Ruprecht-Karls-Universität Heidelberg
Institut für Informatik
Lehrstuhl für Datenbanksysteme

Bachelor Arbeit

Integrating Identity Management Providers based on Online Access Law

Name:	Jonas Gann
Matrikelnummer:	3367576
Betreuer:	Prof. Dr. Michael Gertz
Datum der Abgabe:	June 27, 2021

Ich versichere, dass ich diese Bachelorarbeit selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe.

Date of Submission: June 27, 2021

Zusammenfassung

Diese Bachelorarbeit stellt Identity Management Provisioning (IMP) als mögliche Lösung von Problemen Benutzerprofil basierter Identitätsmanagementsysteme vor. IMP bietet Identitätsmanagement als Service für Benutzer und Dienstanbieter. Es ermöglicht Nutzern eine IMP Identität zu erstellen, um persönliche Informationen und Nachrichten mit mehreren Dienstanbietern auszutauschen.

Damit Dienstanbieter mit bestehenden, auf Benutzerprofilen basierenden Identitätsmanagementsystemen IMP nutzen können, ist eine Integration in bestehende Geschäftsprozesse und bestehende Systemarchitekturen erforderlich. Es werden zwei IMP Lösungen vorgestellt, die beschreiben, wie Service Provider IMP verwenden können. Außerdem wird ein Messaging System für die technologische Integration präsentiert.

Ziel der IMP Lösungen ist es, Möglichkeiten zu beschreiben, die Benutzerfreundlichkeit, Datenschutz und Sicherheit des Identitätsmanagements durch die Nutzung des IMP Dienstes erhöhen. Die IMP-Lösungen werden, basierend auf dem aktuell relevanten Anwendungsfall des Online-Zugangs-Gesetzes (OZG), konzipiert.

Die erste IMP Lösung beschreibt eine Möglichkeit, welche Benutzern die Erstellung von Benutzerprofilen, Pflege persönlicher Informationen und Interaktion über eine IMP Anwendung ermöglicht. Dieser Integrationsansatz soll die Benutzerfreundlichkeit erhöhen und gleichzeitig das Risiko, die Komplexität und die Kosten der Integration minimieren. Dadurch, dass auf Benutzerprofilen basierende Identitätsmanagementsysteme in Betrieb gelassen werden, bleiben Probleme hinsichtlich des Datenschutzes bestehen. Eine zweite IMP Lösung wird vorgestellt, die den Datenschutz erhöht, indem Benutzerprofile ersetzt werden. Stattdessen geben Nutzer persönliche Informationen nur für einzelne Geschäftsprozesse temporär frei.

Zur Integration von IMP Lösungen wird ein Messaging System vorgestellt, das in der Lage ist, IMP in bestehende Systemarchitekturen von Dienstanbietern zu integrieren. Neben messaging ermöglicht ein modularer Ansatz, dass die Integrationsarchitektur konfigurierbar und erweiterbar ist, um verschiedene IMP Lösungen in unterschiedliche Systemarchitekturen zu integrieren. Die Fähigkeiten des Messaging Systems werden durch die Integration der zuvor beschriebenen, grundsätzlich unterschiedlichen, IMP Lösungen in verschiedene Systemarchitekturen im Kontext des OZG demonstriert.

Abstract

This bachelor thesis presents Identity Management Provisioning (IMP) as a possibility for solving problems of user profile-based identity management systems. IMP provides identity management as a service to users and Service Providers. It enables users to create an IMP identity and use it to share personal information and exchange messages with multiple Service Providers.

In order for Service Providers with existing user profile-based identity management systems to utilize IMP, integration into their existing business processes and existing system architectures is necessary. Two IMP solutions which describe how Service Providers can utilize IMP and one messaging system for technological integration are presented.

The purpose of IMP solutions is to describe possibilities to increase usability, data protection and security of identity management through the utilization of the IMP service. The IMP solutions are designed, based on the currently relevant use case of the Online Access Law (Online Zugangs Gesetz - OZG).

The first IMP solution describes the possibility of enabling users to create user profiles, maintain personal information, and interact through an IMP application. This integration approach is designed to increase usability while minimizing the risk, complexity, and cost of integration. As a result of leaving user profile-based identity management in operation, problems regarding data protection remain. A second IMP solution is presented to increase data protection by replacing user profiles. Instead, users temporarily share personal information for individual business processes.

For the integration of IMP solutions, a messaging system is presented which is capable of integrating IMP into existing system architectures of Service Providers. In addition to messaging, a modular approach enables the integration architecture to be configurable and expandable to integrate various IMP solutions into different system architectures.

The capabilities of the messaging system are demonstrated by integrating the previously described, fundamentally different IMP solutions into different system architectures in the context of the OZG.

Contents

1 Introduction

Today, many services are accessible through the internet. Especially during the COVID-19 pandemic, stores had to switch to online trade due to lockdowns. Even after lockdowns, customers might continue to favour e-commerce [11]. Online Service Providers (SP) often require customers to create user profiles to access their services. Management of personal information as well as interaction and communication between Service Providers and customers are often only possible through a web page or e-mail. It is time consuming to maintain even a small number of user profiles: To change personal information, for example, an e-mail address, the web page of each Service Provider has to be accessed, the correct credentials have to be submitted, and the information has to be manually filled in each time.

In some cases, user profiles are required by Service Providers even if they are not necessary. Especially in the case of small stores, running their individual online shops, user profiles are not necessary for customers to place an order. Personal information can be shared temporarily until processing of the order is completed and the package is delivered. Some online shops allow users to place orders by temporarily sharing personal information, however this limits interaction and communication possibilities to insecure e-mail exchanges.

A currently relevant topic with an interesting approach for identity management is the German Online Access Law (Online Zugangs Gesetz - OZG). It requires the German federal republic, each federal state and each commune to provide administration portals for digital access to administrative services [3]. The federal republic and each member state operate their individual user profile systems accessible through their administration portals [15].

The Online Access Law therefore constructs a system landscape that demonstrates the scenario of distributed partial identities on a small scale while maintaining the same problems as the private sector: Users have to create, maintain, and login into multiple user profiles to access administrative services distributed across administration portals. To solve this problem, a new solution for making OZG user profiles "interoperable" is in development [15]. However, interoperable user profiles can not be accessed by the private sector.

Identity Management Provisioning (IMP) is an approach to identity management which aims to solve the problems of distributed partial identities by enabling users to bring their online identities with them when accessing the systems of Service Providers. It provides identity management as a service to users and Service Providers by enabling users to create and manage a single digital identity and use it to share personal information and interact with multiple Service Providers through "IMP relationships" and "IMP messages". With IMP relationships, users and Service Providers have a tool to securely share personal information which, depending on the use case, can be utilized in different ways. It can, for example, be used to create and manage a persistent SP user profile or to temporarily share personal information for the business process of a SP. IMP messages enable the user and Service Provider to securely exchange structured data and depending on the client application that receives and displays the data, design rich user interactions. This approach to identity management could be an alternative to user profiles in the private sector and in the context of the OZG.

Identity management systems do not stand alone but have to be accessible by various other systems in a system architecture to, for example, access personal information and perform authentication. They also play an important role in the design of business processes. Therefore, for Service Providers to utilize IMP, integration into existing business processes and existing system architectures is necessary.

1.1 Objective

The bachelor thesis uses the scenario of the OZG as a small-scale model for the general problem of distributed partial identities. Focus is the utilization and system integration of IMP for Service Providers with existing user profile-based system architectures. A federal state, in the context of the OZG, is used as an example for a Service Provider.

One objective of the bachelor thesis is to examine the problems of user profile-based identity management and interoperable OZG user profiles and to describe to what extend IMP as an approach can be a solution.

Another objective of the bachelor thesis is to design "IMP solutions" which describe the possibilities of how IMP services and tools can be concretely utilized on the example of - but not limited to - the OZG use case. IMP solutions demonstrate how IMP relationships and IMP messages can be utilized by users and Service Providers to share personal information and interact to solve the problems of distributed partial identities related to usability, data protection, and security.

Using OZG as an example, another objective of the bachelor thesis is to design a technological integration architecture for the integration of IMP solutions into existing system architectures of Service Providers. Its integration capabilities, however, can not be limited to one IMP solution and one system architecture. On the contrary, it has to be capable of integrating various IMP solutions into different system architectures. The integration system therefore has to be configurable and expandable according to the requirements of new IMP solutions and system architectures. To demonstrate the capabilities of the integration architecture in theory, IMP solutions presented as part of the thesis have to be integrated into different system architectures in the context of the OZG.

IMP solutions and integration architecture presented in the bachelor thesis should not be perfectly fitted to the scenario of the OZG but have to also be utilizable by Service Providers in other contexts.

1.2 Structure of Work

The chapter "Background and Related Work" covers important topics that the following chapters rely on. The chapter "User Profile Identity Management" describes the disadvantages of user profile-based identity management in general as well as in the context of the OZG. Possible solutions through IMP are described. The chapter "IMP Utilization as Extension" presents the first IMP solution as well as its integration through the technological integration architecture. The chapter "IMP Utilization as Replacement" presents the second IMP solution as well as its integration through the technological integration architecture. The chapter "Conclusion" summarizes the most important results of the thesis and mentions possible future developments and contributions.

2 Background and Related Work

This chapter covers three important topics that the following chapters rely on. Identity Management Provisioning as an approach to solve problems of distributed partial identities is described along with possible services and systems. The most important regulations of the Online Access Law as well as its basic use case and the resulting system architecture of a federal state are described. Messaging is presented as a way of designing technological integration architectures. Multiple messaging patterns as well as their visual notation are explained.

2.1 Identity Management Provisioning (IMP)

The purpose of this section is to deliver a broad understanding of what Identity Management Provisioning (IMP) is, what an IMP service can look like and how Identity Management Provisioning systems can operate.

2.1.1 IMP

Identity Management Provisioning is a method where identity management is provided as a service to users and Service Providers. This service enables users to create and manage a digital identity and to use it to share personal information and interact with Service Providers.

Many identity management systems currently in use by Service Providers require the user to create a new user profile, specify login credentials, and keep the personal information up to date. Every Service Provider operates their own identity management system and users have to access each system individually through multiple websites to use their user profiles. This approach to identity management leads to several problems which are discussed in section 3.1.

In contrast to a user profile-based identity management approach, IMP provides identity management as a service. Only one identity management provisioning system is hosted and accessed by users and Service Providers. Users therefore only need one IMP identity that is accessed by multiple Service Providers. This approach to identity management is capable of solving various issues of user profile-based identity management that are discussed in section 3.2

To access the IMP service, users can use applications or websites. Service Providers, however, often require integration into their existing system architecture to enable existing system components to use the new identity management method.

2.1.2 IMP Service

There are many ways to design a service for identity management provisioning. This section describes what an identity management provisioning service can look like. The content of this section is based on the IMP service provided by IDAS [6].

Software tools exist for users and Service Providers to access the IMP service. For the user, this is a smartphone application. For the Service Provider, this is an integration component. The smartphone application provides a user-friendly graphical interface which enables the user to receive notifications, maintain personal information, share personal information, and more. The integration component for the Service Provider is a software solution with similar capabilities as the smartphone app but designed towards enterprise use. It therefore has no graphical user interface but additional business relevant features and integration capabilities. IMP application and integration component are described in section 2.1.3 in more detail.

One important part of the IMP service is the management of personal information by users. After installation of the smartphone application, a new identity (IMP identity) can be created. As part of this identity, the user can add any number of key-value pairs as attributes, the list of all attributes making up the personal information of the IMP identity. Despite being able to add any key-value pair, there are some commonly used keys like name, age, home address, etc. Depending on the use case of Service Providers, different keys and their meaning have to be agreed upon. This means the IMP service has to define a canonical data model. Each Service Provider then translates it to their individual data models.

Many Service Providers require users to manually verify their identity and personal information by, for example, visiting a store and showing their ID card. Similar verification processes are expected to be used by the IMP service to verify IMP identities and their personal information. However, for simplification reasons, the details of this verification process are left out in this thesis.

Users and Service Providers can establish relationships and use them to share personal information and interact. The initial form of a relationship is a relationship template, which is created by the Service Provider and describes what type of relationships they are willing to establish. The templates are made available to interested users, which can use them to request relationships.

A Service Provider can fill a relationship template with optional and mandatory information:

Title The title describes the purpose of the relationship in a short way.

Requested Attributes The Service Provider can list the keys of the attributes he requires the user to share to send a relationship request. When the user submits a relationship request based on this relationship template, the values filled in for the requested attributes are copied and sent as part of the request. The recipient of the request can use the personal information to decide whether to accept or reject the relationship.

Shared Attributes Shared Attributes is a list of key-value pairs that the Service Provider makes available to any user interested in requesting a relationship. The Service Provider has to share a minimal number of attributes that enable the user to identify it.

Purpose This is a text field where the Service Provider can give a detailed explanation of what the purpose of the relationship is, e.g, what effects a relationship request and an established relationship will have. The reasons for why the requested attributes are necessary for the relationship have to be explained here as well as how each shared attribute is going to be processed. This helps the user in making an informed decision on whether to submit the relationship request or not.

Attachments Attachments can be all kinds of documents and files. For example, legal information can be included but also product flyers corresponding to the relationship template, etc.

Metadata Metadata can be any type of information which should not be displayed to the user but is necessary for the user application or the Service Provider to process the relationship process.

When the user receives the template through his IMP application, the requested attributes are automatically filled in if they exist in his IMP identity. Otherwise, they can be filled in manually and added as new attributes of the IMP identity.

At this point, it is important to take a look at how IMP identity attributes and shared attributes are separated. IMP identity attributes are managed by the user to reflect the most up to date information. Attributes shared as part of a relationship can be automatically filled with values from the IMP identity but can also be manually entered. This means shared attributes and IMP identity attributes are not necessarily the same.

Based on the information about the Service Provider and the purpose of the relationship, the user can decide to send a relationship request or not. If the user decides to request the relationship, the request is sent to the Service Provider. If the Service Provider approves the request, the relationship is established and both parties get notified. Through the IMP application, the user can see all relationships as well as their status, the content of the underlying relationship template, and a list of shared attributes and their values.

As part of an established relationship, the user and Service Provider can interact with each other by asynchronously exchanging structured data packages as IMP messages. IMP messages can contain any content, however, both IMP application and Service Provider systems should be able to understand the messages. For this purpose, besides content, messages are expected to contain some identification value like a message type. The integration component provided to the SP does not process the content of messages but simply makes the messages accessible to the system architecture of the Service Provider. Without additional integration systems, the Service Provider has to implement his own solutions for understanding and processing messages. The IMP application, however, has a set of messages it understands. The list of messages the application is able to process can be expanded by the identity management provider who develops it.

Some important messages the IMP application understands and the Service Provider should be able to process are:

Mail Messages of the mail type can be used by Service Providers and users to exchange human readable text. Mails sent to an IMP identity are displayed by the IMP application through, for example, a notification. The IMP application defines a format for the content of the mail. The term "mail" is used as an alternative to the term "message", as messages will later be used in the context of a messaging system.

Attribute Change Messages of the attribute change type can be used by the user to request the modification of shared attributes. The user can modify, add, or delete the attributes shared as part of a relationship and submit an attribute change request to the Service Provider which contains the changes. The Service Provider can decide to either accept or reject the request and respond with a corresponding attribute change response message. The IMP application defines a format for the content of the attribute change request and response messages.

Authentication Messages of the authentication type can be used by the Service Provider to request confirmation of the IMP identity for a specific business process. The Service Provider sends an initial request message to the IMP identity which contains a description of what confirmation is requested by the user. Through the IMP application the user is notified and can accept or reject. Depending on the interaction by the user, the IMP application sends a response message to the Service Provider. The IMP application defines a format for the content of the authentication request and response messages.

The IMP system guarantees that all information is encrypted and can only be deciphered by identities that are allowed to read it. This usually does not include the systems hosting the IMP service. Only the owner of an identity can manage the attributes of their identity. A relationship is established only with the identity presented as part of the relationship request and only the specified attributes are shared. Interactions as part of a relationship are only possible between the two parties of the relationship and cannot be intercepted or modified by others.

2.1.3 IMP System

This section describes the IMP system which is the system architecture required for providing the IMP service described in the previous section. The content of this section is based on the IMP system used by IDAS [6].

As shown in figure 2.1, the IMP system can be separated into three domains.
The user domain contains systems that the user directly interacts with. These typically are applications on personal computers, smartphones, and websites. IMP applications on smartphones are provided to users for accessing IMP services. For simplification, each user is assumed to access the IMP service through one device, which eliminates the need for device synchronization. As previously described, the IMP application enables users to manage the attributes of their identity, to establish relationships, to manage relationships, and to exchange messages for interaction.

The Service Provider domain contains the system architecture of the Service Provider and the IMP connector. The IMP connector contains a REST API which enables the system architecture to access IMP services.

The IMP domain contains all identity management provisioning systems required to

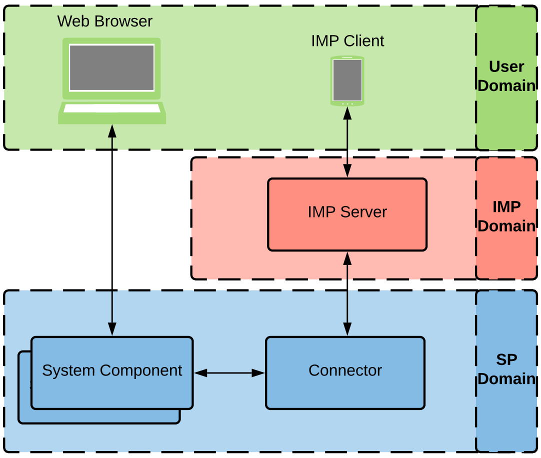

Figure 2.1: IMP System Domains

be hosted by the identity management provider. In this case, the domain contains only the IMP server. The IMP server is able to communicate with each IMP application and IMP connector. It has the purpose of maintaining a - when necessary, encrypted - list of all identities, relationships, relationship templates, and IMP messages. As the IMP server does not know the private key corresponding to the IMP identity, it is unable to decipher the data. The IMP server is also capable of creating relationship templates, processing and routing relationship requests and responses and IMP messages. The exact details of how the IMP server operates are too complex to be covered in this thesis.

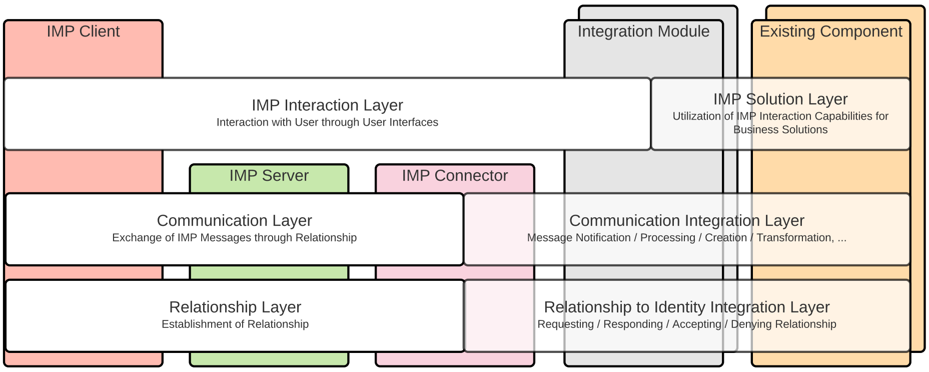
IMP Client
Integration Module
Existing Component
IMP Interaction Layer
Interaction with User through User Interfaces
IMP Solution Layer
Utilization of IMP Interaction Capabilities for Business Solutions
IMP Server
IMP Connector
Communication Layer
Exchange of IMP Messages through Relationship
Communication Integration Layer
Message Notification / Processing / Creation / Transformation, ...
Relationship Layer
Establishment of Relationship
Relationship to Identity Integration Layer
Requesting / Responding / Accepting / Denying Relationship

Figure 2.2: IMP System Layers

As shown in figure 2.2, the operation of the IMP system can be separated into multiple layers. The layers build upon each other (from bottom to top) and provide an increasingly abstract perspective on the functionality of each component.

