Integration of geospatial services into e-Government applications based on e-Government and SDI standards

M.Sc. Thesis in Geoinformatics

Dustin Demuth
MatNr: 350461
d.demuth@wwu.de

December 22, 2014

1st Supervisor: Prof. Dr. Albert Remke
2nd Supervisor: Prof. Dr. Edzer Pebesma

Institute for Geoinformatics
Westfälische Wilhelms-Universität
Münster

Abstract

This thesis analyses the technical means that are necessary to integrate geospatial data services into e-Government applications. To do so, experts from both, the geospatial domain and the e-Government domain were interviewed to find use-cases which emerge from this integration. The examination of these use-cases showed, that an integration is only possible when basic requirements addressing the secure, traceable, and legally binding transport of messages are met. In e-Government infrastructures standardised transport technologies like OSCI were developed to meet these requirements. In order to satisfy the identified requirements and to enable legally binding, secure and traceable information exchange between services of SDIs and e-Government applications, this work applies the techniques of the transport protocol OSCI to a geospatial data service. The developed prototypical application is on the one hand capable of providing the necessary security, on the other hand it preserves the standards which are used in SDIs. This work shows that an integration of geospatial services into standardised e-Government applications is feasible, when all requirements are met.

Acknowledgments

I like to thank Prof. Dr. Albert Remke and Rüdiger Gartman for their extraordinary support, the plenty of good advice and the regular meetings. In addition I also like to thank Prof. Dr. Albert Remke and Prof. Dr. Edzer Pebesma for taking their time to review this work.

Some parts of this thesis would not be possible without the participation of experts from the geospatial and from the e-Health domain. I like to thank Andreas von Dömming and Tobias Kohr (both BKG / GDI-DE), Andreas Brodowski (City of Paderborn), Ulrich Düren (GDI.NRW), Dr. Stefan Ostrau (Kreis Lippe), as well as Dr. Justus Benzler (RKI) and Dr. Michael Dörr (Rhein-Kreis Neuss) for donating their time and expertise to this project.

I also like to thank 52° North GmbH for the resources they provided, especially Daniel Nüst for the informal “Master Meetings”, and those people who dared to proof-read this work. I really enjoyed working with you.

Contents

1 Introduction

Spatial data services, are said to be the key technology to “extensive e-Government” [1]. This is related to the weight of spatial information in almost every decision making process. Geospatial services are web-services that are capable of providing spatial information in a standardised manner. Spatial information is required for administrative processes and thus can be considered as a critical resource for governments [2]. Geospatial services can represent a part of Spatial Data Infrastructures (SDIs). Those are defined as “materials, technology and people”[3] that are “necessary to acquire, process, and distribute”[3] spatial information. As SDIs provide easy access to spatial information, they are convenient support systems in decision making processes [4]. Users and stakeholders of SDIs come from all sectors: industry, governments, administration, agriculture, economy, private organisations, and many more.

Organisations, which are using e-Government applications from domains apart from the geospatial world, do not use SDIs to their full potential, albeit the organisations work often depends on geospatial information. This deficiency is unfortunate, as integration of spatial data services into e-Government applications is supposed to increase productivity, lower the costs of data acquisition, and provide means of data de-duplication. On a European level the initiative *Infrastructure for Spatial Information in the European Community* (INSPIRE) fosters these targets [5].

This work demonstrates an approach how services of an SDI can be combined with existing and possible future e-Government applications. The standards of both infrastructures and applications remain untouched, thus staying compatible to already existing applications within their own domains. It shows the technical requirements that need to be fulfilled to bridge the gap between geospatial services and e-Government applications.

1.1 Status quo

Currently, all German states are operating SDIs on their own (see analysis in section 2.2.2) in addition to SDIs, which are operated by the federal republics agencies. Within an administrative contract [6] the collaboration between states and federation is regulated. Due to the federalism in Germany, the member states, their municipalities, as well as the federation collect and provide geospatial data, such as topographic maps, land-use data and environmental protection areas [6]. The geospatial data is distributed over multiple agencies. No central data silo exists, which holds data of all participating parties.
Federal law and regulations require that all parties have to create or take part in an SDI. Because of standards, which are defined in European and German legislation, the SDIs of all parties are compatible.

The establishment of a federal SDI has already been decided in 2003 by the German federation and the German member states [7]. Nevertheless, German SDIs are closely linked to the infrastructures enforced by the INSPIRE initiative, which was passed as a regulation by the European Commission (EC) in 2007 [5]. The goals behind the German SDIs and those enforced by INSPIRE are so common, that in 2009 the INSPIRE regulation has already been integrated into German legislation [8]. Geospatial data, as well as its metadata has to be offered as standardised services based upon a set of open standards, which were defined by the Open Geospatial Consortium (OGC). These services are supposed to enable standardised access to geospatial information and location data. This is necessary in cross-border scenarios, for instance to foster interaction between environmental protection agencies in order to enable a better environmental protection. In Germany, the a part of the INSPIRE regulation was integrated into §4 of the *law for access to digital geodata* [8]. It defines which types of data have to be provided with such spatial data services. From the lists of requirements of the regulation and the law it is apparent that almost every information in the context of geospatial information and government has to be provided by the means of a geospatial data service, thus enabling easy access and discovery of the information. Other European countries are operating similar infrastructures, as they are also bound to the INSPIRE regulation.

SDIs are a special form of e-Government infrastructures, as they are not based on the exchange of form-based data, but take other more complex data types into account. However, a compatibility gap exists between services of an SDI and non-spatial e-Government applications and infrastructures. This gap arose as standards of non-spatial e-Government applications, like XML in public administration (XÖV) and Online Services Computer Interface (OSCI) (see chapter 2.2.1), were, and still are, developed on a national level in parallel to the standards of the spatial domain. These were, and are, developed by a supranational community (cf. [2]). As these two communities are focussed on developing standards, which fit to their domain of expertise, technologies that bridge between the domains are left out. Consequently, the exchange of geospatial data between agencies consuming and agencies providing geospatial data often continued to be the same paper-based process as in times before SDI and e-Government.

Within both domains similar procedures took place, which lead to the development of standards and technologies.
In the e-Government domain software vendors use different methods and data-formats to exchange data. This heterogeneity leads to semantic and technical incompatibility of the exchanged information. In cases when an administrative agency uses different software than another agency and needs to transfer data to this agency. Such incompatibility can, in the worst case, require paper-based print-outs which have to be re-digitised. To counter this misdeed, the German federation started e-Government initiatives, to foster strong standardised exchange formats and semantics for administrative processes, e.g. XÖV and OSCI (see chapters 2.2.1 and 2.1.3).

Due to the need of closer collaboration of agencies, companies and service-providers in the geospatial domain, the problem of missing interoperability has been addressed early by developing well-defined standards for information exchange with geospatial data services. In monolithic file-based exchange scenarios [9], e.g. in exchange processes between Geographic Information System (GIS) and Computer Aided Design (CAD) software, the interoperability-issue remains [10].

In addition to the different technical and historical backgrounds of the geospatial and the e-Government domain, the legal basis of the standards differs as well. Whilst standards of the geospatial domain are legally binding [8], the proposed standards of the e-Government initiatives have only recommendative character [11].

The missing connection between geospatial services of SDI and e-Government applications causes problems: When geospatial data is updated, it needs to be re-acquired, because outdated information might cause wrong decisions. This forces an agency, using geospatial data, to constantly monitor if data is up-to-date, due to missing notification processes in cases of data updates. This need of monitoring and re-acquisition can lead to higher financial costs. In addition, data redundancy occurs when an agency is tempted to start data-retrieval on its own, for instance by starting to draw its own maps. Such data-retrieval might be motivated by the idea to minimise costs or acquire data more quickly. Unfortunately, it might cause diverging datasets and representations of the same geographic phenomenon, and, according to Rajabifard, the existence of such “data silos” has negative effects on the use and sharing of spatial data [12]. Also troubling is the use of different semantics and data formats, in cases when objects are described differently in the geospatial domain as in the e-Government domain. An example is the difference in the modelling of planning processes between INSPIRE-PLU (Planned Land Use) and the German exchange format XPlanung[1]. Some of these problems can lead to prolonged response times in communication processes between governmental agencies.

These or similar problems might have motivated the creators of INSPIRE whilst they postulated five core-principles of the initiative [13]:

1. “Data should be collected only once and kept where it can be maintained most effectively.”
2. “It should be possible to combine seamless spatial information from different sources across Europe and share it with many users and applications.”
3. “It should be possible for information collected at one level/scale to be shared with all levels/scales; detailed for thorough investigations, general for strategic purposes.”
4. “Geographic information needed for good governance at all levels should be readily and transparently available.”
5. It should be “easy to find what geographic information is available, how it can be used to meet a particular need, and under which conditions it can be acquired and used.”

According to Vancauwenberghe et al. [2], many experts are convinced that geospatial information has to be integrated into applications of the e-Government domain. In their study, they examined four different European geospatial data strategies (Netherlands, Finland, the United Kingdom, and Denmark). The strategies aim to enable closer information exchange between agencies operating SDIs and agencies that require geospatial information or could enhance their processes by using geospatial information. Based on their analysis, they state all four strategies contain clear visions of the importance of geospatial information to solve administrative problems. All four analysed documents address “benefits

[1] URL: http://www.xplanung.de (Retr.: 2014-11-30)

for the public sector, the benefits for citizens, businesses and society" [2], which arise when e-Government and SDI are closely linked. In an article, Claßen [10] identifies the need of deeper integration of geospatial data services and GIS into other administrative processes apart from the land-use cadastres [10].

It can be concluded, that geospatial data strategies that identify the benefits of geospatial-data-integration are the first step to bridge the gap between e-Government and SDI.

The second step, connecting e-Government and SDI, is the harmonisation of data exchange standards and Information and Communication Technology (ICT). To take this step, collaboration among the two domains is required. collaboration must happen on a technical level concerning transport infrastructures and protocols, as well as on a semantic level concerning the use of the same, or translatable, languages to describe the exchanged data. With such collaborations across governmental agencies, industry and citizens, new partnerships and solutions can be created to respond to challenges on a global scale [12].

1.2 Research questions

Findings of the previous chapter led to the conclusion that a closer collaboration of SDI and e-Government applications [12, 2], and agencies using these technologies [11] is required.

To respond to some of the technical challenges of such a collaboration, this thesis addresses the following research questions:

1. Which use-cases exist, where standards from both e-Government applications as well as SDIs are relevant?
2. What are the requirements of an integration of geospatial services into e-Government applications?
3. How can the integration be realised from a technically?

The first research question aims to discover use-cases where a closer collaboration between services of an SDI and e-Government applications leads to benefits and which new applications might emerge from such collaborations. The examples show that the use of SDIs is reasonable within e-Government infrastructures.

The second question focuses on the means necessary to integrate geospatial services into e-Government environments. By analysing the needs of existing e-Government applications, the requirements for a bridge between SDIs and e-Government applications are identified in section 3.6.

Consequently, the third question aims at the technical implementation of a possible solution. The answer to the question shows how geospatial data services can be integrated into e-Government application, whilst fulfilling the requirements which where addressed in the second question. It describes the software components and provides a prototypical implementation for a use-case, which was described previously.

1.3 Structure of this thesis

The next chapter introduces technologies and standards which relate to the topics handled in this thesis. In addition it introduces scientific work that was conducted in this field. Chapter 3 analyses which applications and use-cases would exist when SDIs are combined with e-Government applications and which applications could emerge from such a symbiosis. The identified use-cases are analysed for technical requirements. One of the use-cases is selected and depicted in more detail in chapter 4. Based on this, a technical prototype is drafted that meets the requirements, which were identified in the previous chapter. The succeeding chapter 5 describes the implementation of a prototype and shows how it can be applied to the selected use-case. Chapter 6 discusses the implementation and the findings of this thesis.

2 Background

This chapter provides an introduction to the e-Government domain, and illustrates technologies and standards used in this environment. In addition it depicts some technologies, which are used within the implementation in chapter 5.

2.1 e-Government

This section will give an overview about European and German e-Government projects, initiatives and standards. It contains information on the procedures of e-Government, which are not basic-knowledge within the GI-science domain. The target of this section is that the reader gains basic knowledge on current e-Government initiatives and understands current trends of e-Government.

2.1.1 Definition

The *Speyerer Definition von Electronic Government* [14] defines e-Government as the execution of administrative and governance processes with the help of ICTs, via electronic media, like the internet. It lists four profiles for governmental communication:

1. Government to Government communication (G2G)
2. Government to Citizen communication (G2C and its inversion C2G)
3. Government to Business (G2B and B2G)
4. Non-Profit-/Non-Governmental-Organisations to Government communication (N2G and G2N)

The term e-Government can be subdivided into a plethora of fields, like e-Democracy, focussing on citizen participation and e-Voting, and e-Administration, focussing on the digitalisation of governmental processes. These fields can be subdivided into fields like e-Justice and e-Health. In a lot of cases e-Government processes are used to exchange data with administrative agencies, like tax or emission reports of the industry. E-Government applications can have multiple characteristics. They can be simple web-portals aiming to provide information or allow a user to download forms and upload filled ones. Some applications are also dedicated software, which can be used by the user, for instance to create and upload tax-reports. The efforts of the geospatial domain to establish and maintain an SDI are also counted as a part of e-Government.

In the remainder of this thesis, the term e-Government is used frequently, nevertheless, it shall only designate those processes which are not directly linked to geospatial data services or SDI.

Targets of e-Government

The *European eGovernment Action Plan* [15] confirms the four primary targets for e-Government aforementioned in the *Ministerial Declaration on eGovernment*, known as the *Malmö Declaration* [16]:

1. User-Enforcement: Empowerment of citizens and economy
2. Enhanced mobility on the internal market of the European Union
3. Enhanced efficiency, effectiveness and reduction of carbon emissions
4. Creation of key-technologies and establishment of technical and legal preconditions

As an effect of these four targets, administrative burdons shall be reduced. According to a study on behalf of the European Commission 70% of the European countries foster methods and initiatives to reduce administrative burdon, and increase efficiency [17].

