from below 20% (Vatican City State, Serbia, Moldova, Albania) to more than 85% (Norway, Netherlands).

### 4.1.2.2 Network Operators / Universities

New quadruple play offers will lead to a reconfiguration of the telecommunications companies. This includes:
- vertical separation into sales, services and network companies as well as a
- horizontal integration of fixed-, mobile- and Internet service –provision (convergence).

Network service provision will go along with increased co-operation with content and media suppliers. These companies will compete in saturated 'performing' markets with a low-price level and advanced technology. It is to be assumed that also less advanced markets will reach this status in time.

Competition in the field of identity and attribute management will take place not only among network providers but also with other possible trusted authentication providers.

### 4.1.2.3 (3rd party) Service Provider

Service providers compete in a steadily growing market. For e-commerce alone the market will grow from about 400 billion $ to more than a 1 trillion $ in 2012.

To partake in growth, the service providers will create new/enhanced services and foremost adopt their services to their customers' preferences. Knowledge of the customers attributes will be a key-factor in service creation. Bundled-convergent services and cross-selling will be widespread. This will include advertisement, product placement and sponsorship.

The service provision growth will be done by service enhancement, but also by service enlargement from both sides, the former pure service provider and the network operator and of course by partnering.

### 4.2 Business Models from SWIFT Scenarios

Concerning SWIFT Scenarios the defined roles as described in section “Definitions” will be marked in the figures as follows:
Identified Roles

- User (home, roaming, single, group)
- Super User
- (Service) Subscriber
- Attribute Authority/Provider
- Identity Manager/Aggregator
- Authentication Provider
- Service Provider
- 3rd Party Service Provider
- Temporary Identity Provider*

* Session storage of PDP-function

---

**Figure 4 Symbols for Roles**

**Figure 5: Relationship between Roles**

**Figure 6: Elements of the illustrations**

For the participants in the scenarios this will lead to a possible attribute allocation illustrated in Figure 7.
In Figure 7, the illustration of a service delivered and the concerning payments as used in the description of the scenarios business models is included, too.

In this example a roaming user, connected to the foreign network, is using a service (1) provided by a 3rd-party service provider, marked with the "SP"-sign, also connected to the foreign network. This is described by a red arrow from the service provider to the user marked with a (1) mentioning the provision this specific service.

The payment for this service is done by the payment service of the user's home network operator account, marked by the "SP"-sign, a server-drawing and if useful for clarification a written specification, eg payment service. Therefore a green arrow with a € symbol and a (2) is placed in the illustration from the payment service to the service provider. The payment (3) from the home network operator to the foreign network operator because of the usage of the foreign network by the user (home network operator subscriber) is illustrated by another green arrow marked with a “3” and again a € symbol. Due to the payment (4), marked equally, the user balance his account on the home network operator.

Basic fees not depending on the usage of a specific service provision, e.g. basic fee for network access, are marked by arrows not ending/starting at the network operator's payment service symbol, like in figure 7, because of clarity reasons of the illustration.

### 4.2.1 Business Model University Scenario

For the defined university scenario there are different business opportunities. There are some business opportunities according to the activities at the university campus and others belonging to other activities of the students/professors.
Figure 8: University scenario business

Description:

As shown in University scenario business, the students Fiona, Harry and Tom are using the university systems, e.g. the e-learning system at the foreign university (1). Therefore, they are paying the tuition fee to the FU/HU (2) whereby Tom’s payment – who has his account on telco operator – is performed via the Telco Network Operator. Using the university systems for their work scope, determined by their attributes, is free of charge for the professors and tutors.

The identity service of the home university for Harry and the telco operator for Tom are free of charge for the federated SWIFT-organisations respectively covered by the subscriber's monthly fee to their identity aggregator (3).
Figure 9: University scenario Prof. Peter's business

The Bologna-Coordination between the federated FU and HU is free of charge (4).

The menu options notification for Prof. Peter are part of the cafeteria services, including the attribute adjustment (5), covered by the FU arrangements. When he is using the conference-participation service (6) over the telco network, he is using his credit card (7). This account he has to balance afterwards (8). The usage of the telco network is covered by his telco flat rate access (9).