The vertical bars in the figure represent all previously described components of the IMP system and one additional component called "Integration Module". The "Integration Module" is not important at the moment and will be the focus of the following chapters. The horizontal bars in the figure represent the layers of IMP system operation. From bottom to top, the layers describe the operation of the IMP system increasingly more abstract from the underlying technology. In addition to that, each bar is split up into two sides, however, in this section only the left side is relevant.

The lowest layer is called "Relationship Layer". In this layer, the IMP system operates by establishing relationships. IMP application and IMP connector exchange relationship requests and responses through the IMP server to establish new relationships. The IMP server maintains a list of all relationships and their status.

Once a relationship is established, the IMP system operates on the "Communication Layer". In this layer, IMP messages are exchanged as part of an active IMP relationship between IMP application and IMP connector. The application can create, send, receive, process, and display a list of IMP messages that it is able to understand. The IMP connector is able to send and receive IMP messages through a relationship without requiring to know details about the content. The IMP server stores an encrypted backup of all messages.

Using IMP relationships and IMP messages, the Service Provider can interact with the user on the "IMP Interaction Layer". On this layer, depending on the use case, different purposes can be assigned to the interaction capabilities of IMP. For example, a Service Provider can decide to use relationships as a way to receive product or subscription orders. Another possibility would be to use relationships for filling in a form as part of a survey.

2.1.4 IMP Use Cases

In this section, the IMP system operation for the most important use cases of the IMP service are described in more detail.

Establish Relationship

This section elaborates the sequence of establishing an IMP relationship as shown in figure 2.3. The first step towards a relationship is the interest of a user. A user, for example, wants to subscribe to the newsletter of a Service Provider. The Service Provider needs the personal information of the user to be able to send personalized mails. To obtain the necessary attributes and receive the approval of the user, the Service Provider requires an established relationship.

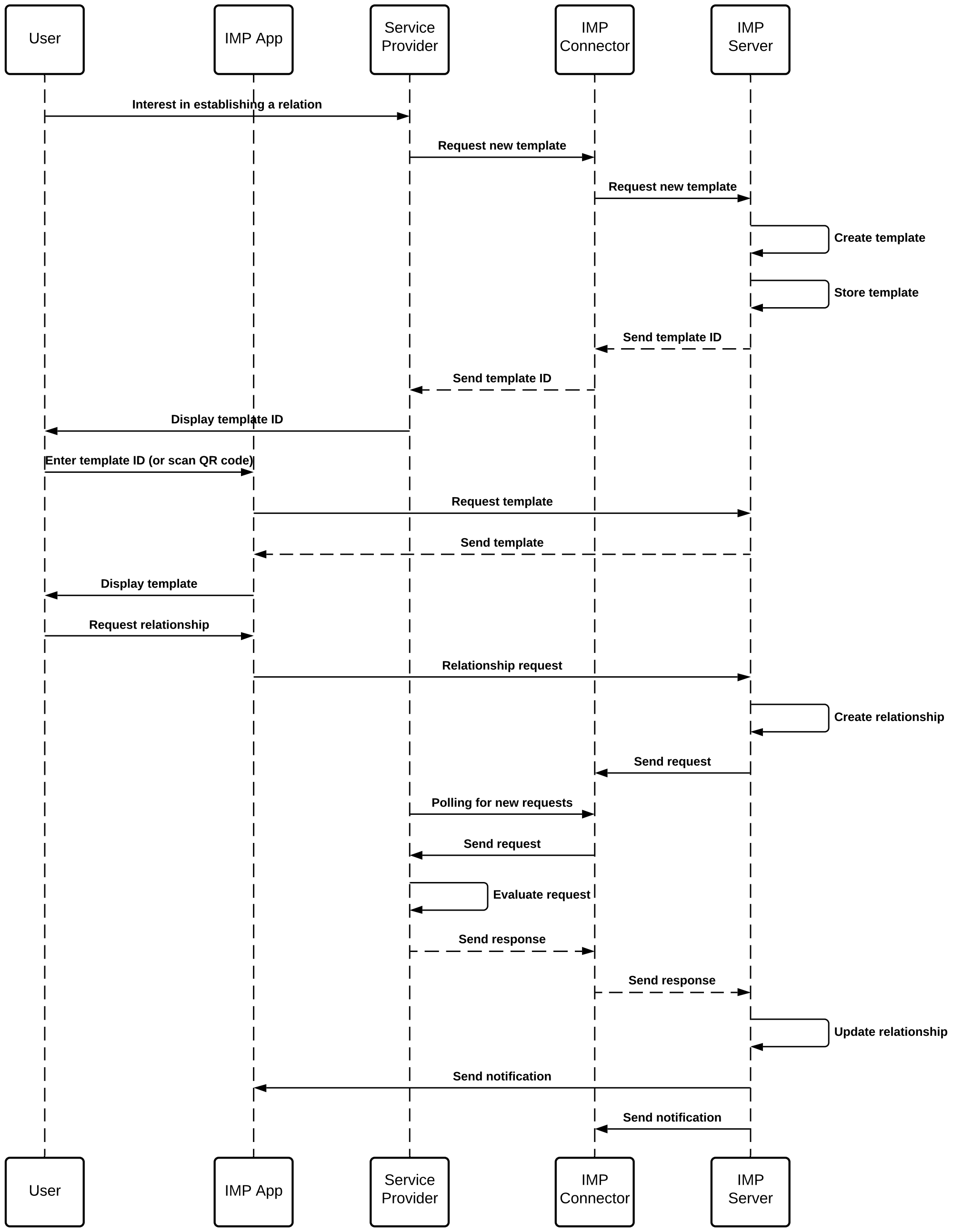

Figure 2.3: Establish Relationship Sequence Diagram

To enable the user to request a relationship with the purpose of subscribing to a newsletter, the Service Provider has to create a relationship template. Through the REST interface of the connector, the SP sends a request for a new relationship template. The request contains parameters specifying the content of the relationship template. In this case, the relationship template could be configured as follows:

- Title: Subscribe to the newsletter
- Requested Attributes: Name, Surname, E-Mail address, Interests
- Shared Attributes: SP Name, SP address, SP phone number, SP e-mail address
- Purpose: By accepting this relationship, you agree to receive personalized emails to the shared address. Name, surname and interests are required to personalize the content of the emails.
- Attachments: required legal document

Based on the parameters of the request, the connector creates a relationship template and sends it to the IMP server. The server stores the template and returns a relationship template ID. Through this ID, the corresponding template can be retrieved from the IMP server. The Service Provider can transmit the template ID to any user who wishes to subscribe to a newsletter. This can be done by, for example, rendering the template ID as a QR code on a website. If the QR code is displayed, the user can scan it using the IMP application. The application understands that the content of the QR code contains a relationship template ID and retrieves the corresponding template from the IMP server.

The IMP application displays the relationship template to the user and automatically fills in as many requested attributes as possible.

The user can now decide whether to accept the relationship and share the requested attributes. If the user accepts, IMP application sends a relationship request to the IMP server. The request contains all information of the relationship template in addition to the shared attributes of the user.

Based on the relationship request, the IMP server creates a relationship with the status "pending". A unique relationship ID is attached. The server then forwards the relationship request to the connector of the Service Provider.

As the system architecture of the Service Provider has no way of knowing when the connector receives a relationship request, it regularly requests an update from the connector through its REST interface. The connector eventually responds with the received relationship request. The system architecture of the Service Provider processes the request to decide if it should be accepted. The Service Provider could, for example, verify if a relationship with the identity already exists or if the e-mail address is already registered.

The system architecture sends a relationship response to the REST interface of the connector. The response contains all information of the received relationship request with optional additional information the Service Provider might want to share now. This could, for example, be the name of the newsletter the Service Provider decided to select for the user based on his specified interests.

The connector sends the relationship response to the IMP server, which updates the content and status of the corresponding relationship. It might be possible that the user retracted the relationship request in the meantime. In that case, the relationship response would be dropped by the IMP server and the connector would be notified. If, however, the IMP server updates the status of the relationship to "established", both IMP application and connector are notified about the final content of the relationship.

After receiving the final "relationship established" notification, the system architecture of the Service Provider can store the shared attributes in a database along with the corresponding relationship ID.

Attribute Change

This section describes the sequence of changing an attribute shared as part of an IMP relationship as shown in figure 2.4. If the user switches to a new e-mail provider, he will need to change the corresponding e-mail attribute shared as part of the relationship to receive the newsletter on his new e-mail address.

Through the IMP application, the user can view relationships and edit shared attributes. After changing an attribute, for example, the e-mail address, the IMP application sends an attribute change request to the IMP server, which forwards it to the IMP connector corresponding to the IMP relationship. Through the REST interface of the IMP connector, the Service Provider regularly polls for new messages and eventually receives the attribute change request. The Service Provider evaluates whether to accept or reject the request and uses the REST interface of the IMP connector to submit the response. The IMP connector sends the response to the IMP server which - if the Service Provider accepted the request - notifies the IMP connector and IMP application of the successful change of attributes. The Service Provider again polls for new messages and eventually receives the "attribute change established" notification, based on which it now updates the stored attributes associated with the relationship. When the IMP application receives the attribute change established message, it displays a notification to the user.

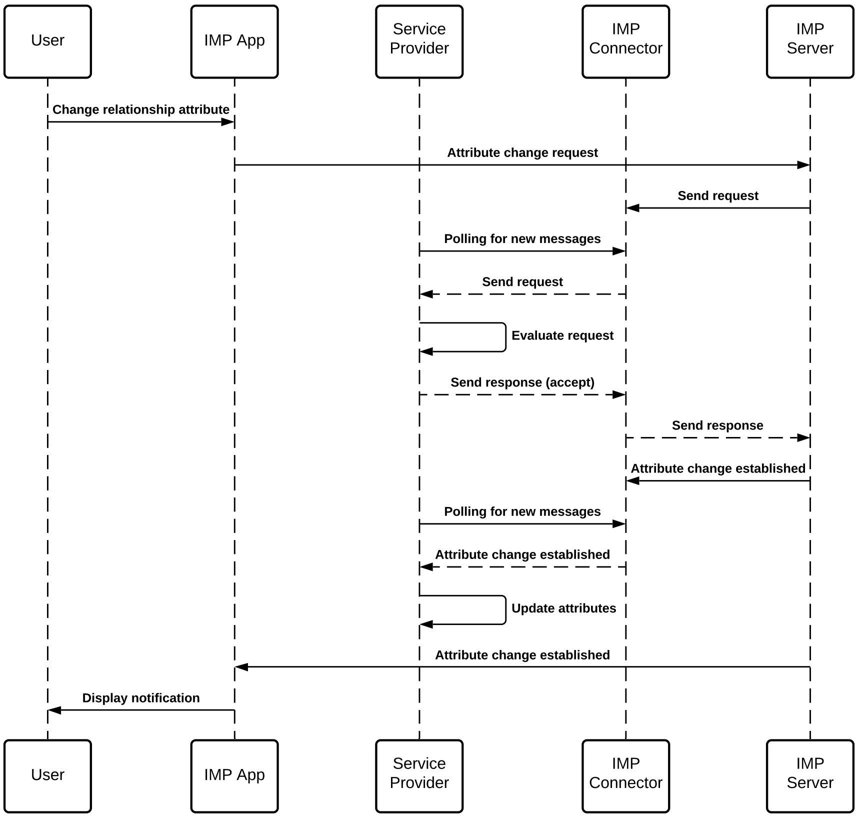

Figure 2.4: Change Relationship Attributes Sequence Diagram

Mail

This section describes the sequence of sending a mail as part of an IMP relationship as shown in figure 2.5. If a user, for example, has questions about the newsletter, he can send a mail to the Service Provider as part of the established relationship.

With the IMP application the user can view relationships and submit mails. Once submitted, the IMP application sends the mail to the IMP server, which forwards it to the IMP connector corresponding to the relationship. The Service Provider polls for new messages and eventually receives the mail as response. An employee of the Service Provider can process the email and use the REST interface of the IMP connector to send a response mail to the same relationship. The IMP connector sends the mail to the IMP server, which forwards it to the IMP application of the IMP identity corresponding to the IMP relationship. The application then notifies the user of the received mail.

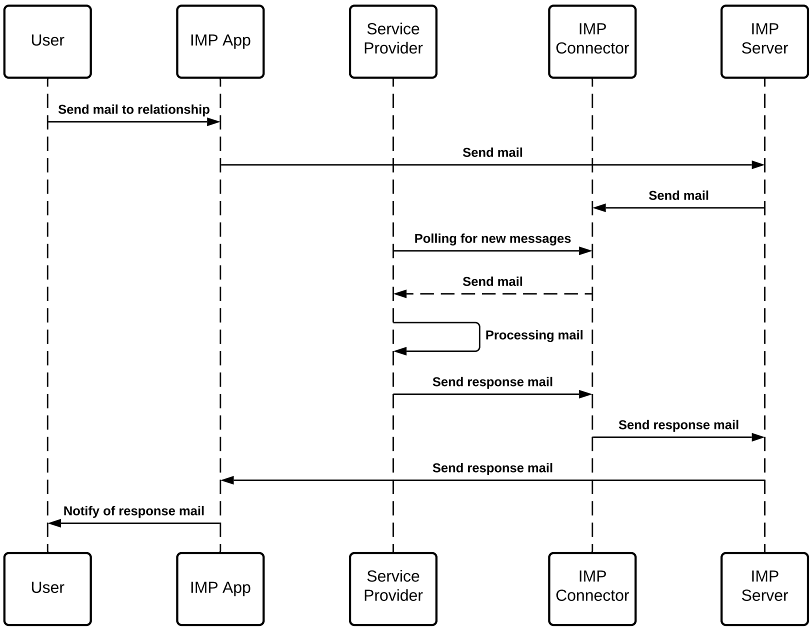

Figure 2.5: Mail Sequence Diagram

Authenticate

This section describes the sequence of authenticating as part of an IMP relationship as shown in figure 2.6. If the Service Provider wants to request confirmation from the user, they can send an authentication request to the corresponding relationship.

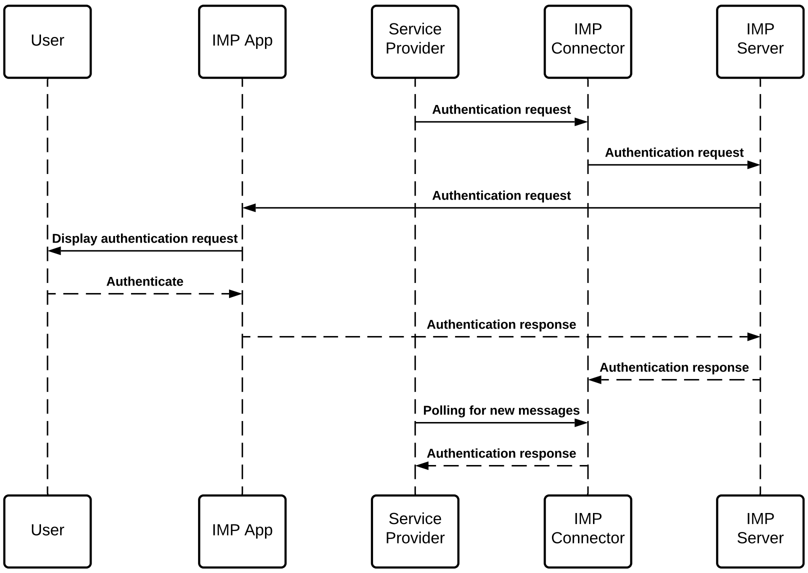

Figure 2.6: Authenticate Sequence Diagram

The SP uses the REST interface of the IMP connector to send an authentication request as part of an IMP relationship. The IMP connector sends the request to the IMP server which forwards it to the IMP application of the IMP identity corresponding to the IMP relationship. The application displays the authentication request to the user. The user can accept or reject the request which will result in the corresponding authentication response by the IMP application. The response is sent to the IMP server which forwards it to the IMP connector corresponding to the IMP relationship. The Service Provider polls for new messages and eventually receives the authentication response.

2.2 Online Access Law (OZG)

This chapter gives an overview about the Online Access Law regarding its regulations, their implementation, the basic OZG use case, and the underlying system architecture.

2.2.1 Regulations

In 2017, the German government passed the Online Access Law (OZG), which requires the federal republic and federal states to execute the following regulations until 2022 [2]:

Digital availability of administrative services An administrative service is the electronic processing of administrative procedures that are available from outside the governmental institution. As it is not clear which administrative services exactly are included in the definition of the OZG, the Federal Ministry of the Interior Building and Community (Bundesministerium des Innern, für Bau und Heimat - BMI) created a catalogue [5]. The OZG requires these services to be digitally available. As a guideline on what is considered sufficient availability, the BMI defined a maturity model [16].

Digital access to administrative services through administration portals of a portal network Federal republic, each federal state and each commune must provide an administration portal. Portals of communes must be linked to the portal of the corresponding federal state. Portals of federal republic and federal states must be connected through a portal network. [14] Each portal must provide a "seek and find" feature, which enables users to find all administrative services provided by any administration portal [13].

Interoperable user profiles for accessing administrative services Federal republic and federal states must provide user profiles that can be used to identify the corresponding person while requesting access to administrative services, to save personal information according to the once-only principle, to receive and send messages via a digital mailbox and to pay for services. The user profiles must be interoperable for every administration portal of the portal network [15].

2.2.2 Implementation of Regulations

The implementation of OZG regulations can be separated into two projects: The digitalization and networking project.

The goal of digitalization in this case is to make administrative services available towards a user in a digitized way: A digitized administrative service can be accessed by a user through a website. The website is hosted either by the federal republic or a federal state and is called "Administration Portal". Access is usually provided through an application form. The administrative service can be managed through a user profile which is provided by the federal republic or the federal state. Management of an administrative service usually includes starting the service by sending in a form, communicating with the responsible institutions through the inbox of the profile, and receiving a result. The user profile can also enable users to upload documents to a datawallet and to save personal information for automatically filling in forms.

Digitalization of an administrative service is the modification of the underlying processes to incorporate the usage of the described features of the user profile and administration portal. In total, the BMI lists 575 relevant services, some of them provided by the federal republic, some by the federal states, and some by the communes [1].

The networking focuses on connecting governmental systems to make all digitized administrative services available for every user. This includes most importantly the connection of administration portals to a portal network through an online gateway and the interoperability of user profiles.

To save investment, a method called "one for all" is used when hosting administrative services. One federal state or the federal republic provides access to a service on their administration portal and distributes the requests to the responsible institutions "under the hood". As administration portals are connected through an "online gateway", each portal contains a search feature, which enables users to find all administrative services through any portal. Interoperable user profiles enable the usage of each profile for the management of administrative services on all portals.

2.2.3 Basic Use Case

Each time users apply for administrative services, they have to go through an application process, in the following section summarized as the basic OZG use case.