2.1.2 Europe

The European Commission is interested in the development of e-Government. To foster developments within the member states, the European Commission founded the *ePractice* initative[1], which is a community of experts from the e-Government domain. The community regularly publishes e-Government fact-sheets that wrap-up the current developments of the European member-states. In addition to this initiative, the members of the European Union agreed on an e-Government Action Plan [16] lasting from 2009 to 2015, which shall be followed by the activities of the objective *A Digital Agenda for Europe* of the *Europe 2020*

[1] URL: http://www.epractice.eu (Retr.: 2014-11-17)

strategy plan [18]. This action plan also defined the targets of e-Government stated above.

Although a central strategy exists, the realisation and development of e-Government services differs rapidly among the member-states, according to [19], where solutions of some selected countries were analysed.

2.1.3 Germany

In Germany, federal, state, and local authorities are responsible for governmental acts. This division leads to a heterogeneity of administrative processes and administrative software. Nevertheless, the federal authorities started to provide a legal framework for e-Governmental activities in 1997, when the law for digital signatures [20] was passed. The law can be considered as a key-enabler for e-Government in Germany, as it put the electronic exchange of data on a legal basis and enabled digital data to have the same legally binding status of a signed paper document. In the year 2000 the initiative *Bund Online2005* [21] was started, which focussed on the integration of every internet-capable administration process into the internet. The federal initiative also contained the communal initiative *media@komm*, which started slightly earlier. One outcome of the Bund Online2005 initiative is the IT-Standards catalogue *Standards and Architectures for e-Government Applications* (SAGA), which is regularly updated. As its name suggests, the catalogue lists and suggests standards, applications and architectures that should be used in administrative and governmental processes. The initiative Bund Online2005, was complemented by *Deutschland Online* in 2003, which also took the needs of state and municipal administration into concern.

Alongside those strategies, several coordination offices were founded on a federal level. These include the *IT-Planning Council* (IT-Planungsrat)[2], aiming to provide political guidance in the fields of ICT, standardised and joint systems, and quality and efficiency control. And the *Coordinating Office for IT-Standards* (KoSIT)[3], which originated from the OSCI-steering office, supporting the IT-Planning Council and aiming to coordinate the efforts of development of standards such as OSCI and XÖV, which are depicted in the next chapter, as well as a consistent character set for e-Government applications. One of the latest projects of the IT-Planning Council and the KoSIT is the establishment of a communication infrastructure which connects all administrative agencies, the Germany Online Infrastructure.

[2] URL: http://www.it-planungsrat.de (Retr.: 2014-11-18)

[3] URL: http://www.xoev.de (Retr.: 2014-11-18)

2.2 Technologies

This section describes the technologies related to this thesis. It gives an overview about standards and protocols in German e-Government applications, and their implementation within the German member states, later it introduces the principles of information security and basic cryptographic systems.

2.2.1 OSCI — Online services computer interface

The Online Services Computer Interface (OSCI) is a transportation protocol for secure, electronic information exchange between governmental and administrative agencies as well as economy and citizens. Its specification is divided into two parts, one addressing message transport and another addressing the content of a message. The term OSCI-Transport depicts the first part of the OSCI specification. The content part of OSCI is almost not addressed under this name in literature and specifications, instead the name *XML in public administration* (XÖV) is used widely. It can be safely assumed that when OSCI is mentioned without an extension, the transport part OSCI-Transport is intended.

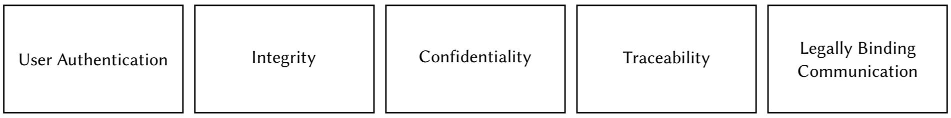


Figure 2.1: The five core features of OSCI-Transport.

Version 1.0 of the transport protocol was specified in November 2000 [22]. Since then the core features of OSCI-Transport are *user authentication*, validation of the messages *integrity*, the guarantee of *confidentiality*, as well as the enablement of *traceable* and *legally binding* communication. According to these features, the protocol enforces replicable transport of information and ensures the authenticity, integrity and confidentiality by using digital signatures and encryption. OSCI-Transport 1.2 is compatible with the German law for digital signatures (SigG) [20, 22], thus it enables legally binding communication. Due its features, OSCI-Transport 1.2 was suggested as a standard for electronic communication with federal administrative agencies in SAGA in 2011 [23].

OSCI-Transport is currently being specified in two mayor releases, which are not compatible, due to different architectural concepts.

OSCI-Transport 1

OSCI 1.2 was developed in the context of the MEDIA@komm project, which lasted from 1999 to 2003. Its goal was to foster technologies and applications in the e-administration domain by creating secure communication without media disruptions between administration, citizens and economy.

OSCI-Transport integrates international developments when dealing with cryptography and the handling of documents based upon Extensible Markup Language (XML) messages and technologies. Thus it is based upon developments coordinated by the World Wide Web Consortium (W3C). OSCI-Transport is designed to handle synchronous as well as asynchronous transportation of messages. Due to timestamps the protocol can be used to keep terms. By using digital signatures, communication handled by services using OSCI-Transport is indisputable and verifiable according to the current legislation. OSCI-Transport is capable of transporting arbitrary data, which does not need to be based upon XML.

An OSCI-Transport message is separated between communication- and content-data. Both parts of a message are handled separately and can be encrypted in different means. OSCI-Transport follows the principle of a doubled envelope. The inner envelope contains the private message, which has to be transported. The outer envelope contains the inner envelope and data which describes how the message has to be transported. Each component within a transport chain can open the outer envelope and add or remove information to this envelope. Unless they are the legal receiver of the message, components within the transport chain are not capable of opening the inner envelope and read the message. This feature makes end-to-end encryption of the content possible.

Whilst the content part can be arbitrary data, unless it is supposed to be an OSCI-XÖV message (see section 2.2.1), the part including the communication data is a heavily structured XML document. The transport part includes all information which is required to transport the message, such as timestamps, certificates of the participants in the communication-chain, like sender and receiver, information on the subject of the message and information about the current state of delivery of the message [24, 25].

OSCI differentiates between *author* and *sender* of a message as well as between *receiver* and *reader*. Whilst the author is the person which created the content of the message, and is responsible for its correctness, the sender is responsible for starting the transport of the message. These two parties can be the same. The receiver-reader differentiation is analogue to the author-sender case. A more sophisticated depiction of the different roles in OSCI-Transport can be found in the technical specification of the protocol [25]. A synchronous message exchange with OSCI-Transport is depicted in figure 2.2.

The author can digitally sign and encrypt the content data. Afterwards the envelope containing the content data is wrapped into a transport envelope which contains the information that is necessary to transport the message. The sender forwards the message to the receiver. The receiver receives the message, removes the transport-envelope and forwards the encrypted content envelope to the reader. The reader decrypts the message and can process it further.

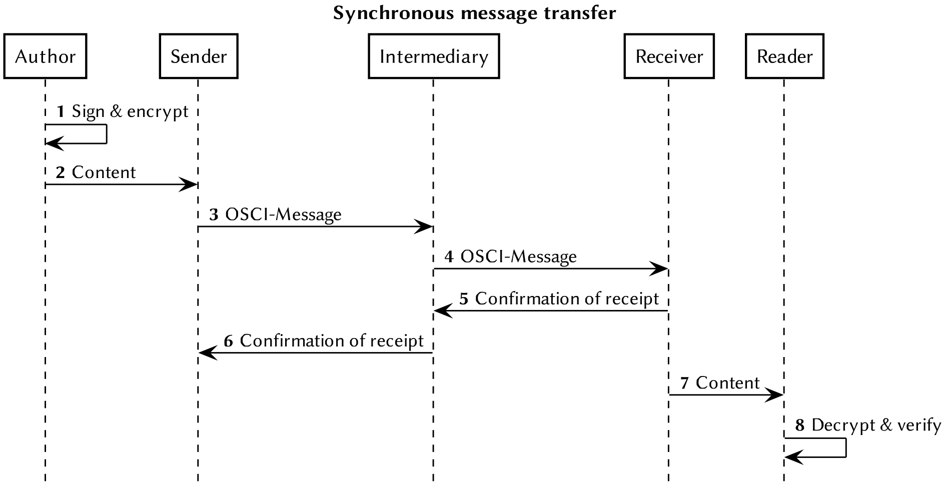


Figure 2.2: Synchronous message transfer within OSCI-Transport 1.2 makes use of receipts and distinguishes between receiver and reader, and author and sender of a message. (As per [25, p.8, fig. 2])

Apart of the four known roles, the fith role *intermediary* is also shown in the figure 2.2. This component is necessary as OSCI-Transport is intended to enable asynchronous information exchange. This is handy, when both, author and reader of the message are persons, which are not always available, e.g. by being bound to office hours, or when processes are used that require manual interference. To enable this asynchronicity, the intermediaries act as mailboxes. Figure 2.3 depicts such an asynchronous flow of information, using the intermediary as a virtual post-office. In German e-Government environments the term *virtuelle Poststelle* is often used for the intermediary. The intermediaries may implement mechanisms that create confirmations of receipt. As intermediaries act as a component, which can be considered as independent from sender and receiver, the confirmations of receipt and the log-book of the intermediary are more trustworthy than those generated by sender and receiver. In addition to log-keeping, the intermediary can implement functions to check the validity of the digital certificates of all other roles. To use an intermediary, no registration is required. Authentication to access a mailbox is handled with X.509 v3 [26] certificates. A new mailbox is created, when the first message arrives that is addressed to the user. Applications using OSCI include virtual post-offices and emission reporting[4].

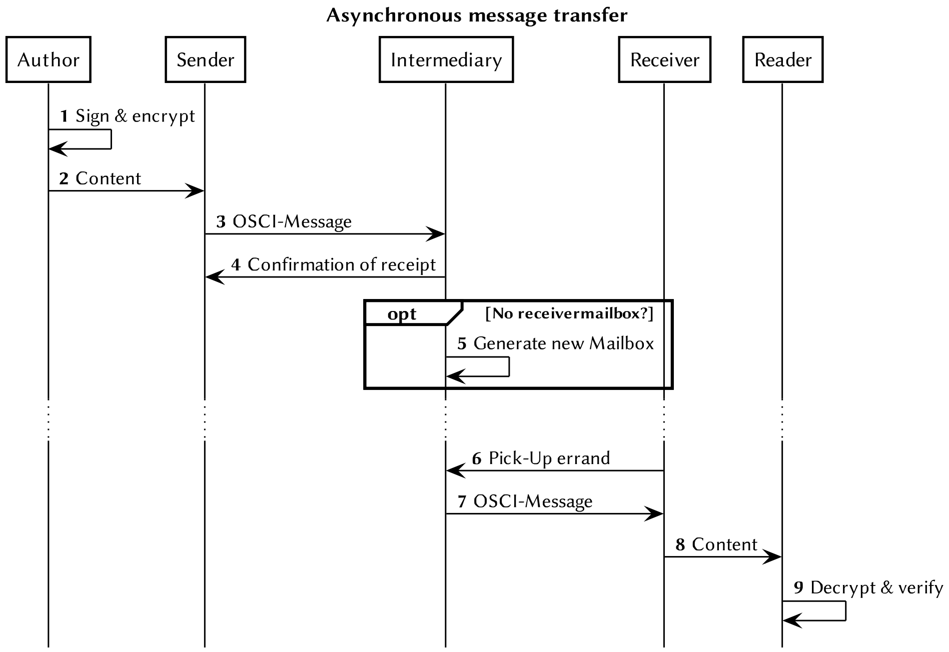


Figure 2.3: Asynchronous message transfer within OSCI-Transport 1.2 makes the same distinctions like synchronous message transfer. For receipts and the transferred data it makes use of intermediaries. (As per [25, p.8, fig. 2])

The KoSIT publishes free and open source implementations of the OSCI-Transport specifications. Those libraries have their own versioning scheme. Thus the most recent library 1.6 still refers to version 1.2 of OSCI-Transport, but with the fourth set of corrections applied.

[4] URL: www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Abgeschlossene_Projekte/Anlagen_Blaupause/Anlage_A14_Anwendungen_auf_Basis_OSCI.html (Retr.: 2014-08-22)

OSCI-Transport 2

OSCI-Transport 2 is the newest specification of OSCI. Its architecture differs heavily from the architecture of the OSCI-Transport 1.2 specification. Due to that, there is no compatibility between the two versions of OSCI.

OSCI2 focuses stronger on the use of already existing web-technologies. Whilst the first version of OSCI was specified, a lot of required features had not been specified on an international level. Meanwhile those features are available within international, non proprietary web services specifications, also known as the WS-Stack. The availability of international standards fostered the need for a new approach on OSCI that focuses stronger on the use of these technologies. [27]

To provide interoperability, OSCI2 bases on the specifications published by the Web Services Interoperability Organization (WS-I)[5], which is a part of the Organization for the Advancement of Structured Information Standards (OASIS)[6]. Such specifications are the WS-I basic profile[7] and the WS-I Basic Security Profile[8].

The specifications of the WS-Stack are extended by OSCI2 because there are requirements, such as the legally binding communication, which are still not addressed in the international standards. Within the OSCI2 specification such extensions are marked as an optional feature, to provide as much interoperability as possible.

OSCI2 rejects the doubled-envelope pattern of its predecessor. Instead, it uses the typical structure of a SOAP message, consisting of only one envelope, a header and a body [27]. The header includes communication data, which is, as in OSCI-Transport 1.x, used for the message transport and message security. The information within the header complies to information which is required by the WS-Stack. In addition, information is added according to the OSCI2 specification, e.g. to enable legally binding communication. The body includes the content data and can be encrypted. Thus it is called *opaque body*.