Figure 10: University scenario book business
Using the federation payment service from his HU (11), Harry is borrowing a book from the FU-library (10). Student Fiona is buying a book at the online-bookstore collaborating with the FU (12). To get the discount as a student of Prof. Peter's lecture, she is changing the privacy policy at her identity aggregator (13) to enable the check (14) of this attribute for the book store. The attribute exchange is free of charge for service providers directly connected to the FU network. Fiona is paying with her credit card (15). This account she is balancing monthly (16).

For arranging the appointment concerning the evening football match Tom starts an audio-conference (17) using his telco's communication service. The football-match is streamed to Tom's smartphone and than handed over to Fiona’s TV-system (18). Paying is done by Fiona, credit card, and Tom, telco payment service, for what he with his attribute "telco costumer" is getting a discount (19).

Additional revenues may be generated by expanding existing services or creating new services using the customers attributes for customization.

4.2.2 Business Model Telco Scenario

For the defined telco scenarios the business opportunities are described separately.

4.2.2.1 Analysis of John’s day

John as the family father is paying the monthly bill for his family's telco account (1) (c.f. Figure 12). He is using a news and podcast service, which is customized according to his attributes (2). Paying is done by the telco's payment service (3) not only for this service, but also for the public transport ticket service (4) he is using on his way to work (5).
As an employee the use of his business network and services (6) is free of charge for John (c.f. Figure 13). For a business lunch he is using a restaurant service, taking into account the preferences and the location of the participants (7). He is paying via his business payment account (8). The communication service of John's telco network operator does the necessary call-screening to connect the urgent private call (9) during his lunch.

On his way to the evening event he is using the online music service (10) (c.f. Figure 14). Paying for this service is divided into 3 parts. The online music service is payed by John’s telco payment service (11) During his stay in the lounge, he still uses the online music services, which partially pays for the network access in the lounge (12). The remaining payment is taken by John’s payment service. (13).
The cinema tickets are delivered online by the cinema service (14) and paid by his credit card (15). His credit card account John is balancing monthly (16).

4.2.2.2 Analysis of Karin’s day

Karin starts the day with checking recipes of her cooking community service (1) automatically adjusted with their food attributes, their food supplies (RFID-Service – 2) and the offerings of her food discounter (3). With her news and advertisement service customized based on her profile she is informed about a new audio book (4), while checking her emails (5). Payment for these services is done by the family's telco account (6).

The audio service including the audio-book shopping during Karin's way to work is handled by her media service provider (7), paid by the family's telco account (8), too. (Splitting of payment with another telco network operator is shown in John's afternoon activities).

Figure 14: Telco scenario John afternoon business

Figure 15: Telco scenario Karin business in the morning
The facility service of the home network is warning to verify the home energy consumption and shuts down the TV-systems on Karin's demand (9). Also she sets the PVR of their entertainment service to record her favourite TV (10).

At work Karin is using the automatic business welcome and timetable service to start her work (c.f. Figure 16). She is using the business meeting service to prepare an ad-hoc meeting (11). As an employee of the company, these services are free of charge to her.

The restaurant service Karin is using for lunch is offering the menu in her preferred language (12) on her PDA according to her attributes. Her restaurant account for her consumption, she balances by the family telco account (13).

After work Karin has to arrange a social event. Therefore she is using the project and event service (14) and the communication (audio-conference) service (15) of their telco network operator. The usage of these services is included in their monthly telco bill.

For updating the evening event with John Karin is using their telco's communication service (16), so she won’t be bothered by something not important.

4.3 Business opportunities

According to the defined SWIFT scenarios there are some business opportunities for the scenario stakeholders.

Network operator / university:
- Network services – providing ubiquitous access to fixed and mobile networks
Authentication services – providing secure identification

Payment/Billing services

Identity management services with easy overview and handling of different VID

Communication services (SMS, email, conference services for voice or video, …)

Additional service-offerings based on the users (anonymous) attribute database

Market data services based on anonymous analysis of the attributes and usage data and resulting reports

(3rd party) Service Provider:

Service provision adapted to their users (anonymous) attributes database. These services may also include payment services.

Additional service-offerings based on the users (anonymous) attribute database

Market data services based on anonymous analysis of the attributes and usage data and resulting reports

User / Student:

Possible savings based on revealing attribute for special offerings

Provide own content for services
Annex A Bibliography


[3] ISO/IES NP 29146 / 1.27.64 / JTC 1/SC 27/WG 5 A framework for access management