A user wants to apply for two administrative services: funding under the Federal Training Assistance Act (BAföG) and a drivers license. Both administrative services are provided through the "one-for-all" method. The federal state Sachsen-Anhalt is responsible for processing BAföG applications on its administration portal and the federal state Hessen is responsible for processing drivers license applications on its administration portal. The user has never accessed OZG services before.

Create User Profile The user wants to apply for BAföG first and therefore visits an administration portal which informs that to apply for administrative services, a user profile is required. As user profiles are designed to be interoperable, it does not matter through which administration portal the user profile is created.

The user is requested to enter personal information and to specify an authentication method. For authentication, for example, a username and password combination can be used.

Selection of Administrative Service Using the search feature of the administration portal, the user enters the search term "bafög" and is presented with a list of administrative services as result. The user selects the correct administrative service from the search result and is forwarded to the web page of the service on the administration portal of Sachsen-Anhalt . It contains information about the administrative service along with instructions on how to access an interactive application form which is can be hosted on a separate web page.

Login to User Profile Before being able to apply for administrative services, the user has to login into the user profile on the administration portal. Depending on the authentication method used for logging in, the trust level of the current session is determined. Only with a high trust level, users can apply for a broad selection of administrative services. The user has selected an authentication method which results in a high trust level.

Application On the web page of the administration portal, the user clicks on a "bring me to the application" button and is forwarded to a web page with an interactive form. Before the user is forwarded, he has the option to transfer personal information for automatic filling of the form. The user decides to accept and is presented with a filled-in form. After pressing the "submit" button, the application is transferred to the responsible institution.

Management of Applications The user is forwarded back to the administration portal and selects to view all active applications created through the portal. Here the user can see the application and is able to manage it by, for example, requesting cancellation.

Communication Through the inbox of the user profile, the user is notified about a message regarding the application. The institution responsible for processing the application informs the user about receiving the application. Eventually, the institution finishes processing the application and sends a message to the inbox of the user to inform them about the result. This marks the end of the basic OZG use case, however, the user wants to apply for a second administrative service.

Selection of Administrative Service Using the search feature of the administration portal, the user now enters the search term "drivers license", selects the correct search result, and is forwarded to the corresponding web page on the administration portal of Hessen.

Login to User Profile The same interoperable user profile can be used as on the administration portal of Sachsen-Anhalt, but the user is required to login again.

Application The application process is designed to be similar for each administration portal, however, as Sachsen-Anhalt and Hessen operate their application processes independently, minor differences exist in, for example, the design and text of the web pages.

Management of Applications The user is again forwarded back to the administration portal and selects to view all active applications created through the portal. The user is only able to see and manage the application for a driving license. As the application for BAföG was created through a the administration portal of Sachsen-Anhalt, it is not accessible through the administration portal of Hessen.

Communication Through the inbox of the user profile, the responsible institution again sends notifications about the current status and results of the application.

2.2.4 System Architecture

This section describes the OZG system architecture of a federal state capable of executing the basic OZG use case. References about OZG system architectures of Baden-Württemberg [8] and Nordrhein-Westfalen [12] are used. The presentation document regarding the administration portal of Baden-Württemberg [4] is used as the basis for describing the administration portal.

As shown in figure 2.7, the OZG system architecture is separated into three components and two domains. Domains in this case separate systems regarding the physical location where they operate. Components in this case describe functionally correlated systems of a system architecture.

The "User Component" directly interacts with users to enable access to administration portals. This can be desktop or mobile applications or as in this specific case, a web browser. The "Administration Portal Component" hosts the administration portal. The "User Profile Component" provides interoperable user profiles. The "Integration Component" transfers filled in applications to responsible institutions. And finally, the "Institution Component" receives and processes applications.

The administration portal directly interacts with the "User Component" through a web page and provides access to the basic OZG use case by interacting with other components. It consists of a web server that is responsible for hosting web pages and a service facade connected to multiple service components. Through the service facade, the web server accesses each service component and makes its service available to the "User Component". The "User Profile Management" component is capable of interacting with the "User Profile Component" to create new user profiles, retrieve personal information from existing user profiles, and process login requests. The "User Profile Component" provides conventional user profile-based identity management. Through the Federated Identity Management of Interoperable User Accounts in Germany (Föderiertes Identitätsmanagement interoperabler Nutzerkonten in Deutschland - FINK) the "User Profile" component of each federal state is made interoperable. The "Search" component can be used to retrieve a list of URLs of administrative services corresponding to a search term. It can retrieve URLs of administrative services from all administration portals through the "Online-Gateway".

The "Online-Gateway" is a system connecting all administration portals and enabling them to exchange information. The "Formula Engine" component is accessed by the web server to display interactive forms to the user when applying for selected administrative services. The interactive form can be either integrated into the web page of the administrative service or hosted on a separate web page. The user can opt in to

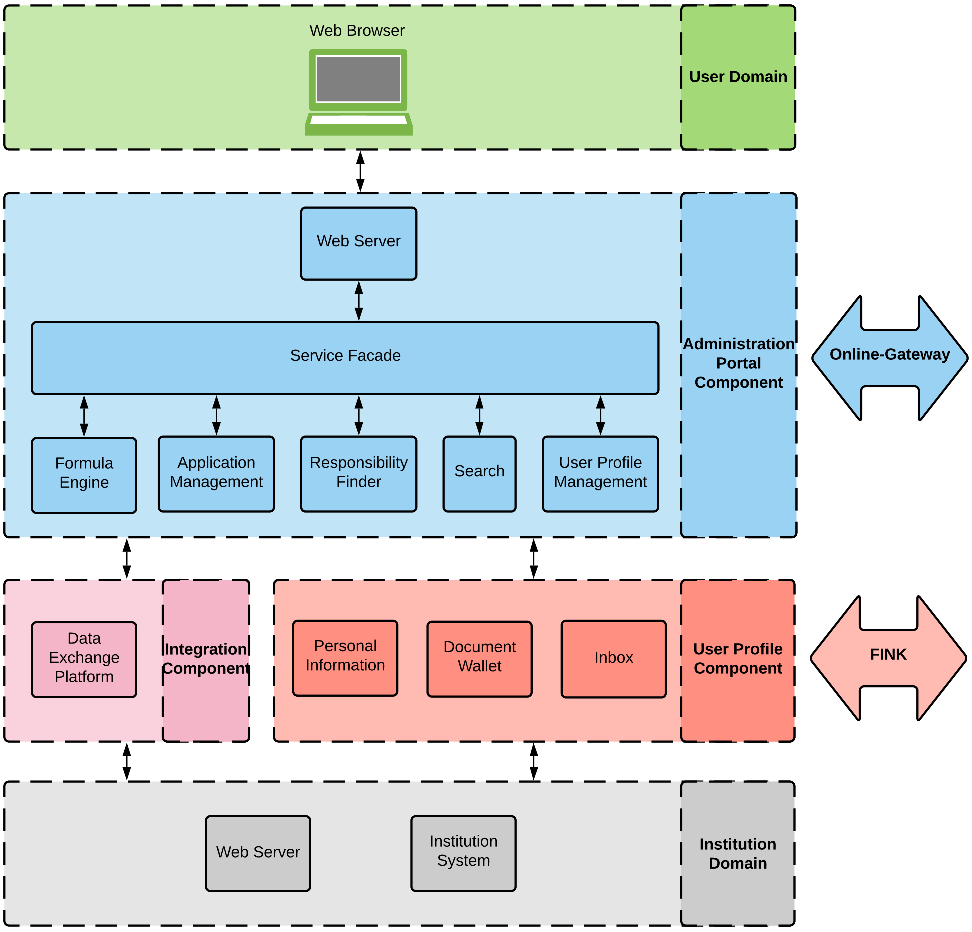

Figure 2.7: OZG System Architecture of Federal State

automatically fill in forms with personal information. In that case, after authentication of the user, the "Administration Portal" component retrieves personal information from the "User Profile" component and sends it to the "Formula Engine" before displaying a filled-in form to the user.

The "Application Management" component receives submitted applications by the "Formula Engine" component for further processing. Depending on the administration portal and the type of application, additional processing steps that are not part of the use case can occur. This includes, for example, payment processes. The component tracks the current status of the application, which the user can view through the web page of the administration portal. It is also capable of terminating the application process if the user requests it.

The "Application Management" component sends information about the application to the "Responsibility Finder" component which returns an identification of the institution responsible for processing the application. Along with the institution ID, the

"Application Management" component submits the application to the "Data Exchange Platform". This component transfers the application data to the institution corresponding to the specified institution ID. The institution can register their "Institution System" to automatically receive the application from the "Data Exchange Platform" where it will be processed. In addition to that, the "Institution Component" hosts a web page with information about the institution.

2.3 Messaging

This chapter gives a brief overview of what messaging is and how it can be used for system integration purposes. It introduces various messaging patterns which will be used by the technological integration in chapters 4 and 5. The content of this chapter is based on the book *Enterprise Integration Patterns* by Gregor Hohpe [7].

Messaging is an asynchronous system-to-system communication, delivering packages of data called messages through channels. Messages can contain any structured data like strings, arrays, or objects. It is up to the sender and receiver to determine and understand its content.

Channels can be seen as a queue of messages accessible to interested systems. Channels have a direction in a sense so that no system simultaneously writes to and reads from a channel. Therefore, by one system writing messages on a channel and another system reading them, a message and data flow can be established.

Depending on the use case, the flow and destination of messages might have to be determined during operation. Therefore, various message routing components exist. Their purpose is to transfer messages from an inbound channel to one or more outbound channels, depending on predefined or dynamic rules.

During the routing of messages between systems, the content of messages might have to be modified. Therefore, various message transformation components exist. Their purpose is to consume messages from an inbound channel, modify their content based on predefined or dynamic rules, and publish the modified message to an outbound channel.

A messaging system manages messaging the way a database system manages data persistence [7, p. 31]. Configuring a messaging system involves the definition of available channels, the type of messages they exchange, their connection between systems, the message flow, and, when necessary, the insertion of routing and transformation components.

Depending on the messaging system solution, additional features can be configured to increase performance, stability, failure safety and more. If properly configured, the messaging system operates reliably, handles unreliable network connections, and persistently stores messages in case of a system crash.

2.3.1 Messaging Integration

One use case for a messaging system is integration.

The main benefit of messaging for integration is that it enables systems to share services and data in a decoupled way. Neither system, whether sending or receiving messages, needs to be aware of each other.

During configuration of the messaging system, datatype channels can be defined. On these channels, only messages with the same content are exchanged. Using message transformation components, messages placed on a datatype channel can be translated to follow a canonical data model.

Systems consuming messages from datatype channels can individually assign a purpose to channels independent from the sending system. As a result of the canonical data model, receiving systems can also choose a data structure independent from the sending system.

As channels are able to function as a message buffer, the sender and receiver of messages do not even have to be running at the same time.

2.3.2 Messaging Patterns

In the book "*Enterprise Integration Patterns*" by Gregor Hohpe [7] multiple patterns for designing messaging systems are presented. This section gives a brief overview of patterns relevant for the thesis and their visual notation. Lucidchart [10] was used for drawing messaging figures.

Message Figure 2.8 shows the visual notation of a message with two attributes.

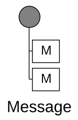

Figure 2.8: Message

Channel Figure 2.9 shows the visual notation of an unnamed channel. Arrows to a message symbol are not a notation for channels but for message flow.

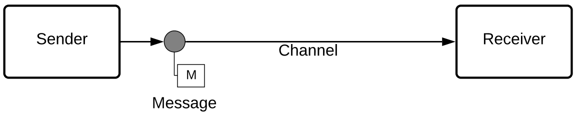

Figure 2.9: Unnamed Channel

Figure 2.10 shows the visual notation of a named channel. Arrows to and from named channels are not a notation for channels but for message flow. Channels are named if they have special importance.

There are different types of channels. In this thesis, the named channels are publish-subscribe datatype channels. Unnamed channels are point-to-point channels. Publish-subscribe channels can be accessed by every system. In contrast to that, point-to-point channels can only be accessed by two systems - one writing and one reading system.

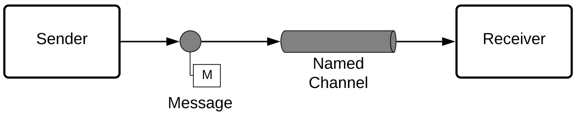

Figure 2.10: Named Channel

Messaging Adapter Systems that do not natively support message-based communication require a messaging adapter which enables the programs of the system to access the messaging system through an API. The messaging adapter usually has to be developed individually for each system, and manually integrated into the code of the system through asynchronous function calls of the adapter API.

Figure 2.11 shows the visual notation of a Messaging Adapter connected to a system.

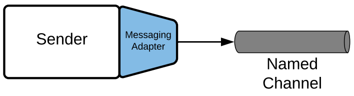

Figure 2.11: Messaging Adapter

Content-Based Router Content-Based Routers contain a preconfigured set of routing rules that instruct the router to place inbound messages on different outbound channels depending on their content. These rules do not change during operation of the system.

Figure 2.12 shows the visual notation of a Message Router.

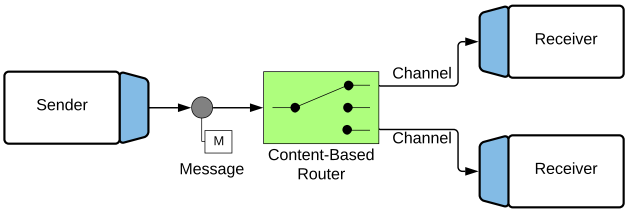

Figure 2.12: Message Router

Message Translator Message Translators have the purpose of translating message content on data representation and data type layer. On the data representation layer, message translators translate message content, for example, from an XML format to a JSON format. On the data type layer, message translators can, for example, concatenate first name and last name fields to a single name field.

Figure 2.13 shows the visual notation of a Message Translator.

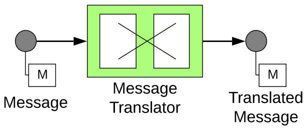

Figure 2.13: Message Translator

As shown in figure 2.14, if using two message translators on both sides of a channel, a canonical data model can be created in between. For more information, read Gregor Hohpe [7, p. 355].

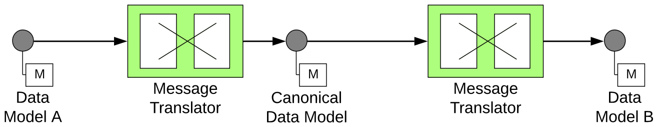

Figure 2.14: Message Translator creating Canonical Data Model

Message Filter Message Filters contain a preconfigured set of filtering rules that instruct the filter to delete messages based on their content. These rules do not change during operation of the system.

Figure 2.15 shows the visual notation of a Message Filter.

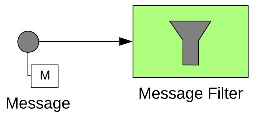

Figure 2.15: Message Filter

As shown in figure 2.16, Message Filters can, in combination with publish-subscribe channels, be used to separate messages to individual datatype channels.

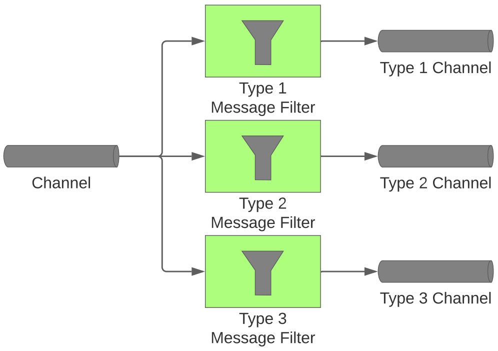

Figure 2.16: Message Filter separating Message Types

Content Enricher Content Enricher have the purpose of adding new attributes to messages. The content which is usually added is a predetermined set of attributes but with dynamically created values.

Figure 2.17 shows the visual notation of a Content Enricher.

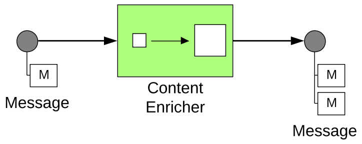

Figure 2.17: Content Enricher

Content Filter Content filters have the purpose of removing a predetermined set of attributes from messages.

Figure 2.18 shows the visual notation of a Content Filter.

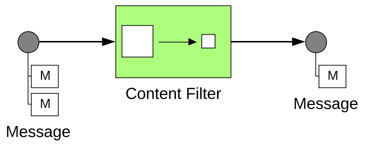

Figure 2.18: Content Filter

Message Store Message Stores have the purpose of storing consumed messages in a database. They are also capable of communicating with other messaging patterns to provide access to stored messages. Communication between message patterns and Message Stores is indicated by a dotted arrow.

Figure 2.19 shows the visual notation of a Message Store. It also shows an example of a Content Enricher accessing the message store.

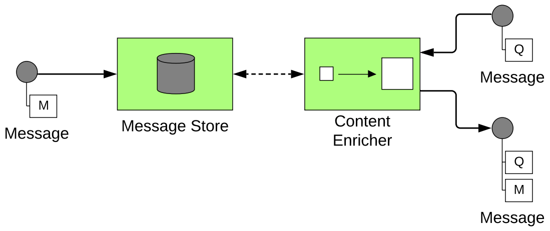

Figure 2.19: Message Store

3 User Profile Identity Management

This chapter describes the issues of user-based identity management in general and for the specific use case of the OZG. It also presents possibilities of how IMP can be utilized to solve the mentioned issues. At the end, the conclusion briefly states whether IMP can be considered for solving the problems of user profile-based identity management.

3.1 Identity Management Issues

The OZG system architecture utilizes user profiles for identity management. This leads to several issues regarding usability, data protection, security, and maintenance costs. The following sections describe problems of user profiles in general as well as problems arising specifically in the context of the OZG.

Usability Each Service Provider has a different platform for the management of personal information and identity-related interactions. This can, for example, be web pages or applications for personal computers and smartphones. Keeping track of all created user profiles is difficult.

In the case of web pages, users will also have to remember various URLs, usernames, and passwords. The risk of forgetting login credentials is high.

To manage the personal information stored in each user profile and, for example, change an e-mail address, users have to access the individual platforms of each Service Provider. Depending on the amount of created profiles, this can be a time-consuming task. Especially if the user has to login to web pages using various authentication methods like passwords, single-sign-on, 2FA, or Magic-Link. Users receiving notifications on multiple platforms can quickly lose track and oversee important notifications.

Each platform is often presented with a different design, although the purpose remains similar. This makes it difficult for users to orientate themselves.

Bidirectional identity-related interactions like subscribing to a service, canceling a subscription, sending or receiving a security relevant mail often only takes place through a web page where e-mails are only used to notify the user to check his user profile ("You have unread messages!"). This is because e-mails do not provide a secure way of exchanging information and do not enable advanced interaction capabilities or exchange of structured content. Although Service Providers could develop mobile applications as an alternative for web pages and benefit from secure communication and advanced interaction capabilities, due to the required investments, smaller SPs might decide not to.

Service Providers rely on the validity of the information stored in the user profile. To guarantee that the information is correct, some SPs require users to take extra identification steps by, for example, performing a video call or requesting the user to show their ID at a local shop. As each Service Provider manages separate user profiles, the user might have to go through this time-consuming process repeatedly.

Users are not able to automatically share personal information from one user profile to another (except for some Single-Sign-On cases). As a result of that, creating a new user profile each time involves entering personal information all over again.