According to the WS-I-Basic specification, OSCI2 services are described by Web Service Description Language (WSDL) documents. Like in the SOAP definitions, Message Exchange Patterns (MEPs) define the exchange of information between

[5] URL: www.ws-i.org

[6] URL: www.oasis-open.org

[7] URL: www.ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html (Retr.: 2014-08-20)

[8] URL: www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html (Retr.: 2014-08-20)

clients and services. Therefore applications, which produce content, are called *Source Applications* (Author). Applications which consume content are called *Target Applications* (Reader). Messages are exchanged between these two applications using OSCI-Gateways, which are called *Initiator* (Sender) on the source and *Recipient* (Receiver) on the target side. Apart from its message relaying capabilities, which require WSDL-support, each OSCI-Gateway has to implement capabilities of data signing, signature verification as well as data en- and decryption.

Whilst OSCI 1.2 specified four different types of communication between source and target application [28], these types where reduced to two in OSCI2 [27]. These are: *synchronous point-to-point* (figure 2.4) and *asynchronous response* (figure 2.5). As this nomenclature already implies, OSCI2 is also supporting the use of mailboxes like its predecessor as well as synchronous point to point communication. Message exchange in OSCI2 is also verifiable and serves the purpose of legally binding communication. Therefore three different types of receipts exist, which make assertions about delivery and receipt of messages. First, the authors of OSCI2 define a *delivery receipt*, which states whether a message has been delivered to a certain recipient. The receipt confirms the time when an information has been delivered to a recipient. Second, a *reception receipt* which is supposed to be send from the final receiver (Target Application) confirms when and from whom an information has been received. And third, a *fetched notification* receipt, in which a mailbox confirms to the initiator of a message exchange that the target application has pulled the message from the mailbox. The different types of receipts are depicted in [27] in detail.

Equally to OSCI 1.2, the specifications for OSCI2 is freely available at KoSIT. In addition to the exemplary implementations at KoSIT the town Esslingen distributes an open source implementation of OSCI2.

According to the KoSIT OSCI2 is used and tested within the German electronic system for infection reporting (DEMIS) project [29] and the Fraunhofer FOKUS project P23R [30].

OSCI-XÖV — XML in public administration

OSCI-XÖV commonly called XÖV (XML in public administration) is a standardisation approach for semantics and grammar in e-Government applications in Germany. It is the second part of the OSCI framework. Like in OSCI-Transport, the standardisation processes of XÖV is also lead and coordinated by KoSIT.

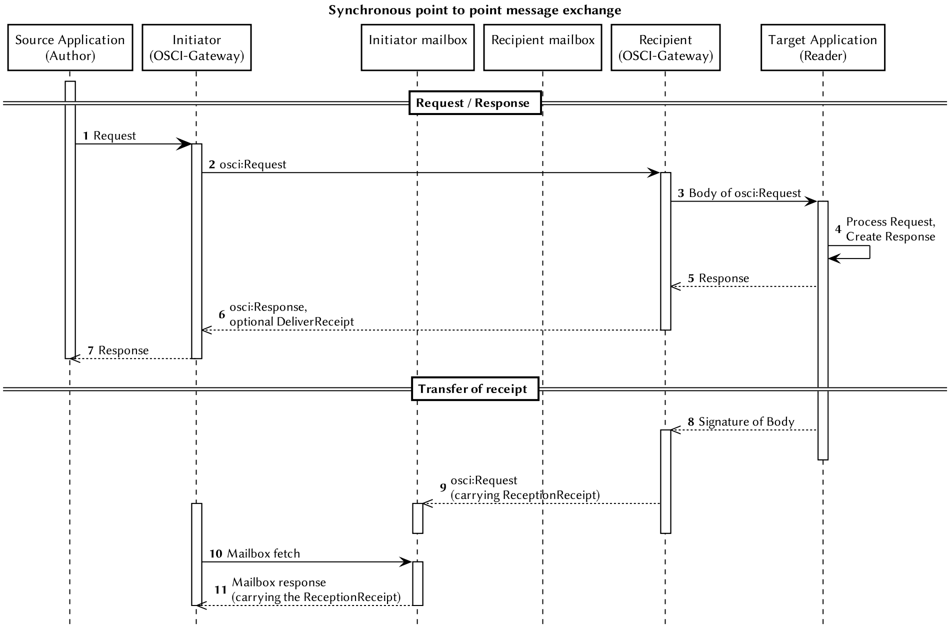

Synchronous point to point message exchange
Source Application (Author)
Initiator (OSCI-Gateway)
Initiator mailbox
Recipient mailbox
Recipient (OSCI-Gateway)
Target Application (Reader)
Request / Response
1 Request
2 osci:Request
3 Body of osci:Request
4 Process Request, Create Response
5 Response
6 osci:Response, optional DeliverReceipt
7 Response
Transfer of receipt
8 Signature of Body
9 osci:Request (carrying ReceptionReceipt)
10 Mailbox fetch
11 Mailbox response (carrying the ReceptionReceipt)

Figure 2.4: Synchronous point-to-point message exchange. This exchange pattern is more similar to today's web services' exchange patterns. (As per [27, p.9, fig. 3])

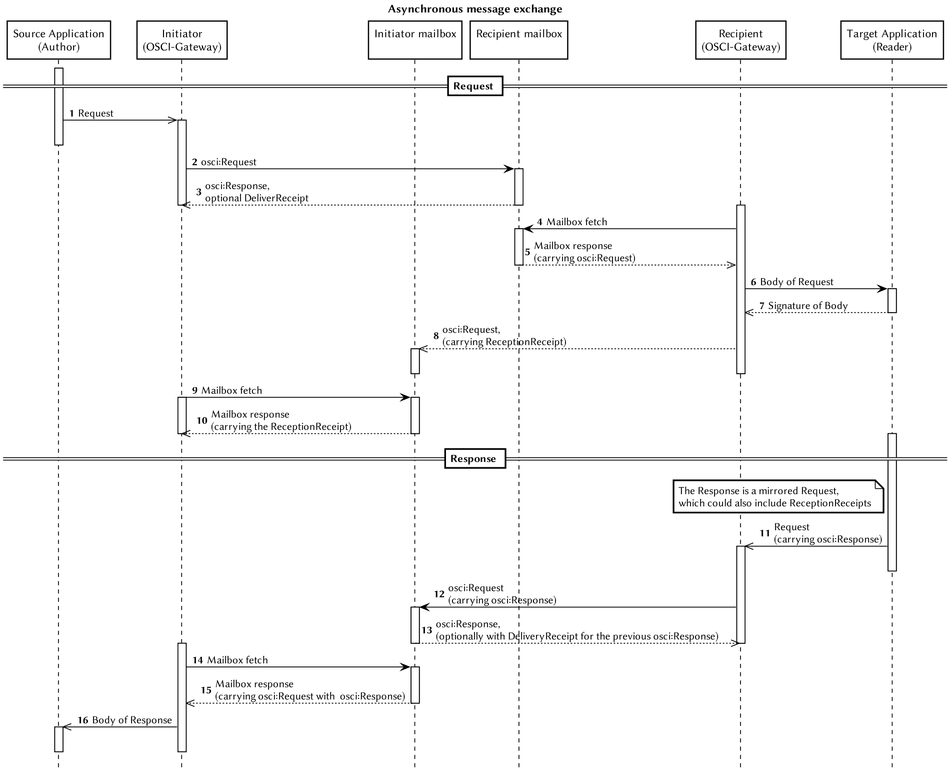

Asynchronous message exchange
Source Application (Author)
Initiator (OSCI-Gateway)
Initiator mailbox
Recipient mailbox
Recipient (OSCI-Gateway)
Target Application (Reader)
Request
1 Request
2 osci:Request
3 osci:Response, optional DeliverReceipt
4 Mailbox fetch
5 Mailbox response (carrying osci:Request)
6 Body of Request
7 Signature of Body
8 osci:Request, (carrying ReceptionReceipt)
9 Mailbox fetch
10 Mailbox response (carrying the ReceptionReceipt)
Response
The Response is a mirrored Request, which could also include ReceptionReceipts
11 Request (carrying osci:Response)
12 osci:Request (carrying osci:Response)
13 osci:Response, (optionally with DeliveryReceipt for the previous osci:Response)
14 Mailbox fetch
15 Mailbox response (carrying osci:Request with osci:Response)
16 Body of Response

Figure 2.5: Asynchronous response message exchange. OSCI2 still supports the use of intermediaries. (As per [27, p.10, fig. 4])

Therefore a central repository[9] has been created which lists the already existing standards, as well as codelists and intentions for new specifications. XÖV is an exchange format for data which is needed in administrative processes, such as citizen or weapon registration. With XÖV-standards different administrative agencies agree upon a common language to describe data. This simplifies electronic communication between administrative agencies of different communities and enables loss-less and fast information exchange between software applications. Currently 13 different specifications exist, which are certified as meeting the common criteria of XÖV. Such specifications reach from citizen registration (XMeld), transfer of financial information (XFinanz), via ordering of passports (XHoheitliche Dokumente) and waste water reporting (XKommunalabwasser), to disaster management (XKatastrophenhilfe). New specifications are created regularly, as needed.

2.2.2 Distribution of OSCI in the German federation

Due to federalism in Germany, all German states may have their own regulations and standards concerning e-Government and Information Technologies (IT), but they are free to combine their efforts [31, Art. 91(c)]. As part of that combination, the IT-Planning Council agreed upon a national e-Government strategy in 2010 [32], to foster a leitmotif for the German states and municipalities. The e-Government strategy follows the european Malmö Declaration on e-Government [16].

To evaluate the use of OSCI, this chapter establishes an overview on the distribution of OSCI and SDI within the federation of Germany. To do so, the websites of the German member-states where analysed for hints pointing towards OSCI or documents which are considered as IT-standards. If such documents could not be found, the states have been contacted and asked which processes are used or if IT-standard documents exist.

Baden-Württemberg

According to a reformation of the administration[10] from 2013, the standards of OSCI have to be used as a model for architecture. The reformations also states that SDIs have to be used.

[9] URL: www.xrepository.de (Retr.: 2014-08-21)

[10] URL: www.verwaltungsreform-bw.de/PUBLIKATIONEN/Studien-Konzepte/Documents/131216_E-GK-Standards%202013.pdf (Retr.: 2014-08-22)

Bavaria (Bayern)

Recent Bavarian projects show that SDIs are used for geospatial data. The existence of a set of *Bavarian IT-Standards*[11] is mentioned, but there is no clarification what is used. The standards have been requested on 2014-04-24 at the concerning ministry (Bayerisches Staatsministerium der Finanzen, für Landesentwicklung und Heimat (StMI)). Unfortunately access to this standards was denied on 2014-05-14:

> "By the very matter of administrative instructions and the announcement of the ministry it unfolds that ICT-standards are not destined for publication."
> Translated from the german original answer:
> "Aus der Natur der Verwaltungsvorschriften als solche und aus der Bekanntmachung des StMI ergibt sich, dass die IKT-Standards nicht zur Veröffentlichung bestimmt sind."

Berlin

The city-state of Berlin has a standards document which regulates the use of IT. It requires OSCI for legally binding communication. For geodata it recommends, but not requires, the use of geoportals like those used within the SDI[12].

Brandenburg

The state of Brandenburg has an IT-Standards document from 2008. It leans closely to the standards and recommendations of SAGA. They require OSCI for secure communication and SDIs are mandatory for geospatial data[13].

[11] URL: www.cio.bayern.de/internet/cio/4/19707/ (Retr.: 2014-04-24)

[12] URL: www.berlin.de/sen/inneres/moderne-verwaltung/informationstechnik/it-standards/it-standards_2014.pdf (Retr.: 2014-04-24)

[13] URL: www.bravors.brandenburg.de/sixcms/detail.php?gsid=land_bb_bravors_01.c.49680.de (Retr.: 2014-04-24)

Bremen

Like Brandenburg, Bremen leans closely to SAGA. This is not surprising, as Bremen is the residence of the KoSIT[14].

Hamburg

Hamburg uses an IT-Strategy which is valid between 2011 and 2015[15]. In this strategy it defines the electronic post office as the mean of secure, legally binding communication. Most likely OSCI is used for this post office. Geospatial data is distributed with SDIs.

Hesse (Hessen)

An *e-Government Masterplan* exists. But it is not conclusive if the recommendations of SAGA are used. The web-representation of Hesse's e-Governement initiative[16] implies that the XÖV-Standard XFall is used. Thus, it is likely that OSCI-Transport is also used for secure communication. Also in Hesse, SDIs are used for geospatial data. To confirm whether OSCI-Transport is used, the ministry for interior and sport was contacted on 2014-04-24. Unfortunately there was no answer.

Lower Saxony (Niedersachsen)

Lower Saxony has a cooperation contract about e-Government[17] that requires the use of SAGA. Geospatial data is distributed with SDIs.

[14] URL: www.finanzen.bremen.de/sixcms/detail.php?gsid=bremen53.c.3200.de (Retr.: 2014-04-24)

[15] URL: www.hamburg.de/contentblob/4268764/data/summery-2014.pdf (Retr.: 2014-04-24)

[16] URL: www.egovernment.hessen.de (Retr.: 2014-04-24)

[17] URL: www.nlt.de/pics/medien/1_1192634028/20071017__eGovernment_Rahmenvereinbarung__endgueltige_Fassung_mit_Unterschriften_.pdf (Retr.: 2014-04-24)

North Rhine-Westphalia (Nordrhein-Westfalen)

North Rhine-Westphalia also has a document which depicts the standards which have to be used. The document *IT-Standards im Geschäftsbereich des Innenministeriums NRW* is intended for internal use only. A regulation[18] depicts this document and mentions SAGA as reference. The request for the document on 2014-04-24 remained unanswered.

Mecklenburg-Hither Pomerania (Mecklenburg-Vorpommern)

Mecklenburg-Hither Pomerania also has an IT-Masterplan[19]. It supposes OSCI for secure communication with virtual post offices, and SDIs for geospatial data.

Rhineland-Palatinate (Rheinland-Pfalz)

According to the *Actionplan eGovernment*[20] OSCI shall be used for secure communication and SDIs for geospatial data.

Saarland

The Saarland uses OSCI for secure communication[21] and SDIs for geospatial data.

Saxony (Sachsen)

Saxony uses SAGA[22]. OSCI is used for secure communication, SDIs are used for geospatial data.

[18] URL: recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&gld_nr=2&ugl_nr=20025&bes_id=7708&menu=1&sg=0&aufgehoben=N (Retr.: 2014-04-24)

[19] URL: www.regierung-mv.de/cms2/Regierungsportal_prod/Regierungsportal/_downloads/IM/IT-Beauftragte/Masterplan_2011.pdf (Retr.: 2014-04-24)

[20] URL: www.isim.rlp.de/no_cache/moderne-verwaltung/e-government/?cid=32518&did=24890&sechash=45d5d0df (Retr.: 2014-04-24)

[21] URL: http://ego-saar.de/index.php?id=675 (Retr.: 2014-08-22)

[22] URL: www.egovernment.sachsen.de/105.htm (Retr.: 2014-04-24)

Saxony-Anhalt (Sachsen-Anhalt)

Geospatial data is distributed with SDIs. Saxony-Anhalt does not distribute information about the use of secure message exchange[23]. A request from 2014-04-24 at the ministry of finances remained unanswered.

Schleswig-Holstein

Schleswig-Holstein uses OSCI[24] and SDIs[25].

Thuringia (Thüringen)

Thuringia uses OSCI for secure communication and SDIs are used for geospatial data. Nevertheless, there is no clear IT-Strategy[26].

Summary of the evaluation

Table 2.1 shows a summary of the evaluation which standards are used for secure communication and geodata within the German member-states. It is interesting, that most of the IT-Standards and documents list OSCI and SDI in close proximity to each other, but not one suggested to combine geospatial data services with the transport capabilities of OSCI to narrow the gap between e-Government applications and geospatial services.

[23] URL: www.mf.sachsen-anhalt.de/informations-und-kommunikationstechnologie (Retr.: 2014-08-22)

[24] URL: www.schleswig-holstein.de/MJKE/DE/Justiz/ElektronischeJustiz/ElektronischerSchriftverkehr/Bekanntmachungen/elektronischerSchriftverkehr.html (Retr.: 2014-08-22)

[25] URL: www.schleswig-holstein.de/LVERMGEOSH/DE/Geodateninfrastruktur/LeitstelleGdi/ServicestelleGeodaten/servicestelleGeodaten_node.html (Retr.: 2014-08-22)

[26] URL: www.thueringen.de/imperia/md/content/rechnungshof/veroeffentlichungen/sonstige/2014_it-beratung.pdf (Retr.: 2014-08-22)

Table 2.1: Overview of standards used within the German states. The last column depicts whether a standards-document is present in which a standard is defined. When the use of a standard is likely but only assumed, it is marked with a $^?$ sign.

State	Standards for: Secure Communication	 Geospatial Data	IT/eGov-Stategy or IT-Standards Document
Baden-Württemberg	OSCI	SDI	eGov Concept incl. IT-Standards
Bavaria	undisclosed	SDI	Bavarian IT-Standards which will not be published
Berlin	OSCI	SDI	IT-Standards of the Berlin Administration
Brandenburg	OSCI	SDI	IT-Standards which relate to SAGA
Bremen	OSCI	SDI	Based upon SAGA
Hamburg	OSCI	SDI	IT-Strategy document
Hesse	OSCI$^?$	SDI	
Lower Saxony	OSCI	SDI	Based upon SAGA
North Rhine-Westphalia	OSCI$^?$	SDI	Related to SAGA
Mecklenburg-Hither Pomerania	OSCI	SDI	IT-Masterplan
Rhineland-Palatinate	OSCI	SDI	
Saarland	OSCI	SDI	A IT-Security guideline from 2003 is used
Saxony	OSCI	SDI	Based upon SAGA
Saxony-Anhalt	No information available	SDI	
Schleswig-Holstein	OSCI	SDI	
Thuringia	OSCI	SDI	No clear IT-Strategy

2.2.3 Principles of information security

In information security three basic principles exist [33], alongside many other principles, which should be taken into account when a new information system is planned, or old systems are assessed. E-Governmentapplications take these basic principles into account. The basic principles are: *Availability*, *Integrity*, and *Confidentiality*. They are accompanied by *Authentisation*, *Authorisation*, and *Information privacy*. The following six definitions are based on the definitions of the Federal Office for Information Security (BSI) [33].

Availability: The principle availability describes the extent of availability of a dataset or information system to the user. It takes into account when a user needs to access the system and assesses if the failure of a system and resulting unavailability are a critical factor for a business process. The concept of availability will not be considered within the solutions proposed in this thesis, as it is highly depending on the use-case of an information system.

Integrity: Integrity has two meanings. On the one hand integrity of a dataset means, that it is complete and not altered by unauthorised persons. On the other hand integrity of an information system means that nobody could gain access to the system which was not authorised. If an information system has lost its integrity, it is likely that the data processed and stored on that system also lost integrity.

Confidentiality: Confidentiality has to be preserved by an information system, when data or information has to remain in private or accessible by a restricted group of users, only.

Authentication: The term authentication is used to describe the process of validating the authenticity of a user or information system.

Authorisation: Authorisation mostly takes place after authentication. It validates if a user or system is allowed to gain access to an information or dataset.

Information privacy: The term information privacy describes the need of protection of an information which is considered as personally identifiable information, like the combination of names and addresses, religions or illnesses.

2.2.4 Cryptographic systems

A lot of mechanisms from the information security domain are based on cryptographic systems. These systems are defined as a "set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context" [34]. Ibidem cryptographic algorithms are defined as algorithms which make use of the tools of cryptographic science, such as "encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms", whilst cryptography is the science of using mathematical methods to alter an information into an unintelligible state (encryption) and to revert this process (decryption). Cryptography may be used to protect an information from unauthorised use, for instance during transport.

Hence cryptographic systems consist of at least one cryptographic algorithm and one key that is used to modify the algorithm.

Symmetric cryptography / secret key cryptography

Symmetric cryptography algorithms are cryptographic algorithms which use the same secret key for encryption and decryption. Hence, symmetric cryptography is also known as secret key cryptography [34]. Within a communication process both, the encryptor and the decryptor need to know this secret key. This key has to remain secret, in order to keep the information safe. Therefore the key has to be shared by using a trusted medium, i.e. personally, by telephone or a courier. Figure 2.6a depicts the workflow of a symmetric-key algorithm.

Popular applications of symmetric cryptography are the encryption of Wireless Local Area Networks (WLANs) (with Wi-Fi Protection Access (WPA) using Advanced Encryption Standard (AES)), or password protected file compression. One of the advantages of symmetric encryption is speed. AES for example has been integrated into the hardware of recent premium class computer processors, which makes cryptography that is using AES much faster. The great disadvantage of symmetric cryptography is the need of sharing a secret key to both parties. This shared key is a common attack vector on systems using symmetric cryptography, e.g. by doing a brute-force attack, or picking words from a dictionary.

Asymmetric cryptography / public-key cryptography

Until the 1970-ies symmetric cryptography was the only known type of cryptography. In 1976 one of the first approaches was published [35]. It proposed a new method, using separate keys for encryption and decryption. In asymmetric cryptography or public-key cryptography a pair of keys instead of a single one is generated. This pair consists of a public and a private key [34]. Within a communication between two parties, both parties need to generate such a key pair, and share the public key with each other. They also need to keep the private key secret, thus they remain the single owner of the private key. Within such a communication scenario, data is encrypted with the public key of the communication partner. The encrypted dataset can only be decrypted with the private key. Figure 2.6b depicts this mechanism.

Public-key cryptography is slower than symmetric cryptography, due to much longer encryption keys, nevertheless the gained safety from the absence of a shared secret is convincing. A popular application of asymmetric cryptography is the network protocol Secure Shell (SSH).

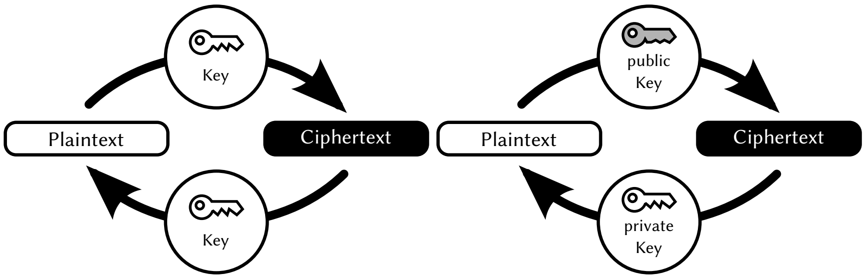
Hybrid cryptography

Hybrid cryptography is a mixture of asymmetric cryptography and symmetric cryptography. It is supposed to enhance the speed of a cryptographic process, as it reduces the the key length which is used to encrypt the dataset. Figure 2.7 depicts the process.

Like in asymmetric cryptography, the public key is used for encryption, but in this case a random symmetric key, called session-key, is generated during the process of encryption. The session-key is used to encrypt the message. In a second step, the session-key is encrypted by using the public key. The now encrypted session-key is attached to the encrypted message. As expected, the message is also decrypted in two steps. First the encrypted session-key is decrypted with the public key, second the message is decrypted with the session-key. This system is used to enhance the speed of cryptographic processes whilst providing the safety of public-key cryptography. Network protocols like IPSec make use of hybrid cryptography. It is also used to encrypt e-mail for instance by using GNU Privacy Guard (GPG).

Public key infrastructures

One of the problems of asymmetric cryptography is the lack of trust into the authenticity of the shared public key. Whilst in symmetric systems the secret key was shared by using a trusted medium the public key in an asymmetric system can be shared by using the same insecure, untrusted method which is used to



(a) Symmetric cryptography (b) Asymmetric cryptography

Figure 2.6: Differences of symmetric and asymmetric cryptography. In symmetric cryptography (a) the same key is used for encryption and decryption, whereas asymmetric cryptography (b) uses a public key for encryption and a private key is for decryption.

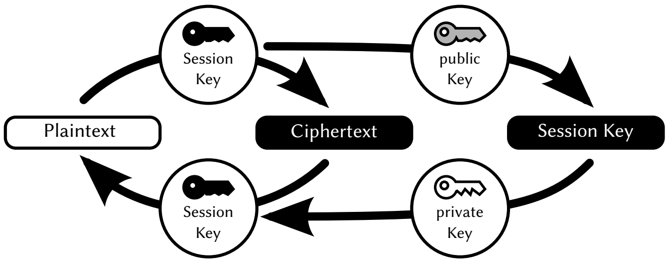


Figure 2.7: The process of hybrid cryptography uses a random session key to encrypt the data. First, the plaintext is encrypted with a random session key. Second, the session key is encrypted with the receivers public key. Third, the session key is decrypted with the receivers private key. In a last step, the cipertext is decrypted with the session key.

transfer the encrypted information. This implies, that a communication scenario, which depends on asymmetric cryptography, is prone to impersonation. In order to circumvent this problem, a Public Key Infrastructure (PKI) is used. Within a PKI a certification authority assumes the role of a trusted third party. The latter validates the public keys of the communication partners and certifies that those keys belong to the real communication partner. This system only works if both parties share at least one trusted third party, which has validated the public keys of the communication partners.

PKI can have different structures. They can be strict and hierarchical, like for instance in an X.509 standardised infrastructure, which is used to validate Websites and to enable Hypertext Transfer Protocol Secure (HTTPS), or decentralised like the Web of Trust (WOT) [36]. In both cases, digital signatures are used to certify the authority of the communication partner.

Digital signatures

A digital signature is a value generated by a cryptographic algorithm from a data object [34]. Typically the digital signature is appended to the data object. The purpose of digital signatures is the validation of integrity and authenticity. Like a manual, paper-based signature the digital signature allows to verify the origin of a dataset, thus proving authenticity. In addition, it can serve the purposes of a seal, like those within an official document. If the document was altered the digital signature cannot be validated, like a seal would be broken. Thus it can be used to proof the integrity of the dataset.

In public-key cryptography, the use of private and public key is reversed for a signature process, like it is depicted in figure 2.8. Only the owner of a private key can digitally sign a dataset, the public key can only be used to validate the dataset. Within a PKI, the public key of a communication partner is digitally signed with the private key of the trusted third party. To validate this signature, the communication partners have to be aware of the public key of the trusted third party.