In the case of the OZG, the usability of user profiles across multiple administration portals is limited: Although user profiles are interoperable, the administration portals are individually responsible for the application process. Applying for different administration services, users might have to visit separate administration portals. Each of the portals manages the application process differently. Active applications are not stored as part of the user profile but remain accessible only through the respective portals they were created through.
An overview of all active applications amongst all administration portals does not exist. The user has to go through each portal to find the application they, for example, want to cancel. Especially due to the „one-for-all“ approach users will have to access dedicated administration portals for certain types of administrative services. To mitigate this issue, the inbox of user profiles is used to notify the user of the status of all applications.

Data Protection Service Providers established a habit of collecting more personal information than necessary to provide their services. As a response, the "Datenschutz Grundverordnung" - DSGVO (General Data Protection Regulation) was passed. Amongst other things, it requires Service Providers to inform the user about which personal information is processed, the reason for processing the information, and how it is being processed. Conventional user profile systems which store all personal information but do not differentiate between possibly different processing legitimisation of attributes increase the risk of illegitimate data usage.

As a result of the multitude of user profiles and the variety of platforms to manage them, users can quickly loose track of which Service Provider processes which personal information. Multiple Service Providers storing sensible information increases the risk of personal information being stolen due to a data breach.

In the case of the OZG, the user shares personal information not only with the institutions responsible for processing an application but also with multiple systems operated by the member state. Especially the administration portal used to initiate the application is problematic as it receives personal information from the interoperable user profile, sends it to a form server, eventually receives the filled-in form and stores it. As a result of that, the administration portal has access to all personal information that in reality only the institution will eventually need to process. In addition, institutions actually do not require user profiles for processing applications. After an application is finished, the institution can delete all data stored as part of this process. The only reason user profiles are required is to verify the validity and authorization of incoming applications and to enable the user to comfortably fill in application forms and communicate through an inbox.

Security User profiles are often secured through passwords. Especially for a large number of profiles, users are tempted to use identical passwords, increasing the risk of them being stolen and all user profiles being accessible. With the number of different Service Providers storing personal information and passwords, the risk of it being stolen increases as the security of system architectures differs between Service Providers.

Users also have to rely on the correct operation of the system architecture of the Service Provider and might not be able to prove failures in the operation of the system. If, for example, the user cancels a subscription but the system architecture quietly fails to process it, the user might have issues to provide proof.

3.2 IMP Solution Opportunities

Identity Management provisioning is capable of solving many of the issues described in the previous section.

Usability The goal of IMP solutions is to replace user profiles with a single IMP identity. Through the IMP client, a user can manage their IMP identity and all connected integrated Service Providers. Instead of creating user profiles, the user can establish a relationship between their IMP identity and the Service Provider. Depending on the use case, the relationship can be utilized differently. Using the IMP client, the user can keep track of all relationships without the need of remembering URLs, usernames, or passwords. It also enables the user to update personal information shared with Service Providers through one application. As the IMP client also contains an inbox, all notifications sent by each Service Provider can be accessed in the same place.

As part of established relationships, IMP clients and Service Providers can securely exchange bidirectional structured data, which along with the advanced interaction capabilities of the IMP client, can be used to create custom interaction scenarios: Service Providers can send structured data to the IMP client along with the information that it should display as a form. Depending on the content of the form and the use case of the Service Provider, the form can, for example, be a purchase agreement or a survey.

Assuming that, through a secure identification and validation process, the identity management provider has made sure that the attributes users store as part of their IMP identity are correct, Service Providers wont require any additional identification steps through for example video calls.

Due to the IMP client being able to automatically fill in the attributes requested as part of a relationship, the user usually wont need to repeatedly manually enter personal information.

In the case of the OZG system architecture, IMP can be used by each member state to individually establish relationships with IMP identities of users to access personal information. This could replace the requirement for user profiles to be interoperable. For the most part, the member states would then be able to operate independently from each other. This solution is described in detail in chapter 4.

Data Protection IMP puts the users back in control of their personal information. As part of the process of establishing a relationship, the Service Provider has to specify exactly which attributes have to be shared, give a detailed explanation of why the attributes are required to be shared, what the purpose of the relationship is and how the attributes are processed. The user can make an informed decision whether to establish the relationship and the Service Provider performs its duty to inform the user as required by the DSGVO.

As personal information is only shared as part of a relationship and with a specified purpose, the Service Provider has an effective tool to differentiate processing legitimisation of attributes based on the type of relationship they are accessible through. This helps the Service Provider in processing personal information according to the DSGVO.

As every relationship is manageable through the IMP client, the user wont loose track of which Service Provider has access to which personal information.

The risk of data being stolen decreases as most of the identity management and data storage is performed by the IMP system and the Service Provider processes only a small portion of the attributes of IMP identities.

In the case of the OZG system architecture, IMP can be used by individual institutions to establish relationships with IMP identities of users to retrieve applications for administrative services. This could eventually eliminate the need for user profiles. Personal information could be shared with only the responsible institution. This solution is described in detail in chapter 5.

Security The IMP client enables users to access their IMP identity and all relationships without the need of remembering a variety of credentials. This removes the risk of credentials being stolen. The IMP client itself can be secured without the need for a password. As the IMP system is capable of signing relationships and exchanged data, the interactions between IMP identity and Service Provider can be validated at any time. This enables both the user and Service Provider to provide proof for every interaction.

3.3 Conclusion

User profile based identity management especially in case of the OZG has several problems in regard to usability, data protection and security. As described, in many cases, IMP has the possibility of solving these issues and eliminating or at least enabling better control over fragmented partial identities. This is the case for interoperable OZG user profiles as well as user profiles in general. Therefore it makes sense to further investigate possibilities of utilizing IMP as a solution to partial identities. Using the small scale model of fragmented partial identities in context of the OZG, the following chapters 4 and 5 present different possibilities of utilizing IMP.

4 IMP Utilization as Extension

This chapter presents an IMP solution which solves issues of user profile-based identity management by enabling users to create, manage, and access user profiles through IMP. For the utilization of IMP services as described by the IMP solution, an integration architecture is presented that enables the OZG system architecture described in section 2.2 to access the IMP system described in section 2.1.

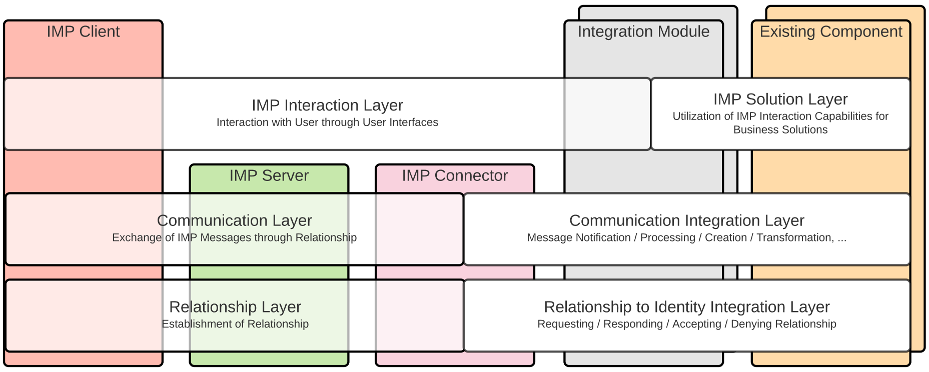
IMP Client
Integration Module
Existing Component
IMP Interaction Layer
Interaction with User through User Interfaces
IMP Solution Layer
Utilization of IMP Interaction Capabilities for Business Solutions
IMP Server
IMP Connector
Communication Layer
Exchange of IMP Messages through Relationship
Communication Integration Layer
Message Notification / Processing / Creation / Transformation, ...
Relationship Layer
Establishment of Relationship
Relationship to Identity Integration Layer
Requesting / Responding / Accepting / Denying Relationship

Figure 4.1: IMP System Layers

As shown in figure 4.1, the integration takes place on three layers:

IMP Solution Layer The IMP solution is integration on the use case level. It presents possibilities of leveraging the interaction capabilities of the IMP system in the context of the Service Provider for the improvement of usability, data protection and security. Furthermore, it describes which types of relationships the Service Provider can use in their business scenario, how relationships can be processed, which types of messages can be exchanged through the relationships, what the purpose of each message can be and how the IMP client can react to different message types.

Technological Integration The Technological Integration is integration on the system level. It consists of an integration architecture enabling the existing systems of the Service Provider to utilize the IMP system as described by the IMP solution. The Technological Integration is separated into a "Communication Integration Layer" and a "Relationship to Identity Integration Layer". On the "Relationship to Identity Integration Layer" the integration architecture enables the existing systems to create relationship templates and establish relationships. On the "Communication Integration Layer" it enables the existing systems to send and receive different types of IMP messages.

4.1 IMP Solution Integration

The IMP solution presented in this section describes the utilization of IMP relationships with the purpose of creating and maintaining OZG user profiles through the IMP client. Message types for attribute synchronization, authentication, and communication are defined. To not disrupt the operation of the existing system architecture, the IMP solution is designed to not replace user profiles but to provide an additional way of accessing them through IMP. To later reduce technological integration efforts, the IMP solution is designed to only require interaction with systems of the portal domain.

4.1.1 Relationship Utilization

The option of using an existing IMP identity for the creation of an OZG user profile is added to the account creation web page of the administration portal. An IMP relationship is used for the account creation process. The web page renders the ID of the following relationship template as a QR-code:

- Title: Create OZG User Profile
- Attributes: Name, Surname, ...
- Shared Attributes: Administration Portal of the member state ...
- Reason: Create an OZG user profile and connect the IMP identity.
- Metadata: «data for technological integration»

Users visiting the account creation web page of the administration portal can use the IMP client to scan the QR code. The IMP client presents the corresponding relationship template to the user and automatically fills in attributes that the administration portal requests from the user as part of the relationship. It is assumed that the IMP system has systems in place for identifying users and validating the personal information of corresponding IMP identities. As a result of that, Service Providers can rely on the validity of shared attributes.

Based on the presented content of the template, the user can make an informed decision on whether to submit a relationship request. If the user submits the request, the administration portal receives it and, based on the attributes shared by the user, decides whether to accept or reject it. If it accepts the relationship request and the user did not retract the request in the meantime, the relationship is established.

Using the personal information shared as part of the established relationship, the portal creates a new user profile and connects it to the IMP identity.

4.1.2 Message Utilization

As part of an established relationship, Service Providers and users can securely exchange structured data in the form of asynchronous messages. Security in this case is defined as that a message can not be accessed or modified by a third party and are authorized by the corresponding user. Based on this secure data exchange capability, Service Providers can define various types of messages, each with different purposes and effects on the IMP client. This section contains various message types useful for managing the user profile created as a result of an established relationship.

Login to User Profile During the user profile creation process using IMP, the user specifies a username but not a password. The IMP client is used for authentication of login requests to the administration portal.

On the login web page of the administration portal, an option is added to login to a user profile using IMP. After entering and submitting the username specified during the profile creation process, the administration portal and IMP client exchange authentication messages. Through the IMP client, the user will be requested to approve a login attempt along with information about the corresponding relationship, IP address, URL, and more.

If the user accepts the request, the administration portal authenticates the browser session.

Attribute Synchronization The IMP client is used for the management of personal information of the user profile. Through the IMP client, the user can send requests for adding, updating, or deleting shared attributes. Administration portal and IMP client exchange attribute change request and reply messages. The requests can either be accepted or rejected by the Service Provider. Accepting the request will result in according modification of the user profile connected to the relationship.

For simplification purposes, the web page for the management of personal information on the administration portal is expected to be read only. However, it would also be possible for the portal to send attribute change requests to the IMP client based on the modifications the user performed on the web page.

Communication The IMP client is used for receiving and displaying mails sent to the user profile. The administration portal forwards mails sent to a user profile to the inbox of the IMP identity corresponding to the connected relationship.

For simplification purposes, the option of the user to send mails to the administration portal is left out.

4.1.3 Evaluation

The approach of this IMP solution is to map partial identities to IMP relationships. This section evaluates the advantages and disadvantages of this approach as well as its application in the OZG context.

Advantages User profiles are known to the existing system architecture and are often used as an identity management solution. Many Service Providers, especially in the private sector, will want to keep using a profile-based identity management approach. The IMP solution presents an opportunity of leveraging existing user profile systems while simplifying identity management through IMP. In addition to that, the IMP solution is designed so that it can almost effortlessly be turned on and off, giving Service Providers the freedom of testing the solution. Service Providers can initially add the IMP solution as an alternative to the conventional user profile identity management solution and after a certain period of time switch to only using the IMP solution.

Mapping user profiles to IMP relationships has many of the usability advantages described in section 3.2. The onboarding process is simplified. Users do not have to manually fill in a form for the creation of a user profile but are supported by the IMP client. As part of established relationships, Service Providers and users are able to directly exchange messages with structured content. In addition to the interaction capabilities of the IMP client, this enables a variety of interaction scenarios not possible through, for example, common e-mail clients. In this case, scenarios for attribute changes, user profile authentication, and communication are made possible.

This approach also increases data protection by providing the user with information on exactly which personal information is shared and how it is being processed as part of the profile creation process. This helps users in making an informed decision on whether to create the user profile. At any time after the onboarding process, users can view the relationship with the IMP client and check which Service Providers process which personal information, why, and how. This enables users to keep an overview of the distribution of their personal information.

Security is also increased as a result of this approach. Through established relationships, Service Providers and users have the ability to not only directly exchange messages but also to do this securely. As a result of that, authentication through the IMP client can replace password-based authentication methods. This eliminates the risk of weak or stolen passwords.

In the case of the OZG, this IMP solution can eventually replace the need for interoperable user profiles. In case each administration portal enables onboarding as described by the IMP solution, regarding usability, the existence of a separation of user profiles can be transparent to the user, but regarding data protection, the user profiles are strongly separated:

After an effortless onboarding process on multiple administration portals, users are able to manage each profile through the IMP client. Logging in to a user profile using the IMP client eliminates the need of remembering passwords, giving the illusion of interoperable user profiles. Finally, if for each user profile, the same profile name is selected, the user wont be able to distinguish OZG user profiles most of the time.

However, in cases where the user requires a distinction between OZG user profiles regarding data protection, the IMP client enables the user to separately view the personal information shared with each portal and information about how each portal processes it.

Disadvantages The IMP solution has also several problems regarding usability and data protection. Most importantly, as a result of integrating the IMP system through user profiles, each administration portal is still required to access personal information. Therefore, the data protection issues described in section 3 remain. In addition to that, application and management of administrative services remains accessible only through the administration portal and form server, which presents a discontinuity in accessing OZG services.

4.2 Technological Integration

In this section, an integration architecture is presented for integration of the IMP system presented in section 2.1 into the existing OZG system architecture presented in section

2.2.

4.2.1 Integration Requirements

Purpose of the integration architecture is to enable the existing OZG system to access IMP services according to the previously described IMP solution. It therefore has to enable the creation of an onboarding relationship template, the processing of onboarding relationship requests, and the processing of established relationships through the creation of user profiles.

In addition to that, it has to enable the definition and utilization of message types listed in the IMP solution. This are messages for attribute change, communication and authentication. As the approach of the IMP solution is the mapping between user profiles and IMP relationships, the integration architecture has to enable an effortless transition between the two entities. OZG system architecture and IMP systems use different data models, especially regarding personal information. The integration architecture therefore has to translate between them. As the IMP connector is not capable of sending asynchronous notifications, the integration architecture has to add this functionality. Depending on the use case of Service Providers, multiple types of relationships or in this case multiple types of user profiles might be necessary. The integration architecture has to enable each type of relationship and user profile to be processed separately, as they might have different processing legitimization. OZG and the presented IMP solution are only one example of a system architecture and IMP use case. The integration architecture should usable in various scenarios. It therefore has to be configurable and expandable to meet new requirements.

4.2.2 Integration Overview

The IMP solution described in the previous section requires the administration portal to access IMP services. As shown in figure 4.2, an IMP connector and a messaging system are added to the administration portal for integration. Using the messaging system, the existing systems of the administration portal and IMP connector can access each others services. IMP server and IMP client of the IMP system as described in section 2.1.3 are also displayed in figure 4.2.

In order for the integration not to be invasive, only the web server and the service facade of the administration portal are connected to the messaging system. All other existing system components remain untouched. Through the service facade, the messaging system can integrate the services of all connected service components.

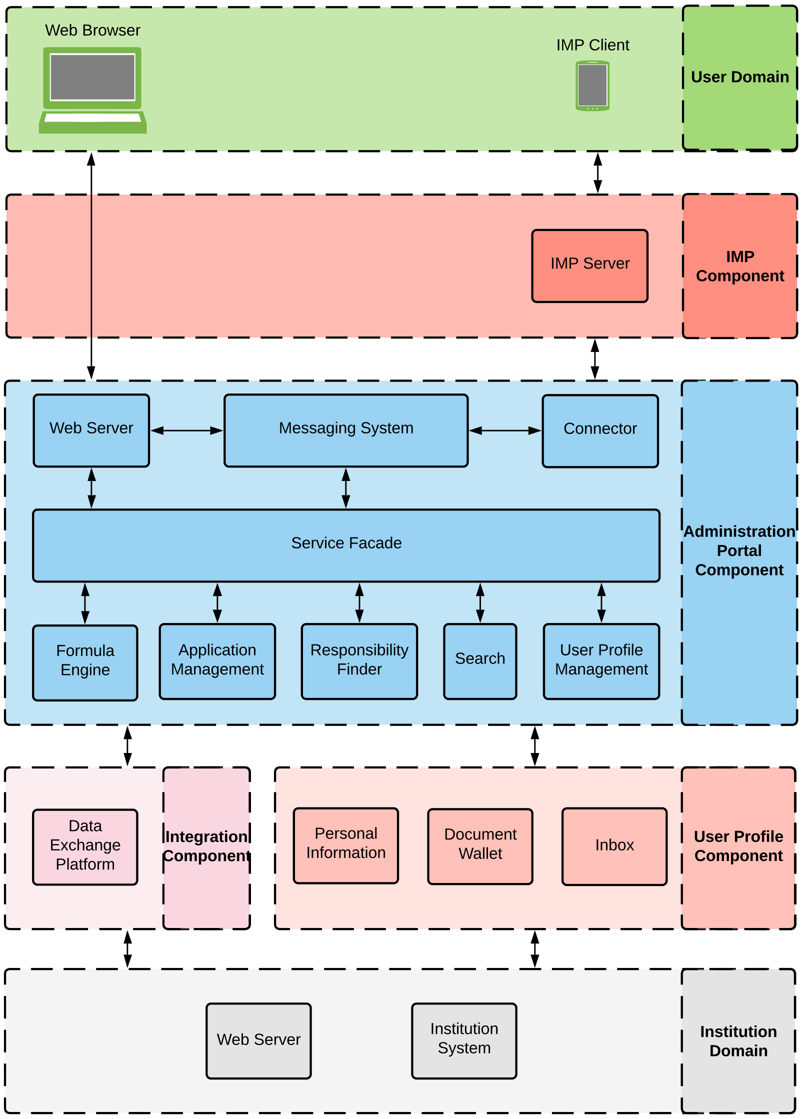

Figure 4.2: IMP Integration for OZG System Architecture

4.2.3 Onboarding Process

This section describes the process of an application for an administrative service as visualized in figure 4.3.

As stated by the IMP solution, the user has to be able to create a new user profile for the OZG system through an existing IMP identity.