2.3 A federal infection reporting system

In Germany, selected diseases and pathogens have to be reported to the authorities, by those who clinically or laboratorially diagnose them [37]. For some of

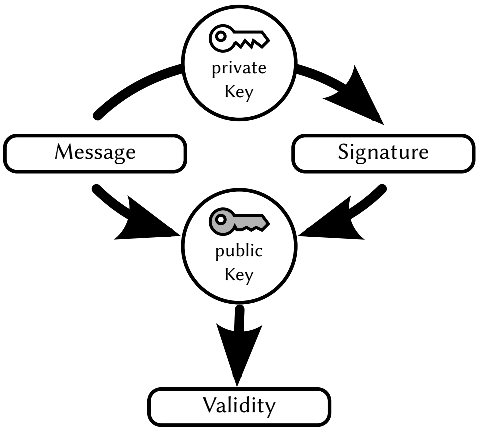
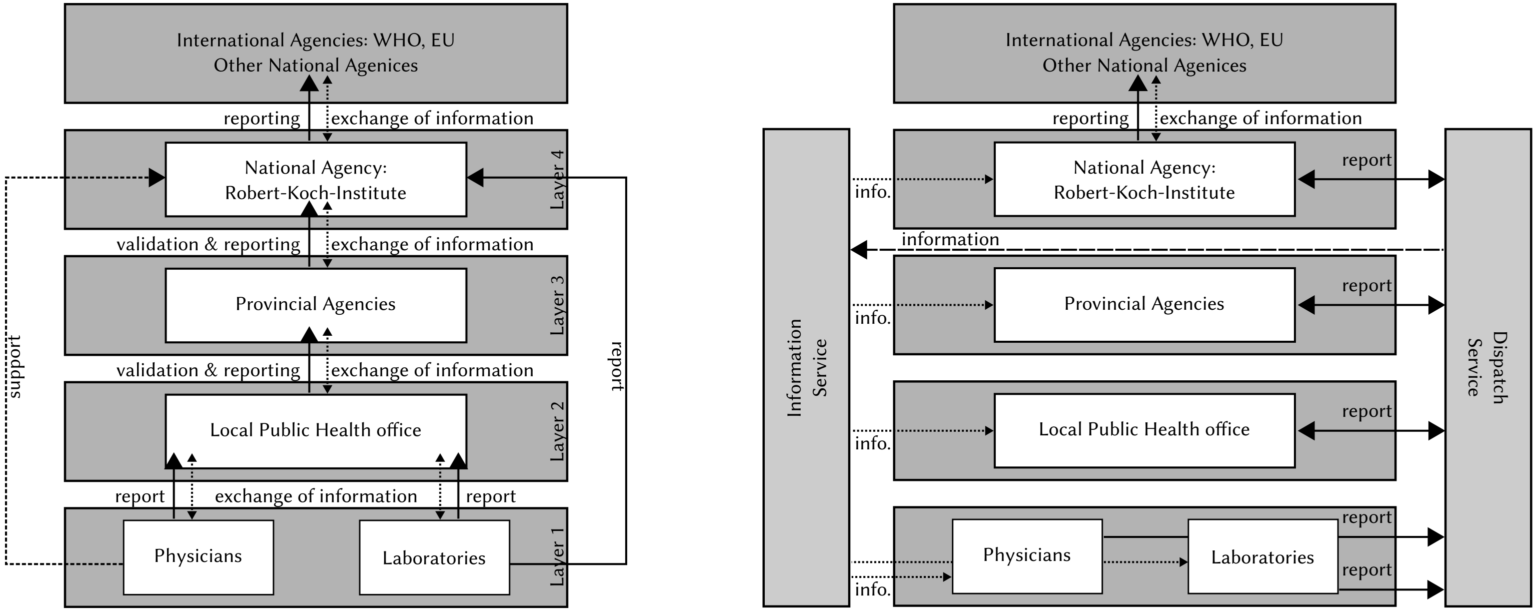


Figure 2.8: Digital signatures are using asymmetric cryptography. A signature is computed with the senders private key. It can be verified with the senders public key.

these diseases, such as Tick-Borne Encephalitis (TBE), hanta-fever, or Legionnaires' disease, spatial distribution is particularly relevant to describe infection risks due to endemicity or outbreak characteristics. Motivated by the EHEC (Verotoxin-producing *Escherichia coli*) outbreak in 2011 and the influenza pandemic in 2009, the German government decided upon developing and testing a new system DEMIS. It enables electronic information exchange about infectious diseases between physicians, laboratories, hospitals and administrative agencies[27], in order to relieve the current paper-based process [38]. It is expected that the electronic system speeds up the reporting-process and lowers the error rate. In addition, information-products about current threats can be created faster and more automated. Figure 2.9a illustrates the current information-flow of infection reports from physician to administrative agency.

[27] URL: http://www.bundestag.de/presse/hib/2013_09/01/257438 (Retr.: 2014-10-07)



(a) Current reporting scheme (redrawn as per: [29, p. 47])

(b) Reporting scheme in DEMIS (redrawn as per: [29, pp. 52])

Figure 2.9: Comparison of the current reporting and information scheme and the scheme used in DEMIS

The information-flow within this infrastructure is mostly linear. Physicians report diseases by letter or telefax to the local public health departments, who then inform the next level in an electronic way. Laboratories are informing the local public health departments and report lab-results to the Robert Koch-Institute (RKI) of the Federal Ministry of Health. As part of the surveillance process, the RKI is creating statistics of the diseases and other information products. Those are communicated back to the health departments, physicians and laboratories. This generation of statistics is also planned within the new infrastructure DEMIS, but in a more sophisticated and automated manner (as illustrated in figure 2.9b).

The new system DEMIS has a different approach to handle the information flow. The electronic reports of the physicians or laboratories will not be sent to the local department, but to a dispatch-service which forwards the reports to the concerning local departments. Only the public health departments receive the complete reports of the physicians, as those contain sensitive data about the infected person. The dispatch service splits of anonymous data from that report and integrates this data into the statistical database of the RKI, which enables the agency to create information products in near real-time. Based upon those statistics, geospatial information products with a low spatial resolution (number of infections per municipality) are also generated. The analyses and information products of the RKI support health departments by means of situation assessment and threat analysis, they also provide a situation assessment on the national scale. With the current legislation, information products with a higher spatial resolution cannot be generated by the federal institutions. This is caused by the rule that sensitive data is stored and processed at the local public health departments only.

Exchange of information between DEMIS, physicians and the government is realised with two sets of technology stacks. On the one hand the *Telematik*-infrastructure (Telematik is a combination of the words telecommunication and informatics, abbrev.: TI) which is typical for the electronic information exchange between physicians, on the other hand the Germany Online Infrastructure (DOI) which depicts the infrastructure for electronic exchange of data between German government departments.

2.4 Related work

This section lists some scientific works that address problems of the integration of geospatial services into e-Government applications.

User authentication and authorisation in GIS
User authorisation and authentication for SDI exists since at least eleven years. Gartmann and Jungermann introduced and implemented a concept for access control in 2003 [39, 40]. Nevertheless, such access prevention and control systems have not been integrated into the standards portfolio of the OGC.

Matheus and Higgins state in their alternative implementation of an access control framework that the OGC is not concerned with security [41]. While access control and user authorisation are already well explored and sufficient solutions exist (e.g. GeoXACML [42]), the OGC or other standardisation organisations did not come up with a proposal for a service which serves as an authentication and authorisation endpoint for geospatial services.

In the recent project ARe3NA AAA [43], a testbed was created which implemented an access management and control infrastructure for INSPIRE on an European level. The project took care of *authentication* and *authorisation* within SDIs, the third A, *accountability*, was out of focus. Accountability in the terms of ARe3NA includes “tracking and controlling the use of content, rights, licences and associated information”[43].

Data from GIS in litigation
Some work exists, that considers the legal situation of GIS in courtrooms of the United States. The situation in Germany and the member states of the European Union might differ significant from the situation in the United States.

In an article from 1992, Onsrud [44] discusses the use of data from GIS as evidence in courtrooms in the United States of America. After discussing four exemplary scenarios, he concludes that most electronic data is is just considered as hearsay and not as a proof, as digital data might have been altered. He mentions the use of digital signatures as a possible solution for this problem.

Dischinger and Wallace describe in their article [45] that the authenticity of GIS evidence is very important for the use of GIS in litigation. The Earth Resources Observation and Science (EROS) center of the United States Geological Survey (USGS) developed an own process chain to enable the use of digital spatial data in courtrooms. The process chain is based on serial numbers for each digital product, which are registered at the USGS [46]. Nevertheless, this process is only applicable if data is transferred with digital media like CDs or DVDs. It is not applicable to a service based approach like an SDI.

The situation in Europe is considered in [47] by Hoeren, here digital signatures are required in order to use a digital document in court, too. However, the analysis focuses on documents (e.g. files) and not on a web-service based approach.

3 Use-case analysis

This chapter aims at finding applications and scenarios which require standards from the e-Government domain, like those from the OSCI suite, as well as standards from the geospatial domain, like those enforced by INSPIRE. Use-cases and possibilities listed in here would benefit or originate from an integration of SDI into e-Government applications by making use of e-Government standards for information transport. With the help of the use-case analysis, the demands on a transport infrastructure, which is necessary for an integration of SDI into e-Government processes, are found.

The listed use-cases were identified in telephone interviews with experts from the geospatial and e-Health domain. The group of experts from the geospatial domain was distributed about several hierarchical levels, reaching from federal (Bundesamt für Kartographie und Geodäsie / GDI-DE), over provincial (GEObasis.nrw / GDI-NRW), to municipal (Paderborn, Lippstadt) agencies. The group of experts from the e-Health domain, came from the federal level (Robert-Koch-Institut) and the municipal level (Kreis Neuss).

In order to find the use-cases, it is assumed that exchange of geospatial information is possible by using transport-protocols from non-geospatial e-Government applications. Afterwards it is conjectured which use-cases would exist and which process might benefit in such a case. The last step is to deduce the requirements of such a use-case.

This chapter finishes with a conclusion of the identified use-cases, which summarises their requirements.

3.1 Closer collaboration of registry of deeds and land-use cadastres

In Germany, the registry of deeds (“Grundbuchamt”) is seated within the local courts (“Amtsgericht”). The registry of deeds registers the address of a parcel, the name of the owner, the number of the parcel within the land-use cadastre, usage

rights and claims of creditors. The registry does not store geographic coordinates of a parcel. Those have to be looked up at the land use cadastre. In North-Rhine-Westphalia, information is exchanged between registry of deeds and the land-use cadastre with text-files and servers using the simple File Transfer Protocol (FTP). If spatial data needs to be exchanged, paper based approaches are used[1].
A closer connection of e-Government applications and geospatial services would provide means of legally binding electronic transport of geospatial data and would allow to easily merge information stored at the registry of deeds and the land-use cadastre. If a solution for the integration of geospatial data services into e-Government applications, which enables legally binding information exchange with geospatial data services, is found the data exchange process between cadastre and registry of deeds can be improved. The registry of deeds can make stronger use of GIS, which will make the exchange of printed maps dispensable.
In order to enable exchange between the registry of deeds and the cadastre, it is important that the communication is traceable to see when an information was transmitted. Communication also needs to be legally binding, and the authenticity and integrity of the information needs to be assured, in order to sustain the authoritative character of the data.

This use-case demands:

- Legally binding communication
- Authenticity
- Confidentiality (optional)
- Integrity
- Traceability

3.1.1 Self-service portals

A new generation of self-service portals for citizens could be created. Portals which enable a view into the land-use cadastre already exist. With their help, users can obtain copies from the land-use cadastre (“Auszug aus dem Liegenschaftskataster”). Nevertheless, they could be enhanced in multiple ways. In addition to the geodata, which was retrieved from geospatial data services, records from the land register records (”Grundbuchauszug“), could be obtained from these portals.

[1] As per an e-mail conversation with the ministry of justice from 2014-07-21 and 2014-07-23

This is useful for selling property or getting information about a property which is intended to be bought. Portals like these would become a one-stop-shop for authoritative information on property. Reports and records which are created here could be legally binding, authoritative data, as the infrastructure behind the portal uses encryption, consistency and authenticity checks with digital signatures.

Such a use-case demands:

- Legally binding communication
- Authenticity
- Confidentiality
- Integrity
- Traceability

3.1.2 Geocoding in e-Justice systems

In 2022, the use of e-Justice systems will be mandatory [48] in Germany. Correspondence with courts will have to be performed with standardised, secured electronic systems only. SDI could be integrated into these systems, to support a courts decision-making process with spatial information. For instance by automatically geocoding datasets which contain addresses. The attorney can rely on this information, because the data came verifiable from a trustworthy, reliable source and the transport of the information was secured with encryption. Until 2022, a lot of things can change in ICT, requiring adaption to new technologies and responses to new challenges. An integration of SDI into e-Justice systems is desirable, but far away from today's point of view.

This use-case requires:

- Legally binding communication
- Authenticity
- High Confidentiality
- Integrity
- Traceability

3.2 Planning processes

When a municipality has a new planning project, for example a new airport, several contractors are involved. They include planning offices, architects and engineers, all requiring geospatial data for their work. Currently, contractors still receive printed maps or files containing the geospatial data. When geospatial data is updated (e.g. structure removal), it happens that contractors are informed about that change, but continue to work with the outdated data. This is especially expensive when false assumptions were made from the outdated datasets. Such errors can manifest in missed deadlines, as well as erroneously build structures.

The availability of geospatial data services for the contractors would enable up-to-date geospatial information retrieval. An electronic exchange of geospatial data, between contractor and agency, reduces the risk of outdated-data, as the agency could have means of monitoring (the contractors) access to the geospatial data service. If new data has not been accessed within a certain timeframe the authority could use other means to inform and remind the contractor about the update. If legally binding communication is enabled, it can even be proved by contractor or agency that a certain dataset was retrieved from the services. Electronic data exchange between contractors and agencies, could reduce errors and helps to match deadlines. The decrease of planning errors caused by outdated geospatial data and the strict keeping of deadlines could also reduce costs of planning processes.

This use-case requires:

- Legally binding communication
- Authenticity
- Confidentiality (optional)
- Integrity
- Traceability

3.2.1 Explosive ordnance disposal

Due to the bombardments of the second world war, unexploded aerial bombs still remain in the ground. In order to find and neutralise these ordnances, the Explosive Ordnance Disposal (EOD) requires geospatial data. Aerial photographs, which where taken during and shortly after the war, are analysed. Those photographs show the impact craters of the bombs, which help to deduce where unexploded ordnances might remain. As those bombs are still dangerous and pose a threat to the population, the EOD is involved into planning processes, and they have to sign off planning-areas as free of ordnance.

The analysis and the inspection of aerial photographs and historic documents alone can be a tedious task. To augment this process, SDIs could be used to provide historic geospatial data. However, todays SDIs are lacking features of legally binding documentation which would meet the requirements of such responsible processes. An integration of SDI into e-Government applications which provide these features of documentation can speed up the process of decision-making as geospatial data can be made available in a faster manner. Results and findings can be documented more easily and sent to the planning-agencies electronically, which simplifies the automated distribution of results and findings. To integrate SDI and e-Government processes with the processes of the EOD, separate analyses must be conducted. This is also conditioned by the different hierarchical structures of the EOD, as each German member state has its own legislation and organisation for this task.

This use-case requires:

- Authenticity
- Integrity
- Traceability

3.3 Emergency services

Emergency services, such as police, fire departments, or ambulances require geospatial data and maps. Geospatial data is considered as priceless information for emergency services. When emergency services ask the land-use cadastre for maps and geospatial data, they often get a PDF-file, a printed map, or access to web-portals. The collaboration of emergency services and land-use cadastres can be improved and sped up by using geospatial data services for information retrieval. Whilst emergency services are available 24/7, the personnel of land-use cadastres is not always available. The web-services of an SDI can close this availability gap. To do so, geospatial services can be integrated with software applications that are used at the emergency services public-safety answering point ("Leitstelle“), providing an up-to-date view on geospatial data.

Due to the importance of emergency services, the interplay of geospatial data service and the application software of the emergency services requires a higher level of protection. Communication between geospatial data services and the emergency services software application should be encrypted to prevent eavesdropping. In addition, emergency services might need access to more detailed maps than the average customer of the land-use cadastre, or maps that may not be made public. Such a need requires access control to services which provide the detailed information. As it is customary in German disaster relief, every order and decision is documented. When integrating geospatial services into e-Government applications of emergency services this documentation must also be supported to facilitate tracing within the decision-making process.

Such a use-case demands:

- Authenticity
- Confidentiality
- Integrity
- Traceability

3.4 Infection reporting systems

E-Health systems can benefit from a collaboration of geospatial services and e-Government applications, for instance in infection reporting. In an infection reporting system, physicians report certain infections to a local authority. Based upon these reports, the authority generates analyses for infections, or act in response to the threat an infectious disease causes. As of now, these reports are sent by mail or telefax to the corresponding authority.

A project which created an electronic infrastructure for these reports already exists with DEMIS (as depicted in section 2.3). Data gathered in this infrastructure can be augmented with the help of SDIs, for instance by providing means of geospatial analysis of the reports. Such geospatial analysis could be realised with a central operated Web Processing Service (WPS), for example. Chapter 4 gets into the details of this use-case.

As data about patients and their health is sensitive, the transport between geospatial service and e-health applications has to be secured. Unfortunately, the broad use of centralised geospatial data services in an infection reporting system might require changes in legislation. Despite of the possible legal problems of an integration of geospatial services into infection reporting systems, they are a promising use-case. The current outbreak of the Ebola-virus in West-Africa could for instance be predicted with the help of news reports, social media and governmental data [49]. With this in mind, better predictions can be expected when geospatial analysis would be possible with qualified medical data. To support the trustworthiness of the predictions, the use of legally binding information exchange and traceable communication are required.

This use-case requires:

- Legally binding communication
- Authenticity
- High Confidentiality
- Integrity
- Traceability

3.5 Emission-reporting

As a final use-case, emission-reporting and trading can benefit from a close collaboration of e-Government applications and geospatial services. For example, the realtime integration of data reported to the German Emissions Trading Authority (DEHSt) into GISs. The DEHSt receives electronic reports from companies which are operating emission sources, e.g. power plants or other industry. Such reports could be analysed in realtime and integrated into geospatial data services, providing up-to-date maps with sources for air pollutants and greenhouse gases. Emission reporting is one of the exemplary use-cases within the OSCI2 requirements specification [50].

Such a use-case demands:

- Legally binding communication
- Authenticity
- Traceability
- Integrity

3.6 Synopsis

Some of the use-cases depicted in this chapter are realistic and in close reach, whilst others require large efforts. The latter can be challenging on the technical side, and/or they need a lot of persuasion to make the agencies see the benefits, because the chances arising from spatial analysis are unknown, or spatial factors are regarded as irrelevant. At least one use-case might even require changes in legislation.

All use-cases in this chapter have strong demands on a transport infrastructure, which have to be met:

- Legally binding communication
- Authenticity of information
- Confidentiality / encryption of information
- Integrity of information
- Traceability of communication

In summary, the transport infrastructure has to provide an *assurance of confidentiality*, which includes measures of data protection like *encryption*, to protect the transported information from the views of third parties. It has to provide an *assurance of integrity* of datasets as well, to detect that a dataset was not corrupted during transport. An *assurance of authenticity* is required, to detect alterations of the dataset which might occur due to third parties which gain access to the transport infrastructure. These three requirements are typical and standard for ICT-systems. In addition to the three standard requirements, an *assurance of tracability* is needed, to keep track who send what in which point in time, as well as an *assurance of legally binding* information exchange, to make the transported information approvable in courts.

4 Integration of geoservices into a federal infection reporting system

Section 2.3 introduced a federal infection reporting system, the use-case analysis in chapter 3.4 identified such an infection reporting system as promising for an integration of geospatial services into e-Government infrastructures which are based on OSCI communication. For the remainder of this thesis, it is hypothesised that DEMIS is not just a research project, but a real existing system, which has a sufficient basis of participating physicians, laboratories and public health agencies.
This chapter shows a concept how standardised geospatial services could be integrated into an e-Health system, thus supporting authorities and administration in decision making processes and threat analysis, and providing new possibilities for scientific research.

Within the concept (depicted in figure 4.1), the public health department receives the infection reports as it is realised in DEMIS. After integrating the report into their local e-Health application, the department transmits the reported addresses to a centrally operated geocoding service. The geocoding service responds with a set of coordinates. The infection report is now spatially enhanced and stored within the e-Health application. In case the e-Health application is capable of displaying reports on a map, users or algorithms might be capable of deducing relations between infected persons and spatial objects, e.g. schools, or other public places more quickly.

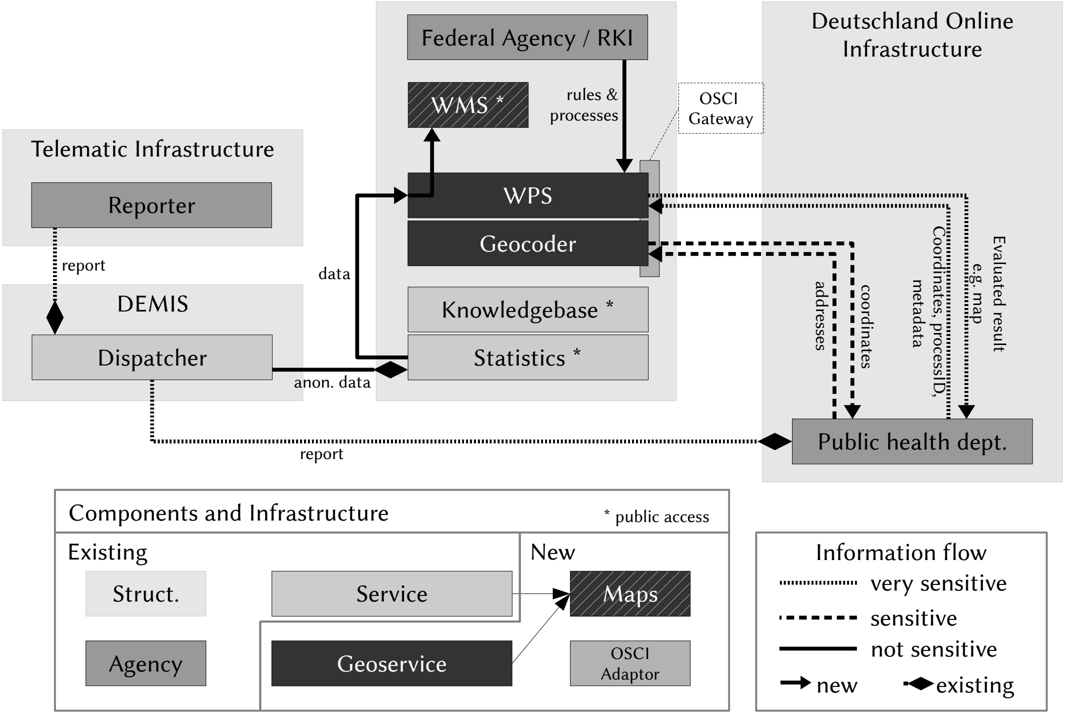


Figure 4.1: Integration of geoservices into an e-Government environment for infection reporting. Sensitive and very sensitive data is transferred in such a scenario. This requires sophisticated security concepts, which can be established with an OSCI-Gateway.

The process of geocoding requires *confidentiality*, because address data which is related to patients is transferred in the geocoding process. Although the data is just an address, and neither symptoms nor names, it might be sufficient to deduce the ill persons identity, e.g. in rural areas. This deduction could for instance be performed by a geocoding-provider that analyses the data stream of its service and concludes that certain requests are made from a public health authority. The provider might then hypothesise that the request is related to a possible sickness. In times of big-data and meta-data analysis, this investigation is still unlikely, but not impossible. In order to prevent such analyses by a third party, a trusted geocoding service must be used. It could be operated by the health office itself or a central organisation, e.g. on a federal level. If the service is an internal service no special protection is required. Nevertheless, public-health offices might lack the resources to operate such a service. In addition, decentralised services might be inefficient, as they create high efforts for maintenance and updating. A better way would be a centralised service. The service would require less resources and could be maintained more easily than a set of decentralised services. Unfortunately, the service requires a more sophisticated data-transport-architecture to guarantee confidentiality.

In addition to the manual analysis of the user, an automated analysis process could take place, in cases when a certain signal or event has occurred, e.g. the number of reports for a disease exceeds a threshold. Such a process might relate to patterns like: "If the amount of today's diagnosed measels-infections exceeds three" then "determine all public-places which are in proximity of the patients". Today, those analyses are based on the users' expertise and experience, and plans which might differ between the public health departments. Thus, it happens that different public health offices are doing different analyses for a similar situation. Such differences complicate comparison of the findings of different public health departments, when doing scientific research afterwards. To simplify the situation, patients' data and meta-data could be analysed by using standardises processes. This could for instance be achieved by analysing the data on the infected patients with the help of a Web Processing Service (WPS).

The WPS is a service which was designed to perform spatial analysis of geospatial data. Although the data is intended to be spatial, it is not mandatory; almost every other statistical analysis is possible. For the sake of simplicity, the WPS is also located in a central place and can be used by all public health departments. The service stores pre-defined processes. A process can, for instance, be started when an input dataset is sent to the service and the process which has to run is specified. If everything went well, the service returns a result.
To achieve comparable results, analysis processes can be pre-defined by federal

institutions, such as the RKI or local or regional agencies. Such predefined analysis processes have the advantages that their results are comparable among different agencies.
Data which is tranferred to the WPS is sensitive as it contains information on patients or people related to the patients. Therefore it has to be transferred in a secure, confidential way. For a public health office, which is responsible for the correct response to the threat of an infection, it is important that data, which was sent to the WPS and was retrieved from, is accurate. As data is sensitive, all data has to be encrypted during transport. In addition, it is required to provide legally binding means of communication, in order to make it possible for the health department to document the conducted analysis. Thus, it is important that the request as well as its response are documented in a legally secure and binding way. To enhance privacy, and meet the requirements of the laws, no data is stored within the service longer than needed to process it.

In addition to the use by the public health departments, the WPS can be used by the RKI in order to generate spatial analyses from low-resolution data. Similar analyses are already conducted by the RKI. They can be retrieved with a web portal[1] which also displays a map. However, this map can not be integrated in to GIS. Using automation of a WPS in combination with a Web Map Service (WMS) to provide near-realtime maps, would reduce response times and could free manpower for more important tasks. In addition, the map-product can be offered via standardised interfaces and can be integrated into common GIS, thus being used more comfortable by public authorities, tourism agencies, physicians, and many more.

The proposed process has several advantages:

- Analyses of data become comparable, as the same processes and methods are used. Until today, there are no standardised processes.
- Expert knowledge enhances processes which are used by all public health agencies, not just a few selected ones.
- Analyses can have a better quality than before.
- Processes and methods can be made public more easily, which allows transparent scientific dispute.
- Errors in reasoning can be found quicker.
- Local public health agencies are safe to assume that the analysis is correct, as it was calculated by using the predefined algorithms.

[1] URL: https://survstat.rki.de (Retr.: 2014-11-19)

The key to the integration of geospatial services into such an environment is the satisfaction of the technical requirements of a secure e-Government infrastructure, as they were defined in chapter 3.6. The transport-protocol OSCI, which was shown in section 2.2.1, is capable of satisfying these requirements. Due to this, the following solution is proposed:

4.1 An OSCI-Gateway for geospatial data services

To integrate geospatial data services into an infection reporting system, the geospatial applications have to become capable of using the OSCI transport protocol. This can be achieved with the help of gateways which act as a component between the e-Health application and the geoservice. The implementation of such a gateway is described in chapter 5.

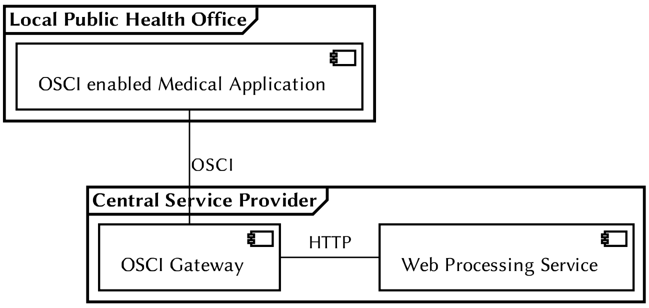


Figure 4.2: Connection of a medical application to a WPS by using OSCI

The task of the gateway is to provide an endpoint for OSCI2 communication. When an e-Health application contacts the gateway, it sends an OSCI message, which is validated and processed according to the OSCI protocol by the gateway. The gateway also performs user authentication and authorisation, as intended by the OSCI specification. After it has processed the OSCI message, the gateway forwards the message to a geoservice, e.g. a WPS. When the gateway receives the response of the geoservice, the response is wrapped into an OSCI message and transmitted to the e-health application which can unwrap this information and process it. Chapter 5 describes how an OSCI-Gateway can be implemented.