On the existing website of the administration portal, where users can create a user profile, the relationship template for onboarding should be displayed. When the web server receives a GET request for the profile creation website, it issues a request to the messaging system for a new onboarding template. The messaging system interacts with

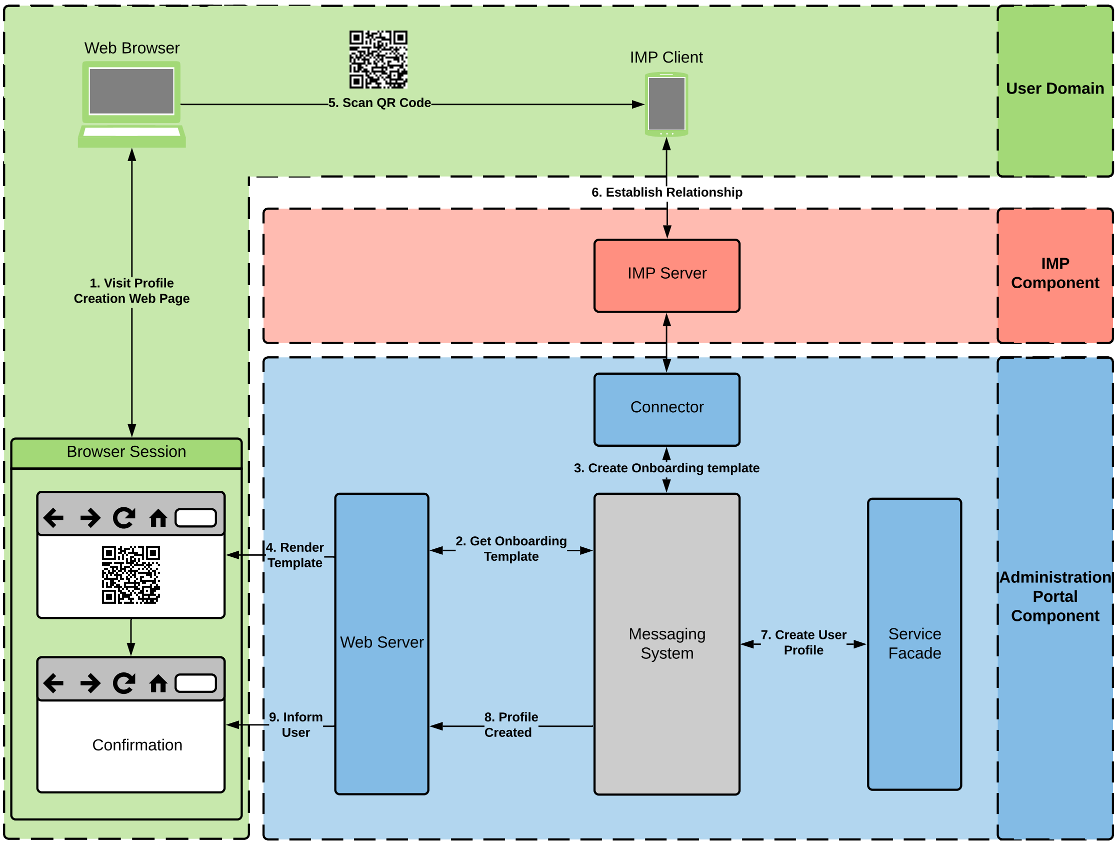

Figure 4.3: User Profile Onboarding Process

the IMP connector to construct the template and send it back to the web server. The web server renders the template as a QR code. The QR code is displayed on the device of the user who can use the IMP client to scan it and initiate a relationship request. The messaging system interacts with the connector to establish the relationship and eventually issues the service facade to create a new user profile based on the attributes shared as part of the IMP relationship.
After successful creation of the user profile, the messaging system stores the relationship ID and the user profile ID in a database. In the future, each request containing either a user profile ID or relationship ID can be mapped to the correct OZG and IMP identities. The messaging system notifies the web server of the successful creation of the user profile and the web server displays a corresponding notification to the user.

4.2.4 Messaging Overview

A messaging approach is used for the technological integration. As described in section 2.3, messaging enables the systems to access each others services in a decoupled way.

This is a useful feature as the integration architecture should be reusable for different system architectures. The messaging patterns described in section 2.3 also enable the integration architecture to be configured according to changes in the operation of the existing systems. The asynchronous nature of messaging systems translates well to the asynchronous and message-based operation of the IMP system and IMP solution.

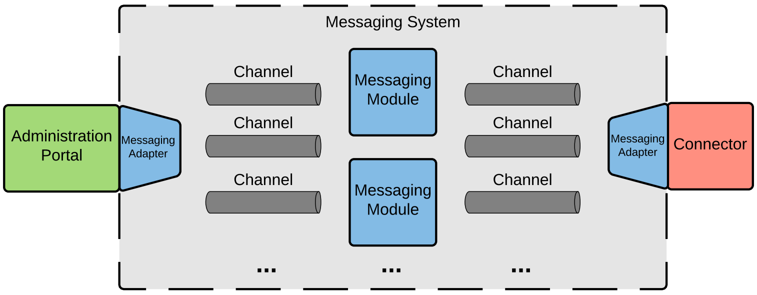

Figure 4.4: Messaging System Layout

The main task of the integration system is to translate between the domain of the existing system architecture and the domain of the IMP system. None of the existing systems can process IMP relationships, but they can process user profiles and vice versa.

As shown in figure 4.4 on the side of the administration portal, messaging adapters provide an API to the existing systems. They give access to IMP services while hiding the technological details of the operation of the IMP system and the underlying messaging system. The adapters communicate with the messaging system through channels. Messages placed on each channel can be simultaneously accessed by multiple systems. Using these channels, message adapters can send requests and replies, and receive replies, notifications, and requests

On the side of the connector, messaging adapters translate the REST API of the connector to a set of publish-subscribe datatype channels. Using these channels, the messaging system can send REST requests by placing messages on channels corresponding to a certain interface. This also enables the messaging system to receive events from the connector.

Messaging adapters do not communicate directly through channels, but with messaging modules. Messaging modules consist of messaging patterns which are able to modify, delete, and route messages. Purpose of the modules is to translate messages sent by messaging adapters of either Service Provider or connector to be understood by the respective recipient. Each module is assigned to an individual integration task. By adding or removing modules, the integration capabilities of the messaging system can be suited to the system architecture of the Service Provider. Modules can be designed to provide services to messaging adapters or other modules. Designing modules specifically for usage by other modules helps in distributing integration responsibilities and avoiding a single monolithic integration component.

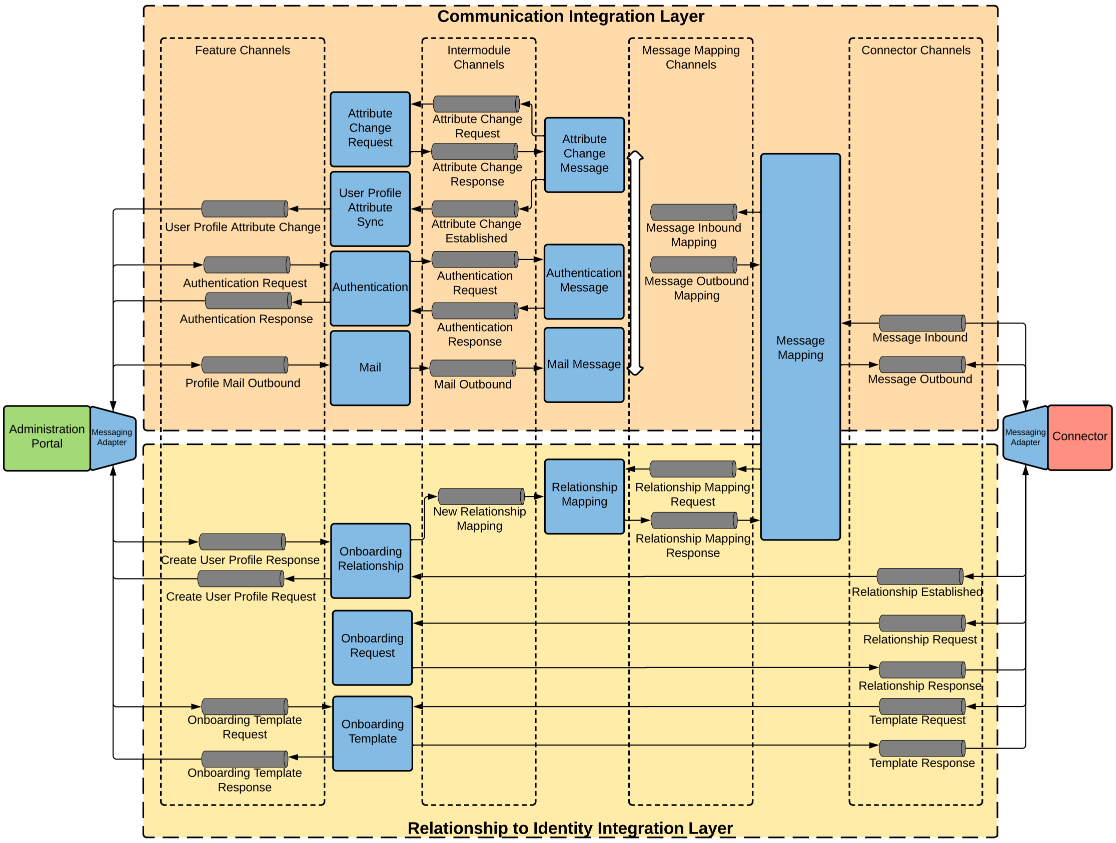

Figure 4.5: Messaging System Detailed Layout

Figure 4.5 gives an overview of the messaging system, which will be discussed in detail in the following sections. The figure contains all channels and messaging modules along with their connectivity.

As introduced in the beginning of this chapter, the technological integration can be separated into two layers: The "Relationship to Identity Integration Layer" and the "Communication Integration Layer" which it is built upon. As described in section 2.1, communication between IMP identity and Service Provider is only possible through an established relationship.

Three messaging modules exist on the "Relationship to Identity Integration Layer", which directly access services of the connector. The onboarding template module provides the feature of creating relationship templates for onboarding. The onboarding request module provides the feature of processing and responding to relationship requests. And the onboarding relationship module provides the feature of processing established relationships by creating a new user profile. The relationship mapping module has the purpose of combining "Relationship to Identity Integration Layer" and "Communication Integration Layer" by enabling the messaging system to map relationships to the corresponding entity of the Service Provider. In this case, the module maps IDs of relationships to IDs of user profiles.

The "Communication Integration Layer" consists of modules that enable the existing systems to exchange structured data with the IMP client. Purpose of the modules is to translate between the data models of the Service Provider and the IMP system. Most importantly, in this case, none of the existing systems is able to understand relationships or relationship IDs. Therefore, the message mapping module has the purpose of translating all incoming relationship IDs to user profile IDs with the help of the previously mentioned relationship mapping module on the underlying layer.
Three message modules are included. Each of them has the purpose of identifying messages of a certain type and separating them into individual channels. This enables the construction of various modules processing the same message types in different ways. Modules that eventually process the messages have the purpose of translating the message content between the data models of Service Provider and IMP system. For example, the mail module consumes messages which contain a mail received by a user profile. It is very likely that the inbox of the user profile and the inbox of the IMP system process mails with different data representation and data types. The mail module therefore has to convert the format of the mail content.

4.2.5 Messaging Modules

In this section, each messaging module mentioned in the overview of the message architecture is described.

Onboarding Template Module To present an onboarding relationship template to the user, the web server first has to retrieve it from the messaging system. For this purpose, an "Onboarding Template Module" is added to the messaging system. Using the API of a messaging adapter provided in addition to the module, the web server can request the creation of new onboarding templates. Optionally, the web server can pass additional attributes which should be stored in the metadata section of the template. The web server will need to notify the user about the successful creation of his user profile and therefore adds the session ID of the user as metadata to the template.

The messaging adapter is aware of the existence of two channels: the "Onboarding Template Request" channel, where it publishes its requests, and the "Onboarding Tem-

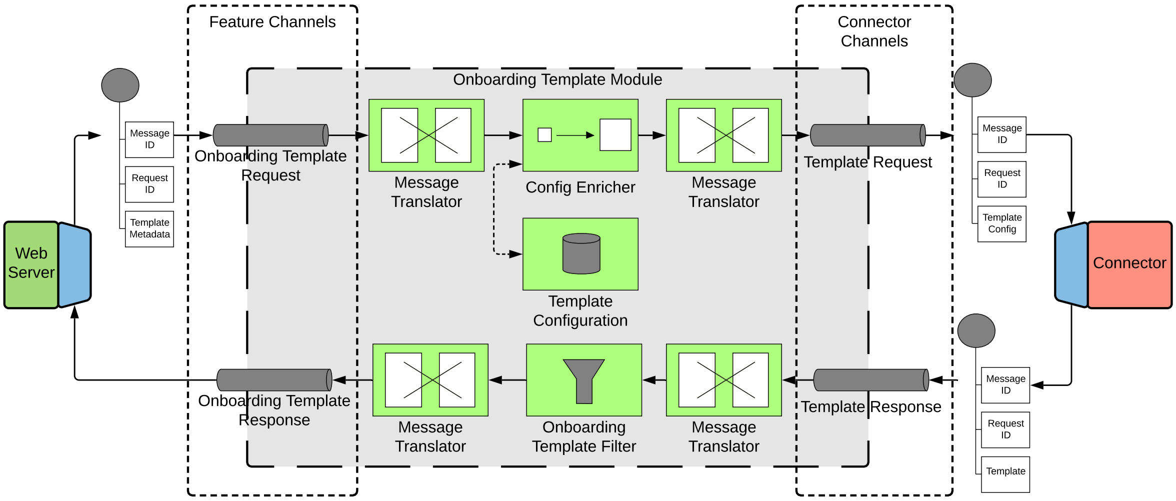

Figure 4.6: Onboarding Template Module

plate Response" channel, where it listens for responses. In order for the adapter to correlate request and reply messages, it creates a message that contains a request ID additionally to the Template Metadata. This ID is expected to be included in the response message. The message ID is a unique identifier and is part of every message. The module consumes messages from the "Onboarding Template Request" channel. On each channel connected to a messaging adapter, message translators are attached. These translators have the purpose of providing a canonical data model within the module by translating messages on the data representation, data type, and data structure layers. It might happen that in the future one of the adapters switches from using, for example, an XML instead of a JSON data representation. Using message translators on each side enables to adapt to these changes by only configuring the translator while leaving the rest of the module untouched.

In between the message translators, the module copies a configuration object stored in a template configuration database into the message and combines it with the template metadata attribute. This configuration contains information on how the relationship templates with type onboarding are supposed to look like. It specifies the title of the template, which attributes will be requested from the user, the reason the attributes are requested, and more. If the content of relationship templates should be changed in the future, depending on the severity of the changes, either a new template module can be created or the configuration stored in the database can be edited. Purpose of the relationship template is to eventually create a new user profile based on the attributes shared by the IMP identity.

Therefore, all attributes that are required to create a user profile have to be requested by the template. In the template, attributes have to be requested according to the data model of the IMP system in order for the IMP client to understand them. When receiving a response later, a module will translate the attributes back to the OZG data model.

After enriching the message with the template configuration, the message is published on the "Template Request" channel. The messaging adapter of the connector consumes the message and issues the appropriate REST request to the connector. After receiving a response from the connector, it publishes the resulting template along with the request ID on the "Template Response Channel". As this channel can contain responses to requests from any amount of modules concerning different template types, the "Onboarding Template Module" filters all incoming messages which contain templates of the type "onboarding" and publishes them on the "Onboarding Template Response" channel.

The messaging adapter consumes the message on the response channel and returns the template to the web server which based on the session ID in the template metadata can display the template as QR code to the user.

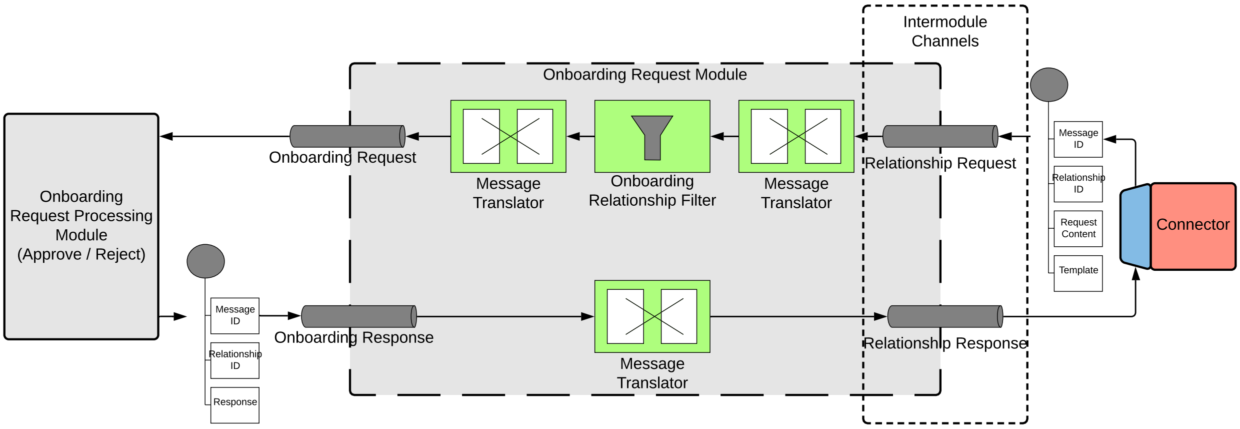

Figure 4.7: Onboarding Request Module

Onboarding Request Module Eventually, the user scans the QR code, fills in the attributes, and submits a relationship request. The request is received by the connector, then forwarded to the messaging adapter and published on the "Relationship Request" channel. The message contains a relationship ID created by the IMP server to uniquely identify the request and the resulting relationship. It also contains the request content with attributes shared by the user and the template the request originated from. Messages on the "Relationship Request" channel are consumed by the "Onboarding Request Module". As in the previous example, message translators are included to construct a canonical data model for the module. A message filter only lets messages through that contain templates of type onboarding. The message translator connected to the "Onboarding Request" channel translates the attributes shared by the user from the IMP data model to the OZG data model.

Based on the attributes the user shares, the OZG system has to decide if the relationship should be established or not. As this process heavily depends on the use case of the relationship and on the Service Provider, the messaging system expects the SP to add a module called "Onboarding Request Processing Module" which consumes the request and responds with either approve or reject on the "Onboarding Response" channel. To correlate the response to the request, the message also has to contain the relationship ID. The "Onboarding Request Module" forwards the response to the "Relationship Response" channel, where the connector will further interact with the IMP system to either establish or cancel the relationship.

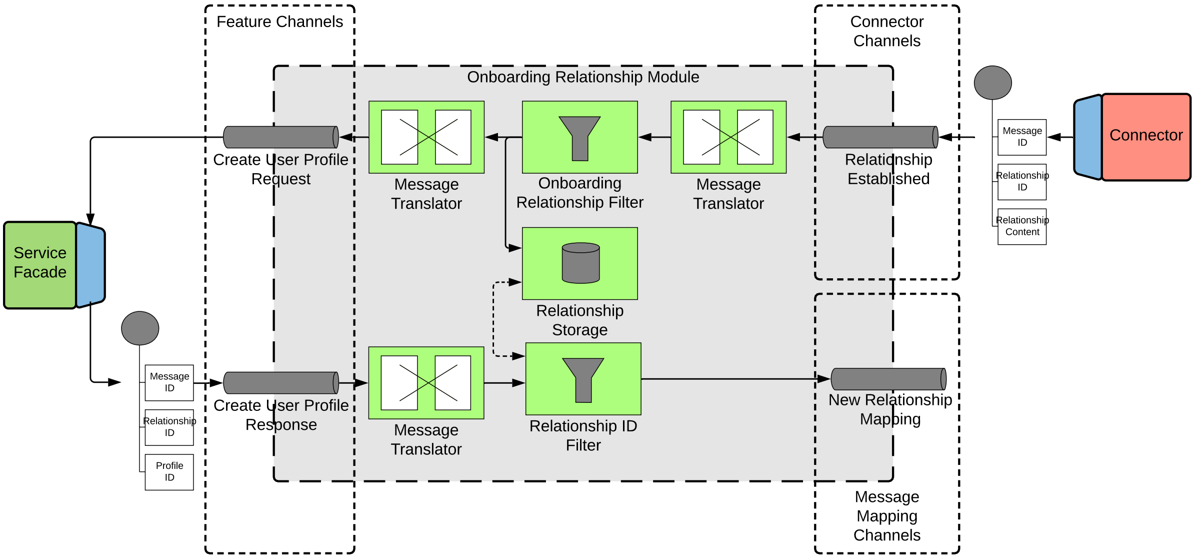

Figure 4.8: Onboarding Relationship Module

Onboarding Relationship Module If the user did not retract their relationship request before the OZG system accepted it, the relationship is established and the connector receives a corresponding notification that the messaging adapter publishes on the "Relationship Established" channel. The message contains the ID of the established relationship along with all attributes shared by the user. The "Onboarding Relationship" module consumes messages from the channel and is responsible for maintaining the state of onboarding relationships. In this case, the module only processes the establishing of relationships, it could however be expanded to process the termination of relationships.

Message translators are inserted again for creating a canonical data model.

The module processes an established relationship by initiating the creation of a new user profile. First, a message filter lets through only messages of type "onboarding". Afterwards, each message is stored in a "Relationship Storage" database and published on the "Create User Profile Request" channel. However, before publishing the message, a message translator maps attributes from the IMP data model to the OZG data model.

To create a user profile, a messaging adapter attached to the service facade of the administration portal consumes messages from the "Create User Profile Request" channel and issues the corresponding requests to the service facade for creating a new user profile based on the attributes stored in the relationship content. After successful creation of the user profile, the messaging adapter publishes a response message on the "Create User Profile Response" channel which contains the relationship ID and the newly created user profile ID.

As responses to requests from other modules might be published on this channel, the "Onboarding Relationship" module filters all messages which do not contain a relationship ID stored in the "Relationship Storage". The module then publishes the response on the "New Relationship Mapping" channel.

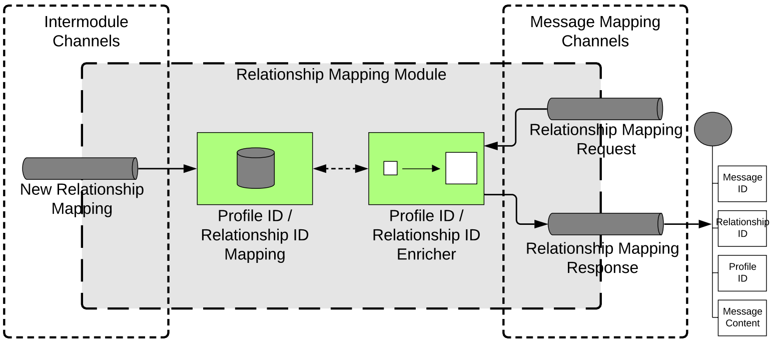
Intermodule Channels
Message Mapping Channels
Relationship Mapping Module
Relationship Mapping Request
New Relationship Mapping
Profile ID / Relationship ID Mapping
Profile ID / Relationship ID Enricher
Relationship Mapping Response
Message ID
Relationship ID
Profile ID
Message Content

Figure 4.9: Relationship Mapping Module

Relationship Mapping Module Through the "New Relationship Mapping" channel the "Relationship Mapping" module receives the messages sent by the previously described module. Purpose of the "Relationship Mapping" module is to map relationships to corresponding entities in the existing system architecture. In this case, relationships are mapped to user profiles and vice versa using relationship IDs and user profile IDs. The message consumed through the "New Relationship Mapping" channel is stored in a database for enabling future translation between the contained relationship ID and user profile ID. Using the "Relationship Mapping Request" channel modules can request the "Relationship Mapping" module to add a user profile ID for a given relationship ID and vice versa.

Using messaging for this form of database access enables modules to stay unaware of the complexity of the underlying data storage mechanisms. An alternative would be for modules to use the database as a shared database.

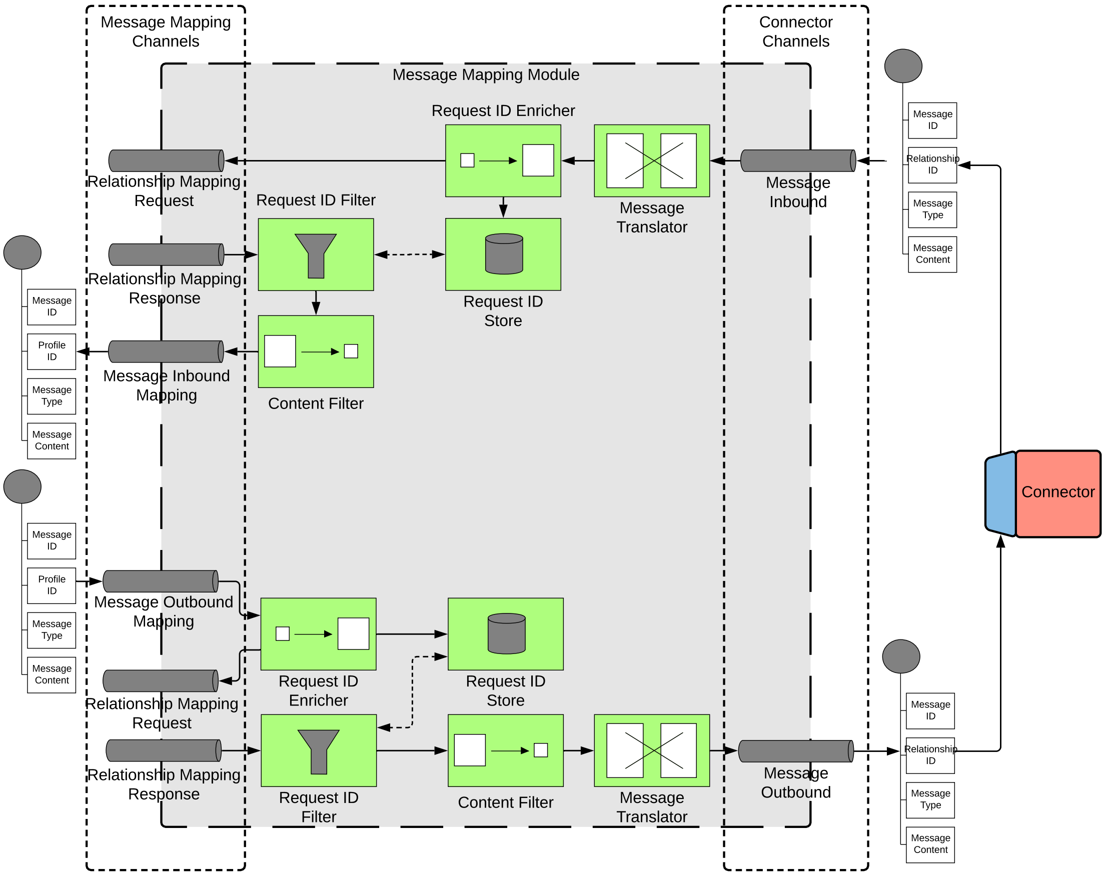

Figure 4.10: Message Mapping Module

Message Mapping Module Using the previously defined "Relationship Mapping" module, the "Message Mapping" module has the purpose of translating the relationship ID of all inbound messages to the corresponding user profile ID and translating the user profile ID of all outbound messages to the corresponding relationship ID. As a result of that, on the left side of the figure 4.10, messages coming from or going to the existing system architecture contain the identification of the known user profile entity instead of the unknown relationship entity. On the right side, messages coming from or going to the IMP system contain the identification of the known relationship instead of the unknown user profile.

Incoming messages on the "Message Inbound" channel are consumed by the module and translated by a message translator to a canonical data model. In order for the module to identify a response after publishing the message on the "Relationship Mapping Request" channel, a Content Enricher adds a unique request ID to the message and stores the ID in a database. Only messages on the "Relationship Mapping Response" channel containing a request ID stored in the database are let through by the request ID message filter. As the following systems will process the inserted user profile ID instead of the relationship ID, a content filter removes the relationship IDs from the message before publishing it to the "Message Inbound Mapping" channel.

Outbound messages on the "Message Outbound Mapping" channel are processed similarly to inbound messages. The difference is that the user profile ID contained in the message is replaced by the corresponding relationship ID.

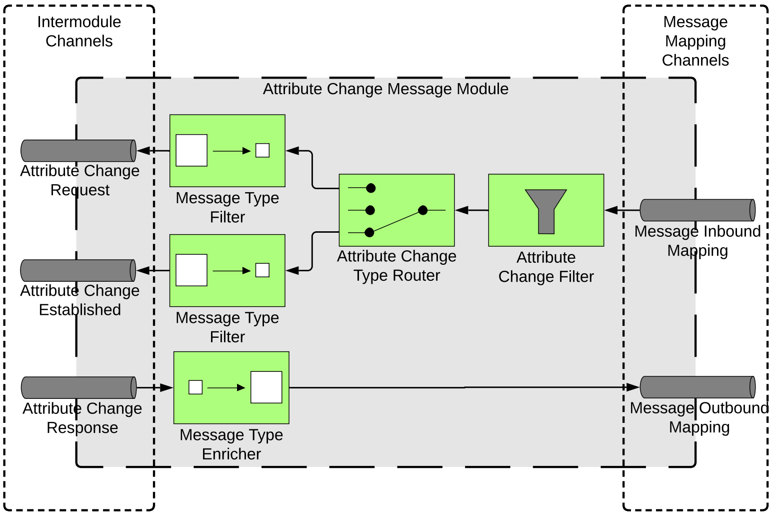

Figure 4.11: Attribute Change Message Module

Attribute Change Message Module For the messaging system, to process messages being exchanged as part of relationships, message modules can be added. Their purpose is to map messages of certain types from the "Message Inbound Mapping" channel to individual message type channels so that the modules can process them. They also map messages from the individual message type channels to the "Message Outbound Mapping" channel so that the connector can submit them.

In this case an "Attribute Change Message Module" is included, which processes messages related to the attribute change process. Messages exchanged through IMP relationships can have arbitrary content. However, the messages are assumed to contain a message type attribute and a message content attribute. Based on the message type attribute, a message filter can let messages through that contain a message type attribute correlating to an attribute change process. Based on the type of a message, a content-based message router then copies each message to a datatype channel. In this example, messages with the type "attribute change request" and "attribute change established" are distinguished. Corresponding to that, two data type channels exist. As the type of a message can be inferred from the channel it is placed on, content filters can remove the message type attributes.

Outbound messages related to the attribute change process are consumed in data type channels. In this case, it is only one "Attribute Change Response" channel. A Content Enricher adds a message type attribute correlating to the channel the message was placed on. This is required in order for the IMP client to properly interpret the message. After that, the message is published on the "Message Outbound Mapping" channel.

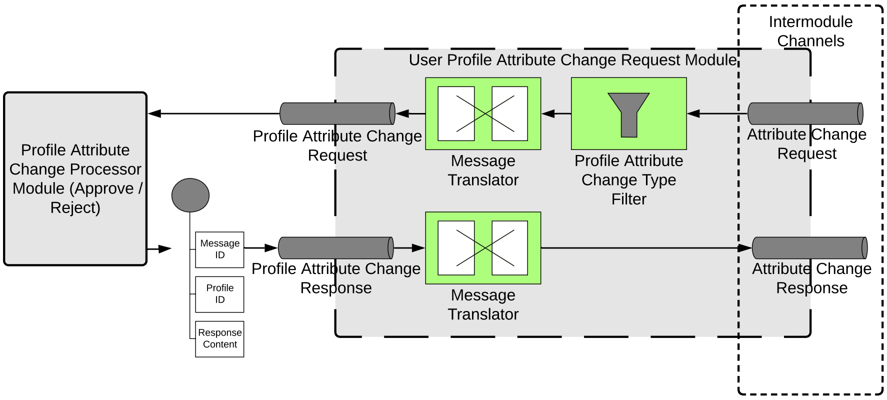
Intermodule Channels
User Profile Attribute Change Request Module
Profile Attribute Change Processor Module (Approve / Reject)
Profile Attribute Change Request
Message Translator
Profile Attribute Change Type Filter
Attribute Change Request
Message ID
Profile ID
Response Content
Profile Attribute Change Response
Message Translator
Attribute Change Response

Figure 4.12: Attribute Change Request Module

User Profile Attribute Change Request Module To process incoming attribute change requests for profiles, a "User Profile Attribute Change Request" module is included, which consumes messages from the "Attribute Change Request" channel. Messages arriving on the "Attribute Change Request" channel were mapped from a relationship ID to a user profile ID in an earlier integration step. Depending on the use case of the Service Provider, not all attribute change requests for user profiles should be processed in the same way. Therefore, message filters are inserted which are able to distinguish possible "types" of user profiles based on the user profile ID. It would also be possible to include an additional module that is able to request user profile type information from the existing systems, separating messages on the "Attribute Change Request" channel appropriately. For example, user profiles for businesses could exist, where processing of attribute change requests requires a more thorough and manual verification by employees.

In the example at hand, however, only one module processes attribute change requests. To translate the canonical data model into the data model of the OZG, a message translator is included. This concerns especially the attributes shared as part of the attribute change request.

Similar to the "Onboarding Request Module", the decision whether to approve or reject an attribute change is specific to the Service Provider. Therefore, the SP is expected to include a "Profile Attribute Change Processor" module, which decides to approve or reject the request based on the user profile ID and the shared attributes. The response is published on the "Attribute Change Response" channel and contains the user profile ID additionally to the response.

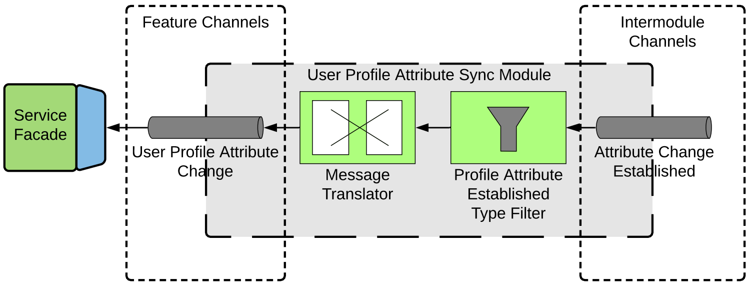
Feature Channels
Intermodule Channels
User Profile Attribute Sync Module
Service Facade
User Profile Attribute Change
Message Translator
Profile Attribute Established Type Filter
Attribute Change Established

Figure 4.13: User Profile Attribute Sync Module

User Profile Attribute Sync Module If the user does not cancel the attribute change request before the OZG system accepts it, the attribute change is established. The connector is notified through a message, which eventually is processed by the "User Profile Attribute Change Message" module described earlier and published on the "Attribute Change Established" channel.

The "User Profile Attribute Sync" module consumes messages from the "Attribute Change Established" channel. Similar to the "User Profile Attribute Change Request" module, a message filter is inserted for distinguishing possible user profile types based on the user profile ID. A message translator is inserted to translate the message content to the OZG data model. This concerns especially the attributes shared as part of the "attribute change established" message.

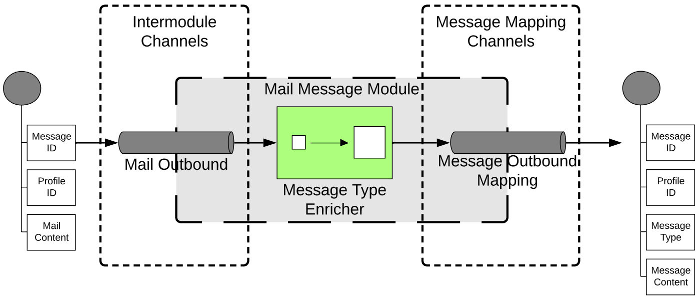

Figure 4.14: Mail Message Module

Mail Message module In order for the user to receive messages sent to their user profile through the IMP client, mail messages are processed by the integration architecture. Similar to the "Profile Attribute Change Message" module, a "Mail Message" module is included, which maps messages on the "Mail Outbound" channel to the "Message Outbound Mapping" channel.

In this module, incoming mails from the IMP client could also be processed.

Before publishing messages on the "Message Outbound Mapping" channel, a Content Enricher adds the implicit message type of the channel as an attribute in order for the IMP client to understand it.

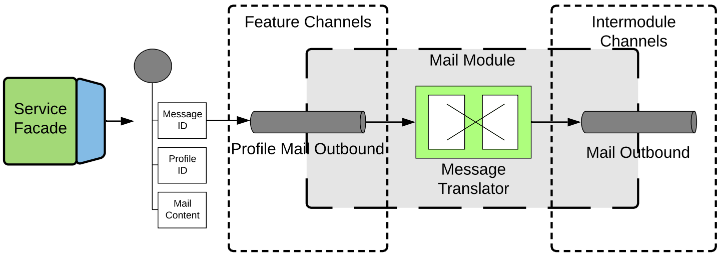

Figure 4.15: Mail Module

Mail Module A messaging adapter attached to the service facade is notified each time a user profile connected to an IMP identity receives a mail and publishes a message on the "Profile Mail Outbound" channel. The message contains the ID of the profile which received the message and the content of the mail.

A "Mail" module is included which consumes the messages from the "Profile Mail Outbound" channel. A message translator is inserted, which translates the mails from the OZG data model to the IMP data model and publishes them on the "Mail Outbound" channel.

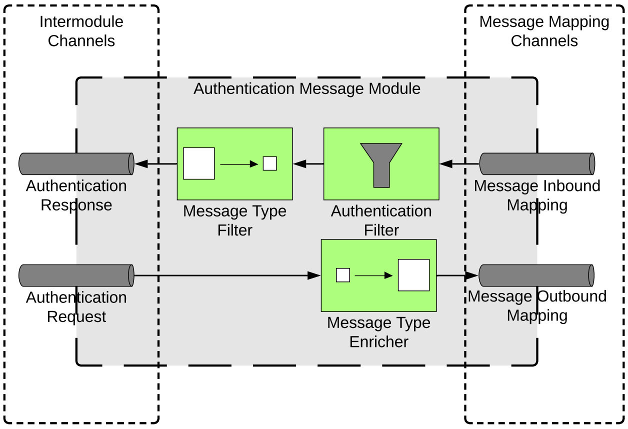

Figure 4.16: Authentication Message Module

Authentication Message Module If the user creates a user profile using their IMP identity, it is possible to replace password authentication with an authentication through the IMP client. It is also possible to use the IMP client for two-factor authentication.

To send and receive messages related to authentication, similar to previous message modules, an "Authentication Message" module is included, which maps incoming messages on the "Message Inbound Mapping" channel to the "Authentication Response" channel and outgoing messages from the "Authentication Request" channel to the "Message Outbound" channel.