5 Implementation of an OSCI-Gateway for geospatial data service

This chapter explores how already existing implementations of OSCI can be integrated into geospatial data services. To do so, it provides information about the Free Open Source Software (FOSS) implementations which are already available and evaluates the suitability of the solution. As it turns out, that available implementations are not fit for integration, the chapter describes an alternative implementation, which prototypically emulates some of the core processes of OSCI communication. With this mockup it shall be shown, that geoservices within an SDI are combineable with the OSCI communication.

5.1 Existing implementations of OSCI

OSCI requires a sophisticated implementation, due to its capabilities of message encryption, signature-verification and authentication, as well as it capabilities to create and handle reception receipts for messages. Thus, an implementation of the OSCI2 is not possible within this thesis. Fortunately, the OSCI2 specification has already been implemented in various ways, amongst them are also FOSS implementations. The following subsections will introduce two of these FOSS implementations, which could be used to create a gateway which connects the e-Government-world using OSCI2 and the spatial-world, using geoservices specified by the OGC:
First, the OSCI-Starterkit which is developed by Bremen Online Services (BOS), and distributed by KoSIT, is analysed. Second the OSCI-Gateway implementation of cit GmbH (CIT) and the Media@komm society, which is distributed by the town of Esslingen is considered.

5.1.1 OSCI2-Starterkit

The OSCI2-Starterkit is a reference implementation of the OSCI2 specification, which aims to support a fast and easy integration of OSCI2 into other applications. It supports synchronous as well as asynchronous message transfer. The Starterkit is licensed under an uncommon, selfmade open-source license, the *Bremer Lizenz für freie Softwarebibliotheken*[1]. The application and samples how to use the OSCI2 protocol are provided by the KoSIT as a zip-file.

Whilst the Starterkit is well documented, it lacks of an up-to-date dependency management for libraries which are required. Thus, the software is challenging to deploy.

5.1.2 OSCI2-Gateway

The OSCI2-Gateway implementation of CIT supports secure and non-disputable communication between applications. It supports synchronous as well as asynchronous message transfer and implements an OSCI-Service component which supports the basic operations of OSCI. This component is intended to act as a bridge between OSCI applications and traditional web-services. The service component is intended to be extended with additional, user-defined interfaces which handle use-case-specific details. The OSCI2-Gateway implementation also contains a RESTful-Interface, which can be used to communicate via OSCI.
According to one of the developers and authors of OSCI2-Starterkit the developments and interests around and in OSCI2 stagnated for some time[2], but they are slowly increasing again.
Unfortunately, the implementation is quite old, thus requiring Java 6, Apache Ant 1.8 and Apache Tomcat 6. An update to support recent versions of Java and Tomcat is planned by the developers, but currently without priority. The OSCI2-Gateway is only provided as a binary file by the city of Esslingen. Documentation of the implementation is unfortunately not included. An incomplete documentation was available after request. Although the application is advertised as FOSS, licensed under the Lesser General Public License (LGPL), the developers where not capable of providing the source-code of the application in time, which makes this solution unusable for a possible implementation.

[1] URL: http://www.xoev.de/sixcms/media.php/13/Bremer_Lizenz.pdf (Retr.: 2014-10-10)

[2] Source: e-Mail conversation from 2014-08-27

5.1.3 Verdict

As shown in the previous subsections, two solutions are existent which are supposed to enable integration of non-OSCI-Services into the OSCI-Infrastructure. Unfortunately, neither of the depicted solutions is currently capable to provide a simple integration of OSCI into other applications. On the one hand, this is caused by a lack of up-to-date dependency-management, as the unusual libraries needed by the OSCI-Implementation are, if at all, provided as files within the implementation, making integration into other applications challenging. On the other hand, both solutions depend on outdated implementations of Java, which are in addition bound to the proprietary Oracle / Sun version of the Java Development Kit (JDK). The FOSS implementation of java (OpenJDK) is not supported, according to the documentation.
This lack of compatibility and also the missing source-code make integration of OSCI an extensive undertaking. Although the existing OSCI2-Gateway implementation would have been a partial solution for the task, the lack of source-code and the missing documentation crosses out this option. In order to see whether an integration of OSCI with the OSCI2-Starterkit is possible within the time frame of this thesis, an estimation of efforts was conducted (see appendix on page vii). The estimation shows that such an endeavour would approximately consume 94 days of work. This target of an implementation can not be reached within this thesis.

5.2 Technical implementation

As an alternative to the integration of software that implements the OSCI protocols, the concepts of OSCI are implemented in a prototypical solution. The solution mirrors the communication-processes of OSCI as well as some of the core features of OSCI communication. Core features of OSCI contain the enablement of user authentication and authorisation, the conservation of confidentiality due to encryption, checks of the integrity of the communicated information, traceability and legally binding information exchange.

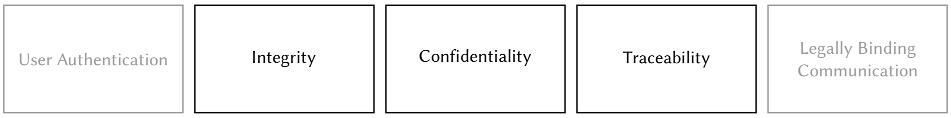


Figure 5.1: Core features of OSCI2. The prototype implements only three of them.

The prototype implements three of the five core features (see figure 5.1) those are: conservation of confidentiality, integrity checks and traceability. Authentication of users is already adequately implemented, for instance in solutions like the Web Security Service (WSS) [40]. Legally binding digital information exchange on the other hand is strictly defined by laws like the *law for digital signatures* [20]. The implementation of this core feature would require a sophisticated PKI, which would also include expensive digital certificates.

5.2.1 Architecture

In order to enable OSCI-styled communication between a geoservice and a GIS two gateways are required. The first one is is called Service Gateway. It is connected to the geoservice. The gateway can act as gatekeeper to protect the geoservice. When an application tries to contact the geoservice the communication is routed over this gateway. Figure 5.2 illustrates the components of this architecture. Towards the geoservice it acts like a normal client.
The second gateway, the Application Gateway, can be an application which runs on a client computer, or an application that runs within the clients network on a server. It provides an entry point for the client into the OSCI-styled communication process. Within the client application, the Application Gateway is configured exactly like the geoservice it proxies.
This architecture is already used within the geospatial domain, for example in applications which are using the WSS and the Web Security Client (WSC). In such scenarios the WSS is the Service Gateway, the WSC is the Application Gateway [40]. Whilst OSCI gateways use SOAP to communicate with each other, this prototypical implementation uses the plain Hypertext Transfer Protocol (HTTP). A request of a Service Gateway is wrapped into a message and send to the Application Gateway by HTTP POST. Each response is wrapped into a message and send as a HTTP-Response to the Service Gateway. The messages are simple array based data structures that differ to the XML messages which are sent in OSCI2 communication. Each message contains content data, meta-data describing the content data, and cryptographic information.

When omitting authentication and delivery receipts, a typical communication sequence (like it is depicted in figure 5.3) within an OSCI-styled architecture (like it was shown in section 2.2.1) would contain the following steps:

At first, the client formulates a HTTP request and sends it to the Application Gateway. The Application Gateway transforms this request into a message. Now the content-data of the message is encrypted and digitally signed by the gateway.

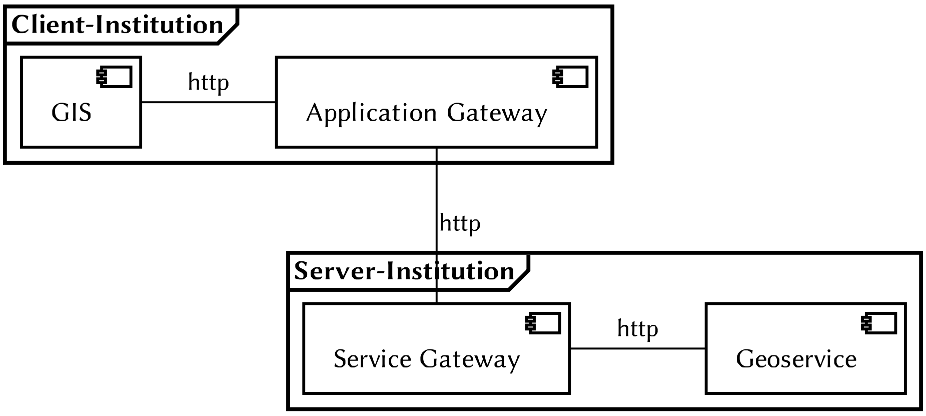


Figure 5.2: Components in an OSCI-styled communication process between GIS and geoservices

The message, containing encrypted data, a digital signature and meta-data, like information about security requirements, is posted to the Service Gateway. When the Service Gateway receives the message, it validates the digital signature and decrypts the message. If the Application Gateway required a delivery receipt it would now be send to the mailbox of the client. When the signature checks were successful, the message is decoded into a request, which is forwarded to the geoservice. The geoservice sends a response, which is received by the Service Gateway and converted into a message. Again, the data within the message is encrypted and digitally signed and annotated with meta-data. This message is sent as a response to the Application Gateway, which validates and decrypts the message. It transforms it into a response that can be handled by the GIS. If a reception-receipt was required by the Service Gateway, the Application Gateway sends this to the corresponding mailbox.

The communication process does only differ slightly from the synchronous message exchange of OSCI2 which was depicted in section 2.2.1 and figure 2.4, as the geoservice is not capable of sending reception receipts when a message was received.

The proposed architecture is transparent for GIS and geoservice. Nevertheless, it has to be expected, that response times increase. In addition further thoughts have to be made on error-handling, for example when signature validation or encryption fail and in how far the user is informed in such cases.

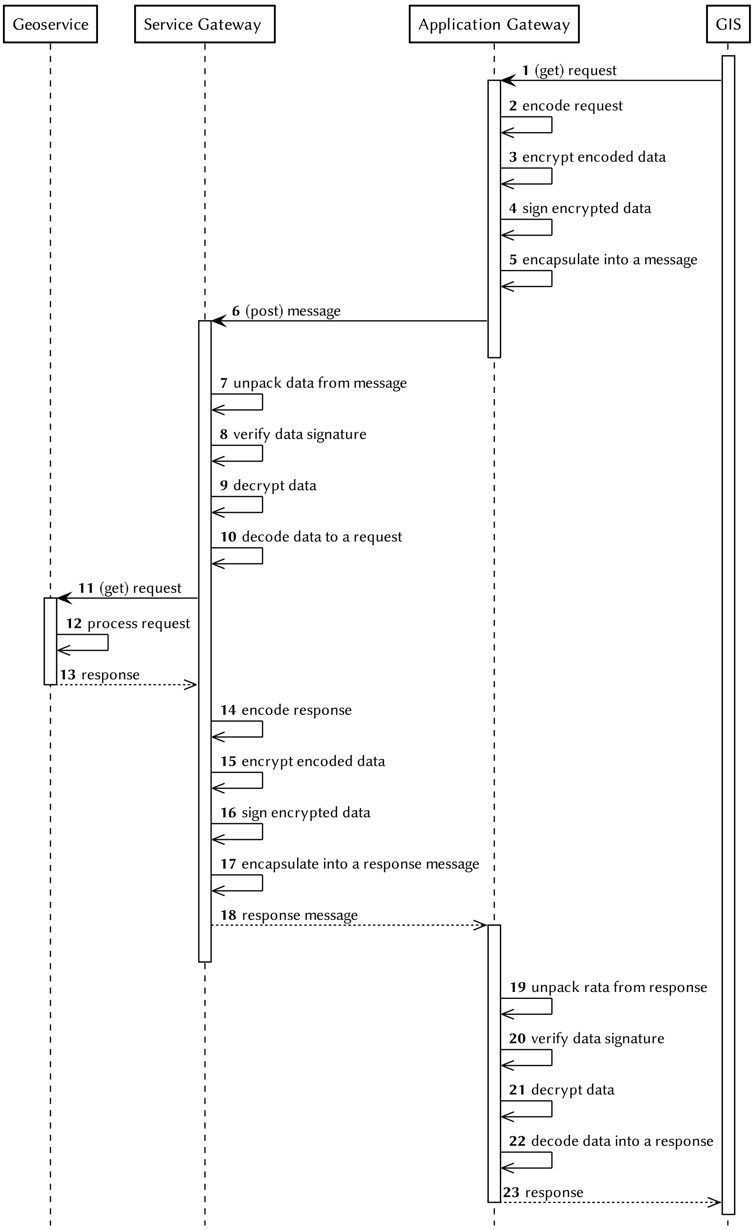


Figure 5.3: Sequence diagram of communication between GIS and a geoservice via a OSCI2-styled communication infrastructure

5.2.2 Application and Service Gateway

Both gateways are implemented as web services in the scripting language PHP. PHP was chosen because it supports rapid development of web-applications, has a good support for the integration of cryptography as well as a native support for mailing systems.

Once the PHP scripts, implementing Application and Service Gateway, have been installed on a web-server, they can be configured to run as an Application Gateway or a Service Gateway or both. The Application Gateway provides an HTTP endpoint which can be used by a client application, for instance a GIS. It processes the request of the client application and forwards it to the endpoint of a Service Application which was configured for the Application Gateway endpoint. The Service Gateway receives this request, processes it and sends the request to a configured service, for instance a WPS.