Authentication Module When the users visit the web page of the administration portal to apply for an administrative service, they will have to login. To utilize the IMP client for authentication, the web server can use a channel adapter to publish an authentication request concerning a user profile ID and a certain session ID. The adapter publishes a message on the "Authenticate" channel which contains the profile ID and a request content. Next to the session ID, the request content may also include information for presentation to the user like the current time or the IP address of the browser. Similar to the previous modules, a message translator is inserted to translate

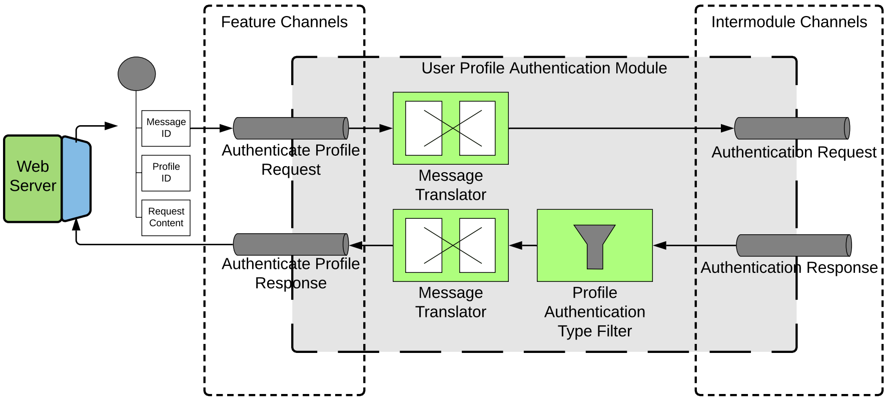

Figure 4.17: Authentication Module

the message to a canonical data model and publish it on the "Authentication Request Message" channel.

Eventually, the IMP client sends a response as a message, which the "Authentication Message" module publishes on the "Authentication Response" channel. Similar to previous modules, the Service Provider can use a message filter to process user profile types differently. After translating the message to the OZG data model, it is published on the "Authenticate Profile Response" channel. The channel adapter of the web server receives the message and based on the session ID contained in the response content can authenticate the browser session.

4.2.6 Evaluation

The messaging system and the modular approach make the integration architecture expandable and configurable for new integration scenarios. Message mapping module and relationship mapping module enable the translation between user profile and relationship. Onboarding template, onboarding request, and onboarding relationship module enable the definition and utilization of one or more relationship types. Message modules enable the definition of message types. Message processing modules enable the translation between data models. Messaging system enables asynchronous, event-based, and direct communication between users and Service Providers. Assigning special modules to each type of relationship and message type enables the separation of processing depending on differences in processing legitimization.

5 IMP Utilization as Replacement

This chapter presents an IMP solution which focuses on data protection by replacing user -profile-based identity management and only temporarily sharing personal information for individual business processes. The IMP solution is integrated using the same messaging system as described in section 4.2.

5.1 IMP Solution Integration

The main issue of the IMP solution presented in chapter 4 is the utilization of user profiles and the resulting lack of data protection. The IMP solution described in this chapter puts the institutions in the center of integration to eliminate the need for user profiles and administration portals to process personal information.

5.1.1 Relationship Utilization

As part of the existing operation of the OZG system architecture, applications submitted to administration portals will eventually be transferred to responsible governmental institutions. Using IMP relationships can be used to send applications directly to institutions without the need for an administration portal, form server or data exchange platform.

Each institution has a predetermined set of administrative services it can process. For each administrative service, the institution can create a relationship template, containing the description of the service, the list of attributes required from the user necessary for processing the application, and information on how the personal information will be processed:

- Title: Apply for administrative service XYZ
- Attributes: Name, Surname, ...
- Shared Attributes: Institution Name ...
- Reason: Apply for the administrative service XYZ ...

In contrast to the relationship templates in the previous IMP solution, these will not have to be dynamically created but only once. The reason is that in the previous IMP solution templates had to contain personalized information like the session ID. This is not necessary in this case.

Once the templates are created, the corresponding template IDs can be rendered as QR code on the web page of the institution. If the content of a template has to be changed, an employee can manually create a new template and switch the template IDs on the web page.

Visiting the web page of the institution, the user can scan the QR code and the corresponding relationship template for an application is shown. The user can read through the included description of the corresponding administrative service to determine if it is the correct one. Based on the requested attributes and the information on how they are processed, the user can make an informed decision whether to apply for the administrative service.

When sending the relationship request, the institution directly receives it without an administration portal being involved. Based on the shared attributes, the institution can decide to either accept or reject the application request. It might, for example, verify whether the home address of the user is within the area that it is responsible for.

When accepting the application request and therefore the whole relationship, and if the user did not retract his request in the meantime, the relationship is established and the institution gets notified about a new application.

After the administrative service is finished, the relationship can be terminated and the institution loses access to all shared personal information.

However, the administration portal cannot be completely replaced. It is still required by users for directing them to the correct institution based on the selected administrative service and, for example, their home address. Therefore, users visiting any administration portal search for an administrative service and specify their home address. The administration portal is able to determine the responsible institution and forward the user to an URL provided by the institution.

5.1.2 Message Utilization

This IMP solution utilizes the same message types as the previous IMP solution, however, for a different purpose.

Attribute Synchronization Through the IMP client, users can request attribute changes for established relationships. The purpose of these messages is to enable users to change the content of an application even after it was submitted.

Communication As in the previous IMP solution, users should be able to receive mails from every institution through the IMP client. Each mail is associated with a relationship, enabling the user to easily correlate mails to active applications.

Authentication As no user profiles are necessary in this IMP solution, users will not have to use the IMP client for logging into a user profile. However, authentication messages can still be used as an accept / reject based communication method.

5.1.3 Evaluation

The approach of this IMP solution is to map temporary business processes to IMP relationships. This section evaluates the advantages and disadvantages of this approach as well as its application in the OZG context in comparison to the previous IMP solution.

Advantages As a result of mapping IMP relationships to individual business processes, the user has more granular control of sharing personal information. Compared to the previous IMP solution, the user does not give general access to personal information for creating a user profile but for individual processes. The users can better control whether they agree to share personal information for processing an administrative service, while in the previous IMP solution the IMP client was not involved. In the case of the OZG, the user profile component did require authentication prior to sharing attributes with administration portals, but this might not be the case for all Service Providers.

Using relationships for the execution of business processes eliminates the need for Service Providers to operate identity management systems. It is sufficient to integrate the identity management capabilities of the IMP system according to the IMP solution. This leaves the Service Provider with the main task of executing the business processes.

The IMP solution enables users to share personal information directly with responsible institutions, restricting access to, for example, administration portals. It also enables direct and secure exchange of messages. As a result of the direct mapping of relationships to applications, users can request the modification of application content even after submission.

The IMP solution can also operate alongside the previous IMP solution and eventually replace it.

Disadvantages The disadvantage of this IMP solution is the invasive integration which does not only provide an alternative way of accessing existing systems but for the most part completely replaces them.

5.2 Technological Integration

This section presents how the messaging system described as part of the previous chapter can be reused for the IMP solution of this chapter.

5.2.1 Integration Requirements

The focus of the technological integration is to use the messaging system as described in section 4.2 to integrate the new IMP solution into the different system architecture of institutions. The layout of the messaging system should not change and the purpose of each module should stay the same. To adapt the architecture to the new system architecture and IMP solution, the modules can be configured and named differently.

5.2.2 Integration Overview

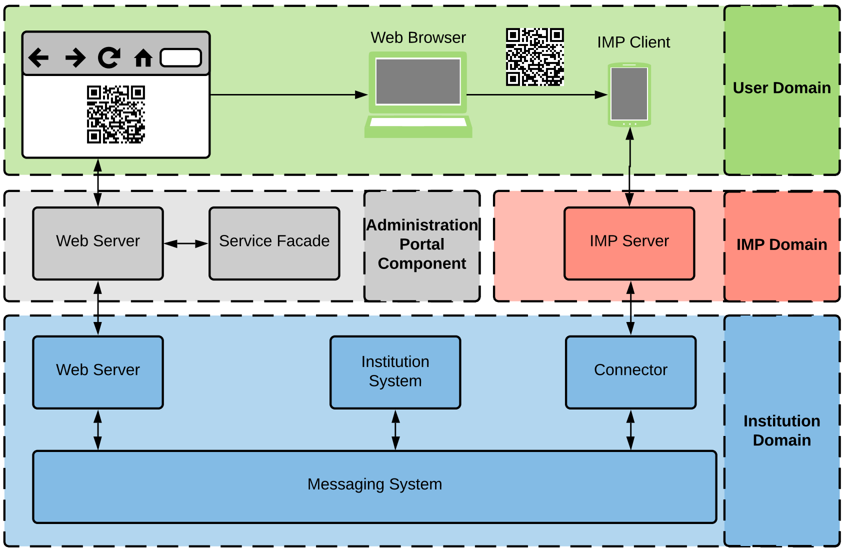

Figure 5.1: Integration Overview

As shown in figure 5.1, to implement the IMP solution, a connector as well as the messaging system described in section 4.2 is included in the existing system architecture of each institution. Instead of the web server and service facade in the portal domain, the messaging system is connected to the web server and institution system of the institution domain.

As shown in figure 5.2, the layout of the messaging system is identical to the one presented in section 4.2. The same type of messages are exchanged with a slightly different purpose and content. Therefore, in this and the following sections, only the important differences between the operation of the messaging system will be detailed.

On the "Relationship to Identity Integration Layer" modules exist for establishing different types of application relationships. For simplification, only modules for an exemplary application process "Application A" are shown. Although the content and purpose of the relationships in this case are different to the relationships of chapter 4, they are processed the same: each type of relationship request is processed by an individual application request module and each type of established relationship is processed by an individual application relationship module. As the purpose of relationships in this case are applications for administrative services, each module has to be configured appropriately. For an established relationship, instead of issuing the existing system architecture to create a user profile, the application relationship module issues the existing system architecture to process an application based on the attributes shared as

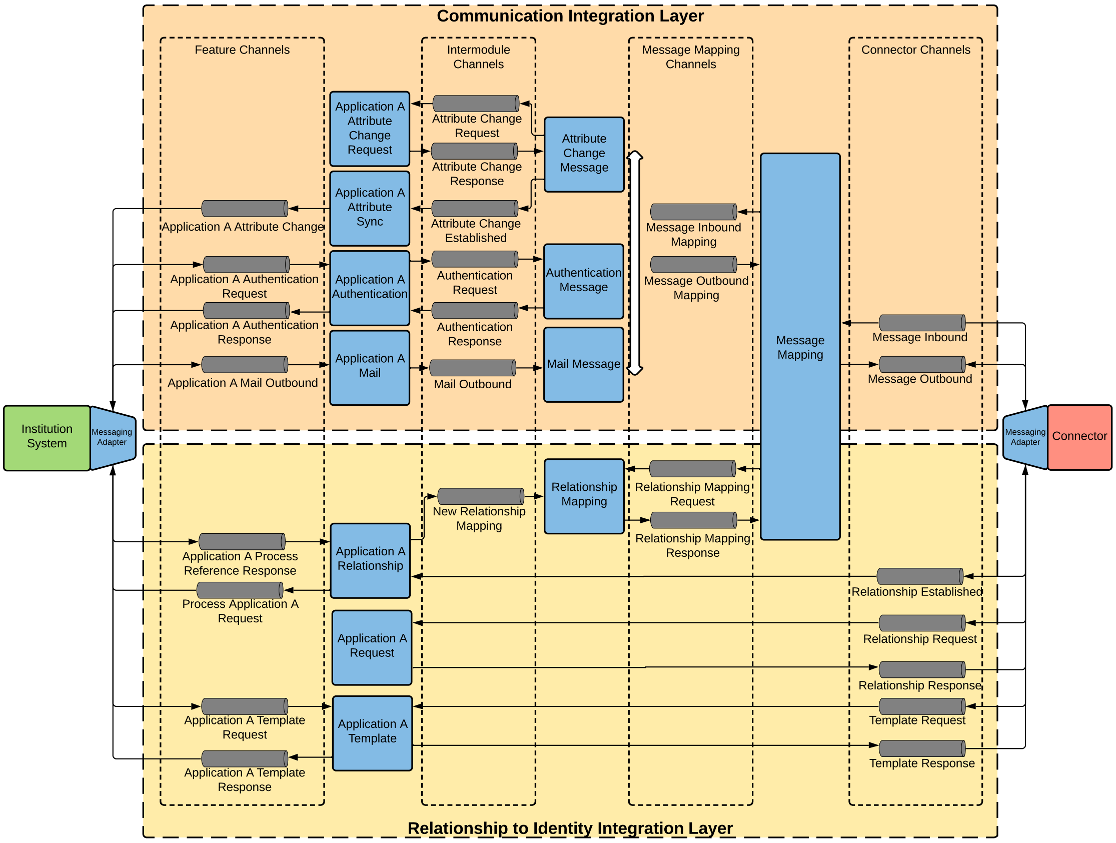

Figure 5.2: Messaging Overview

part of the relationship. Moreover, instead of a user profile ID, the existing system architecture responds with an application process ID. This application process ID is used in the same way the user profile ID is utilized in section 4.2. Through the "New Relationship Mapping" channel, it is sent to the relationship mapping module, which maps each relationship to an application process and vice versa.

On the "Communication Integration Layer" the same types of messages are exchanged. However, instead of user profile IDs, relationship IDs are mapped to application process IDs. In chapter 4, each module connected to the messaging adapter of the institution system was designed to be able to distinguish between different types of user profile IDs to, for example, distinguish an enterprise profile from the profile of a private person. In this case, modules can distinguish between different application types based on the application process ID.

5.2.3 Application Process

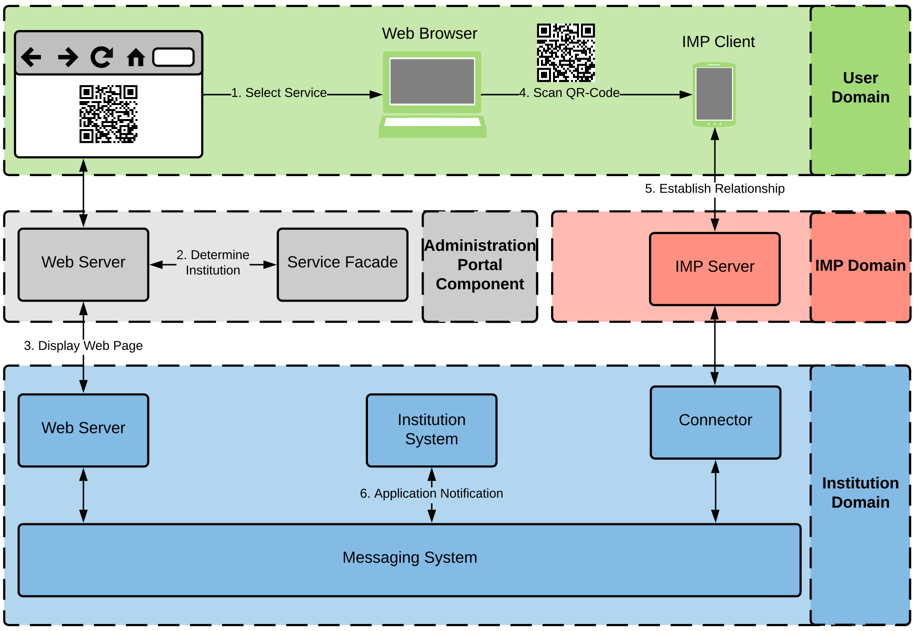

Figure 5.3: Administrative Service Application Overview

This section describes the process of applying for an administrative service as shown in figure 5.3. Institutions are able to process a predetermined set of administrative services. For each service, the institution can create a relationship template once and store it as QR code on their web page. Users visiting an administration portal can select an administrative service, specify their home address, and be forwarded to the web page of the respective institution. After scanning the appropriate QR code with the IMP client, the user can fill in the requested attributes and send the relationship request. After the relationship is established, the institution is notified and starts processing the application utilizing the shared attributes.

5.2.4 Messaging Modules

In this section, each messaging module mentioned in the overview of the message architecture is described.

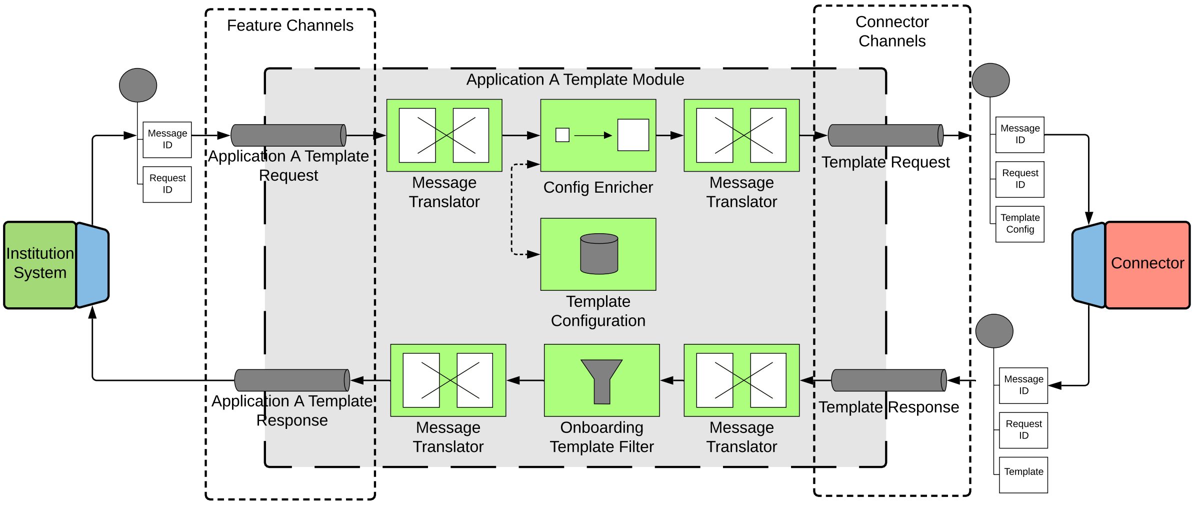

Figure 5.4: Application Template Module

Application Template Module Relationship templates are created manually and stored as a QR-code on the web page of the institution. For each application type, a separate application template module can be included, which stores the configuration for the template type and issues the connector to create new relationship templates. Instead of the web page, the institution system itself is connected, as application templates are not dynamically created for user requests but only once by an employee of the institution. Each time the content of an application template has to be changed, the institution creates a new one with this module.

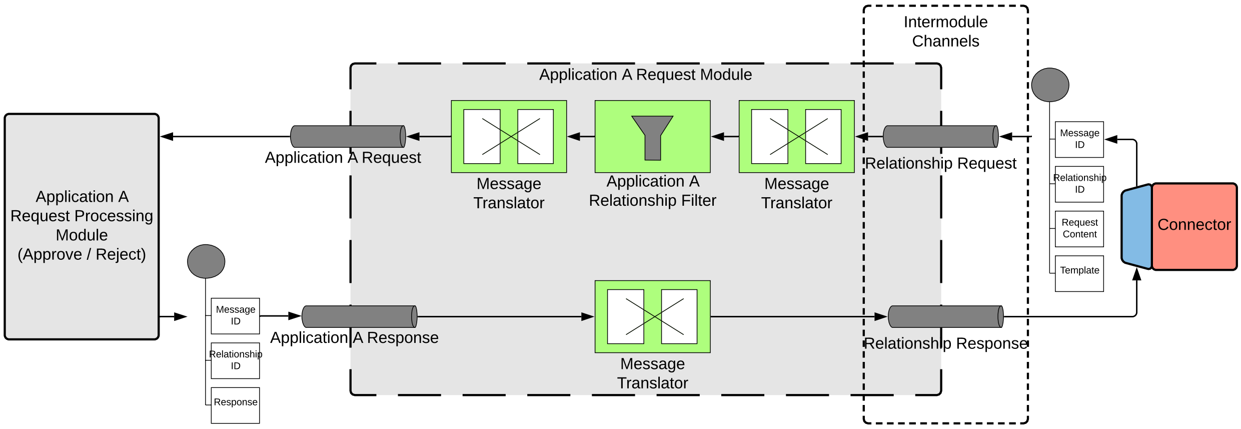

Figure 5.5: Application Request Module

Application Request Module For each type of application relationship, a different application request module is used to separate the processing of requests for different application types into application request processing modules. Depending on the type of application, different requirements regarding the acceptance of application requests exist. A request processing module might, for example, check if the home address of the user is within the area of responsibility of the institution. Only after the relationship and therefore the application request is accepted, the application will be processed.

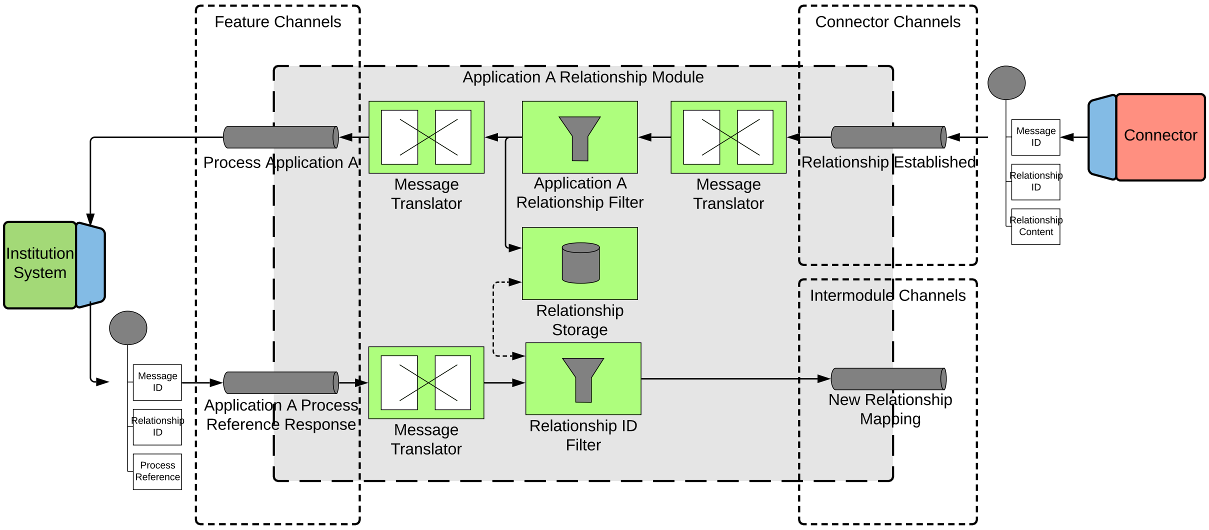

Figure 5.6: Application Relationship Module

Application Relationship Module For each type of application relationship, a different application relationship module is used for processing the established relationships. The institution system is notified of an accepted application through the "Process Application Request" channel. As part of the existing system architecture, institution systems receive applications through the data exchange platform as an application document. To adhere to this standard, the message translator connected to the "Process Application Request" channel translates the relationship content into the application format of documents delivered through the data exchange platform.

Institution systems are assumed to uniquely reference active applications with process IDs. After starting the application process, the institution responds through the messaging adapter with the process ID on the "Application Process Reference Response" channel. This process ID is then published to the "New Relationship Mapping" channel. In contrast to the messaging system of chapter 4, the relationships in this case are not mapped to user profiles but to application processes.

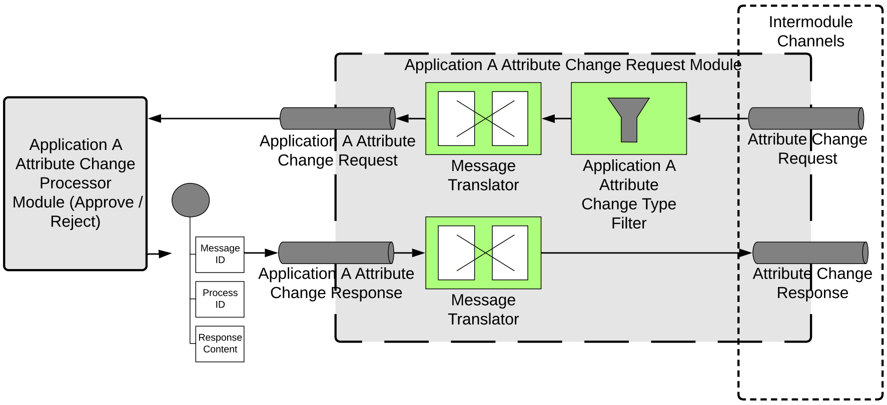
Intermodule Channels
Application A Attribute Change Request Module
Application A Attribute Change Processor Module (Approve / Reject)
Application A Attribute Change Request
Message Translator
Application A Attribute Change Type Filter
Attribute Change Request
Message ID
Process ID
Response Content
Application A Attribute Change Response
Message Translator
Attribute Change Response

Figure 5.7: Application Attribute Change Request Module

Application Attribute Change Request Module As an example, for a message type processed on the "Communication Integration Layer", the application attribute change messages are selected.

Similar to the process in chapter 4, attribute change message types are published on individual channels, this time however, instead of a user profile ID, they contain a process ID. As described in the example of different user profile ID types in chapter 4, different process ID types may exist in this case too. For example, an attribute change request for an application of type "A" might be processed differently to an attribute change request for an application of type "B". To process different types of attribute change requests separately, multiple application attribute change request modules can be included, each of them filtering for different types of process IDs. If it is possible to retrieve the application type from the process ID, the processing of each application type could be separated into multiple application change request modules. For the case that application types are not retrievable from process IDs, an additional module can be included, which requests the application type from the institution system based on the process ID. An alternative way would be for the application relationship module to not only publish the process ID corresponding to a relationship ID on the "New Relationship Mapping" channel but also the application type.

Only when the attribute change request is accepted, the institution system will be notified about the attribute change.

Application Attribute Sync Module Continuing the example of how application attribute change messages are processed on the "Communication Integration Layer", the application attribute sync module processes messages on the "Attribute Change Established" channel. With the same reasoning as in the previous section, the message filter attached to the channel enables to include multiple application attribute sync modules, each processing different application types.

The institution system receives the notification from the application through the messaging adapter. Depending on the capabilities of the institution system, this could result in either an automated update of the referenced application process or an automated e-mail to the assigned employee.

Application Mail Module Similar to attribute change messages, mail messages can be fitted to the process-based scenario, enabling institutions to send mails to a process ID which the messaging system translates to a relationship ID in order for the correct IMP identity to receive it. In addition to the one-directional message transfer from the institution to the IMP identity, the application mail module and the mail message module could be expanded to be able to receive mails from an IMP identity through an established relationship. The relationship ID of the message would be mapped to the corresponding process ID and submitted to the institution system. The institution system could then send the mail to the responsible employee.

Application Authentication Module Authentication messages and modules are not required for this IMP solution, as no user profile and therefore no login process exists. However, depending on the use case, authentication messages could be included as an additional accept / reject communication method between the institution and user.

5.2.5 Evaluation

The integration architecture enables users to directly interact with the system architecture of the Service Provider for submitting applications. This eliminates the need for administration portals to process personal information. As shown in figure 5.8, every component and every domain of the existing OZG system architecture processes personal information. Using the IMP solution presented in this chapter, only the user and the responsible institution have access to personal information, which improves data protection.

The integration architecture described in section 4.2 was able to integrate into two different system architectures. This demonstrates that the presented integration architecture is applicable to a variety of system architectures. In addition, it was able to integrate a user-oriented (persistent) relationship scenario as well as a process-oriented (temporary) relationship scenario. This demonstrates that the presented integration architecture can be used for integrating a variety of IMP solutions. The modular message-

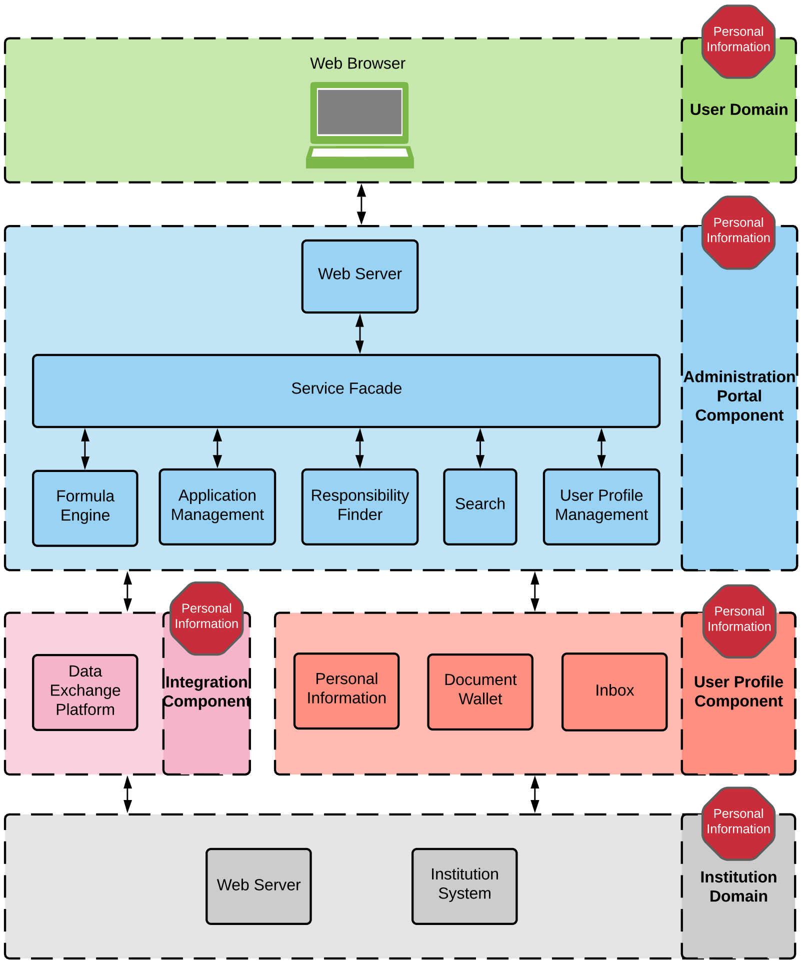

Figure 5.8: OZG System Architecture Personal Information

based approach makes it possible to use the integration architecture in different scenarios by enabling easy configuration of modules for new requirements.

6 Conclusion

Finally, this chapter summarizes the most important results of this thesis and gives an outlook on possible future developments and contributions.

6.1 Summary

The bachelor thesis uses the scenario of the OZG as a small-scale model for the general problem of distributed partial identities. Focus is the utilization and system integration of IMP for Service Providers with existing user profile-based system architectures.

The first objective of the bachelor thesis is to examine the problems of user profile-based identity management and interoperable OZG user profiles and to describe to what extent IMP can be a solution. In chapter 3 the thesis describes multiple problems of user profile-based identity management regarding usability, data protection and security. They lack usability as they lead to fragmentation into partial identities, accessible only through separate applications and web pages. Data protection is reduced due to the lack of oversight for the user about existing user profiles and shared personal information. The distribution of personal information to various Service Providers increases the risk of data being stolen. Especially in the case of the OZG, issues regarding data protection exist:
As a result of the "one-for-all" method, access to administrative services is distributed across multiple administration portals. Users applying for services therefore have to share large quantities of personal information with the administration portals of multiple federal states. As it is the institutions and not the administration portals that eventually process the personal information, sharing personal information directly with institutions would be favourable regarding data minimisation.
Possibilities for solving the mentioned problems through IMP are presented. IMP enables to increase usability by enabling users to interact, manage, and share personal information with Service Providers through only one application. Data protection is increased, as users can keep an overview of shared personal information. Security is improved, as IMP provides secure communication channels. In the case of the OZG, IMP is a possibility to increase usability and even eliminate the need for administration

portals to process personal information, favouring data minimization. Based on the mentioned problems and solutions, the chapter concludes that IMP can be taken into consideration for solving problems of fragmented partial identities.

The bachelor thesis therefore moves to the second objective to design "IMP solutions" which describe the possibilities of how IMP services and tools can be specifically utilized on the example of - but not limited to - the OZG use case. The thesis presents two solutions for IMP utilization for Service Providers with existing user profile-based identity management. The first solution utilizes IMP in addition to existing user profiles. It provides an optional way for users to create and manage OZG user profiles through an IMP client.

This is done by enabling users to create new user profiles through existing IMP identities by establishing an IMP relationship. By exchanging IMP messages, users are able to access and manage their user profile. The IMP solution especially improves usability as OZG user profiles can be managed along with many other user profiles of other Service Providers through the same IMP client. The solution requires integration only with the administration portal component and can operate without disrupting the existing operation of the system architecture.

The approach of enhancing accessibility to existing user profiles through an IMP client can be used to replace the need for OZG user profiles to be interoperable. Users can effortlessly create, manage, and login to user profiles for each federal state and administration portal. In addition to that, not only user profiles in the context of the OZG can be managed through IMP but user profiles of any integrated Service Provider. This IMP utilization therefore is a possibility to solve the usability problems of partial identities.

However, this IMP solution does not solve many of the data protection issues, as the user profile-based identity management system remains in operation. Therefore, the bachelor thesis presents a second IMP solution, with a focus on data protection.

The second solution utilizes IMP to replace user profiles. Instead of persistently sharing personal information with administration portals in the form of user profiles, IMP is used to temporarily share personal information with institutions for the period of time where an application is being processed. This is done by enabling users to establish different types of IMP relationships, each corresponding to a different application type. This IMP solution especially improves data protection, as only the institution responsible for processing the application receives personal information. In addition to that, sharing personal information only for a short period of time decreases the risk of personal information being misused or stolen.

The approach of replacing user profiles with temporary sharing of personal information for individual business processes can be used to eliminate partial identities while increasing data protection. However, while this approach might be usable in the context of the OZG, Service Providers in the private sector might not be interested in switching to this fundamentally different approach of identity management. Not as a result of technological problems but due to corporate policy reasons ("Never change a running system"). The advantage of IMP is: users can access Service Providers utilizing either IMP solutions through their IMP application.

The third objective of the bachelor thesis is to design a technological integration architecture for the integration of IMP solutions into existing system architectures of Service Providers. The thesis presents a modular messaging system, which enables the integration of IMP solutions into existing system architectures of Service Providers. Through the messaging system, the system architecture of the Service Provider can establish multiple types of IMP relationships and define, exchange, and process different message types. The messaging system maps relationships to entities that the SP systems understand. This can be, for example, the mapping of an IMP relationship to a user profile or to an application process. It also translates between the data models of IMP and Service Provider. As a result of using messaging and messaging modules, the integration system can be configured and extended to fit the requirements of different IMP solutions and system architectures of Service Providers.

The messaging system is shown, integrating both previously described IMP solutions into different system architectures. The first IMP solution was integrated into the administration portal component, the second IMP solution was integrated into the institution domain. This demonstrates that the messaging system is capable of integrating different IMP solutions into different system architectures.

6.2 Outlook

The bachelor thesis describes the integration of IMP on a theoretical level. Developing a prototype of the messaging system as part of an experimental evaluation can give further information about its feasibility, performance, and stability. The prototype can furthermore be used to test integration of the first IMP solution into the OZG system architecture of a federal state, to validate the functionality of the IMP solution and the messaging system, and to find missing features. Due to the modular design of the messaging system, new messaging modules implementing missing features can be added.

To make the modular approach of the integration architecture more utilizable for Service Providers, a "Module Store" can be hosted, where enterprises can publish messaging modules for integration of enterprise systems they sell. Through an IMP tool, Service Providers could be enabled to generate a custom messaging system with messaging modules for selected systems. With "only" configuration of the messaging modules remaining, this could reduce the time required for implementing and deploying the integration architecture.

The thesis presents OZG as a Service Provider relevant for the integration of IMP. Identity Management Provisioning, however, is relevant for many other Service Providers. For example, in the scope of the National Education Platform, "a digital portal is being created that in the future will support universities as well as national and international students who are seeking a stay abroad, a course of study, or a change of study location in Germany along their educational career through a digital offering that is interoperable across institutions" [9]. In accordance with IMP solutions in the thesis, an IMP solution for this new use case can be designed and the presented messaging system can be configured and expanded to suit new requirements and to be used for system integration.

Bibliography

[1] BMI. *Onlinezugangsgesetz (OZG)*. Website. Nov. 2020. URL: `https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html`.

[2] BMI. *OZG im Wortlaut*. Nov. 2020. URL: `https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-wortlaut/ozg-im-wortlaut-node.html`.

[3] BMI. *Was ist das Onlinezugangsgesetz (OZG)?* URL: `https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-node.html`.

[4] *Das Serviceportal Baden-Württemberg*. Website. 2016. URL: `https://www.service-bw.de/documents/20182/299127/serviceBW-Infoveranstaltung-2016-Handout.pdf/65b76075-1534-4c81-8818-f284a122ebbc`.

[5] *Digitale Umsetzung des OZG-Umsetzungskataloges*. URL: `https://informationsplattform.ozg-umsetzung.de`.

[6] *Digitalisierung zu Ende gedacht*. Website. Mar. 2021. URL: `https://www.idas-solutions.de/index.php`.

[7] Bobby Woolf Gregor Hohpe. *Enterprise Integration Patterns*. 2004. URL: `https://www.enterpriseintegrationpatterns.com/`.

[8] *Informationsseite zu service-bw*. Website. 2021. URL: `https://www.service-bw.de/informationen`.

[9] *Initiative Digitale Bildung*. Website. Mar. 2021. URL: `https://www.bmbf.de/de/bildung-digital-3406.html`.

[10] *Intelligent diagramming for every team*. Website. Mar. 2021. URL: `https://www.lucidchart.com/pages/`.

[11] R. Y. Kim. “The Impact of COVID-19 on Consumers: Preparing for Digital Sales”. In: *IEEE Engineering Management Review* 48.3 (2020), pp. 212–218. DOI: `10.1109/EMR.2020.2990115`.

[12] *OZG in NRW*. Website. 2021. URL: `https://ozg.nrw/service/dokumente`.

[13] IT-Planungsrat. *Die Architektur des Portalverbunds.* URL: https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/01_Architektur/Architektur_node.html.

[14] IT-Planungsrat. *Digitale Verwaltung – direkt, schnell, einfach und sicher: Der Portalverbund mit Nutzerkonten.* URL: https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/Portalverbund_node.html.

[15] IT-Planungsrat. *Nutzerkonten für Bürgerinnen und Bürger sowie Organisationen.* URL: https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/03_Nutzerkonto_BuU/Nutzerkonto_node.html.

[16] FITKO IT-Planungsrat BMI. *Digitale Services im Sinne des OZG.* Nov. 2020. URL: https://leitfaden.ozg-umsetzung.de/display/OZG/2.2+Digitale+Services+im+Sinne+des+OZG.