The configuration also defines policies for a gateway. Within a policy, it is defined if encryption is required or if receipts have to be sent by the counterpart gateway. Table 5.1 lists and describes these policies. Policies define how a gateway has to act and how the structure of a message looks like. They are transferred as separate flags within the transported data-stream between Application Gateway and Service Gateway and vice versa.

5.2.3 Encryption and digital signatures

The gateways make use of GPG to create and verify digital signatures of the datasets transmitted between them. It can also be used to encrypt the datasets. GPG is a cryptographic software which is compliant to the *OpenPGP Message Format* [51]. It is typically used to encrypt and sign e-mail messages, therefore it is an alternative to s/mime with X.509 certificates. GPG combines symmetric cryptography with public-key cryptography to a hybrid cryptosystem (see section 2.2.4), thus creating a fast and secure cryptographic mechanism which uses public-key cryptography. The technology was chosen as it is a strong alternative to X.509 certificates, which does not require a sophisticated PKI, instead GPG makes use of a *Web of Trust* approach [36] to provide trust. Due to the renunciation of a PKI in this implementation, the core feature *legally binding communication* will not be achieved within this implementation, as the law for digital signatures [20] does not consider GPG as a sufficient solution. A non prototypical implementation should use an encryption based on the X.509 standard.

Table 5.1: Policies of a gateway

Policy Name	Description
`DELIVERY_RECEIPT_REQUIRED`	When a gateway receives a message which specifies this policy, it has to send a delivery receipt to the counterpart gateways mailbox.
`RECEPTION_RECEIPT_REQUIRED`	When a gateway receives a message which specifies this policy, it has to send a reception receipt to the counterpart gateways mailbox.
`ENCRYPTION_IS_REQUIRED`	When a gateway receives a message which specifies this policy, it is forced to encrypt its response.
`MESSAGE_IS_ENCRYPTED`	This policy tells the gateway that it has to decrypt the message, before trying to process it otherwise.
`SIGNATURE_IS_REQUIRED`	When a gateway receives a message which specifies this policy, it is forced to digitally sign its response.
`MESSAGE_IS_SIGNED`	This policy tells the gateway that it has to verify the signature of the message, before trying to process it otherwise.

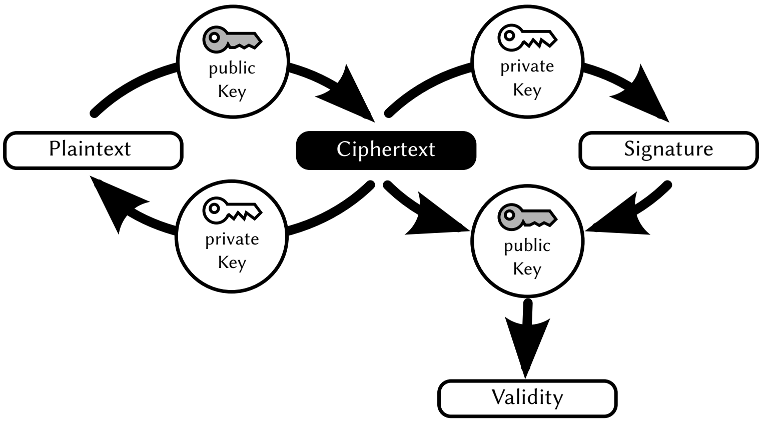


Figure 5.4: The implementation uses the *encrypt-then-sign* approach. In the first step, a the plaintext is encrypted with a hybrid cryptographic system. In the second step, the encrypted text is signed.

In order to determine whether encryption of an information or a digital signature is required, the configured policy of each gateway is used and the flags which were sent by the partner gateway are analysed. When both, encryption and signature, are required, the dataset is encrypted first, then the encrypted dataset is signed. Figure 5.4 shows this approach. Although this approach is prone to attacks like identity forgery [52], it was chosen because it provides sufficient protection for this prototype and is simple to implement.

5.2.4 Receipts and mailboxes

In order to provide traceability and legally binding communication, OSCI makes massive use of reception and delivery receipts. A reception receipt has to be sent by the recipient to the sender of a message, when the target application (ultimate recipient) behind an OSCI gateway has received the message. The delivery receipt is sent by the OSCI gateway to confirm that it forwarded the message to the target application. Receipt process can be compared to the processes that are common in registered mail delivery. In OSCI, intermediaries are used to provide mailboxes which receive these receipts. Within the prototypical implementation standard internet e-mail boxes are used to mockup the receipt process.

To distribute the e-mail address that has to receive the receipt, GPG-keys are used. Each GPG-key is bound to at least one e-mail address. This address is also distributed with the public key, thus it is available for the gateway sending the receipt. In case the partner gateway requires receipts, they are sent to the mailbox defined in the partners public key.

The receipts are digitally signed e-mail messages which contain a hash-value of the transported dataset. To make verification possible, each gateway sends the hash-value of the dataset to its own e-mail address. When a reception is received, the partner gateway sends a hash-value of the received dataset to the senders e-mail address. Now it is possible for a user to compare the hash-values. Currently this has to be done manually. If the hash-values are identical, the message arrived at the partner gateway and it is safe to assume that the message was not altered or tempered with.

5.2.5 Response times

A brief test for response time was conducted. In this test a WPS GetCapabilities request was sent to the WPS and the time was measured which was needed from beginning to the end of communication. To receive a reference time, a request was directly sent to the WPS. Later multiple requests were made using the gateway infrastructure and required encryption and signature or different kinds of receipts. Table 5.2 depicts the outcome of this test.

Table 5.2: Comparison of response times for a WPS-GetCapabilities Request

Operation	Time
Direct Request to WPS	39 ms
Encryption Required	945 ms
Delivery Receipt Required (1 e-mail)	3405 ms
Reception Receipt Required (5 e-mails)	14482 ms

As expected in the architecture section, response times increase (factor 25) due to encryption and digital signature. Less expected was the massive increase of the response times (factor 90 to factor 360) when sending the receipts. To rule out problems, this test was repeated multiple times. However, the increase of response times due to the e-mail dispatch remained high.

The increase in response times due to encryption and signature is manageable, however, the heavy increase due to the dispatch of the receipts can become a problem. This problem could be addressed with multithreading by moving the processes for e-mail dispatch into a background process.

5.3 Application to the use-case

In order to apply the developed technology to the use case, the gateways have been distributed to two different machines, one acting and configured as an Application Gateway on the client side, the other one acting and configured as a Service Gateway on the server side. On a third machine a WPS was installed as a geoservice. This infrastructure is depicted in figure 5.5.

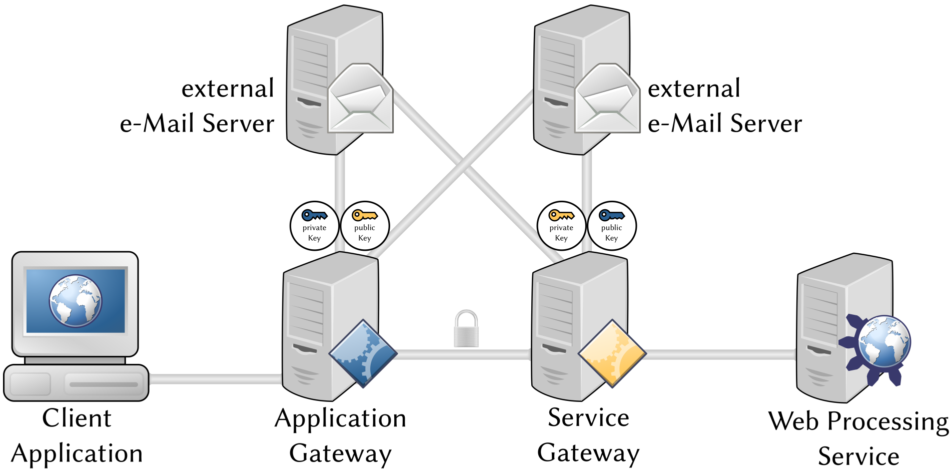


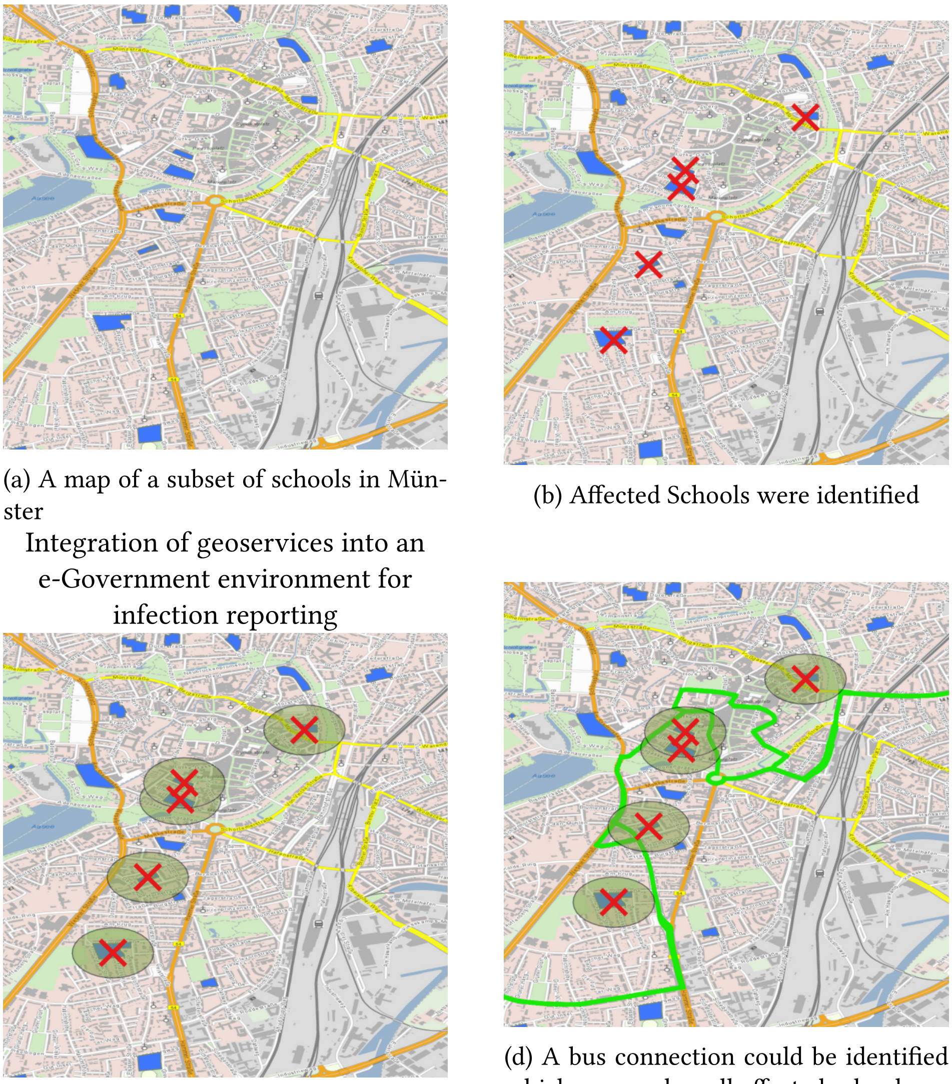
Figure 5.5: Infrastructure of the prototypical implementation

The client application uses the Application Gateway as if it was a WPS. Services behind the Application Gateway are invisible to the client application. Requests and responses to and from the WPS are processed and transferred between Application Gateway, Service Gateway and the WPS behind it. Within DEMIS the client application would be an e-Health system and the Application Gateway would be located at the public health office. The Service Gateway would be located at the institution which provides the WPS. In this prototypical setaup a GIS was used as a client and the WebFormClient of the WPS was used to communicate with the service.

To test the the usability of the proposed solution, a scenario was created. In this very simplified, fictitious scenario the Norovirus, causing infectious diarrhoea, breaks out in several schools in Münster. The outbreak happens almost simultaneously and connections between the schools are unknown. Interviews with the patients and their families were inconclusive. To perform an analysis, the schools, which are visited by the patients, were mapped (see figure 5.6a). Their locations could be derived from the information gathered in the infection reports, according to the law for infection protection [37] (see figure 5.6b).
With the help of the "OSCI-mocked" WPS, a simple spatial buffer around the affected schools was calculated (see figure 5.6c).

As the WPS is integrated into the OSCI-mockup infrastructure, receipts are sent to the the configured mailboxes. For this setup two mailboxes were created. One owned by the Application Gateway, the other one is owned by the Service Gateway. The first message, as visualised in figure 5.7a, is sent by the Application Gateway to its own Mailbox, in order to start a new Mail-thread and announce a hashed value of the dataset that is transmitted to the Service Gateway. To assure the validity of this message, it is digitally signed by the Application Gateway. The second e-Mail, visualised in figure 5.7b, which is received in the Application Gateways Mailbox is a confirmation of receipt which was send by the Service Gateway. This message contains a hashed value of the data which was received. In order to verify the validity of the message, it is digitally signed by the Service Gateway. Now the user is capable of validating whether the received data was identical to the sent data. By comparing the hashed values, the user concludes everything went well. If the hashes do not match, it is likely that the data was tempered with or an error occurred.
The same process happens for the response of the Service Gateway. This time the Service Gateway starts a new e-mail thread, and the reception receipt is sent by the Application Gateway. In cases where delivery receipts are not required, in total four e-mails are transmitted for each transaction, two for a request and two for a response. If delivery receipts are required, an additional e-mail is sent by the Service Gateway to the Application Gateway to confirm that the data was delivered to the Service Gateway.

After the buffer around the schools was calculated, the analyst added features to the map which are known to be places with high infection risks. Such places contain public places, swimming baths, subways or bus connections. The map showed, that one special bus connection is in close proximity to all schools (see figure 5.6d). After additional research this bus route could be determined as the vector for the infection of the pupils.



(a) A map of a subset of schools in Münster

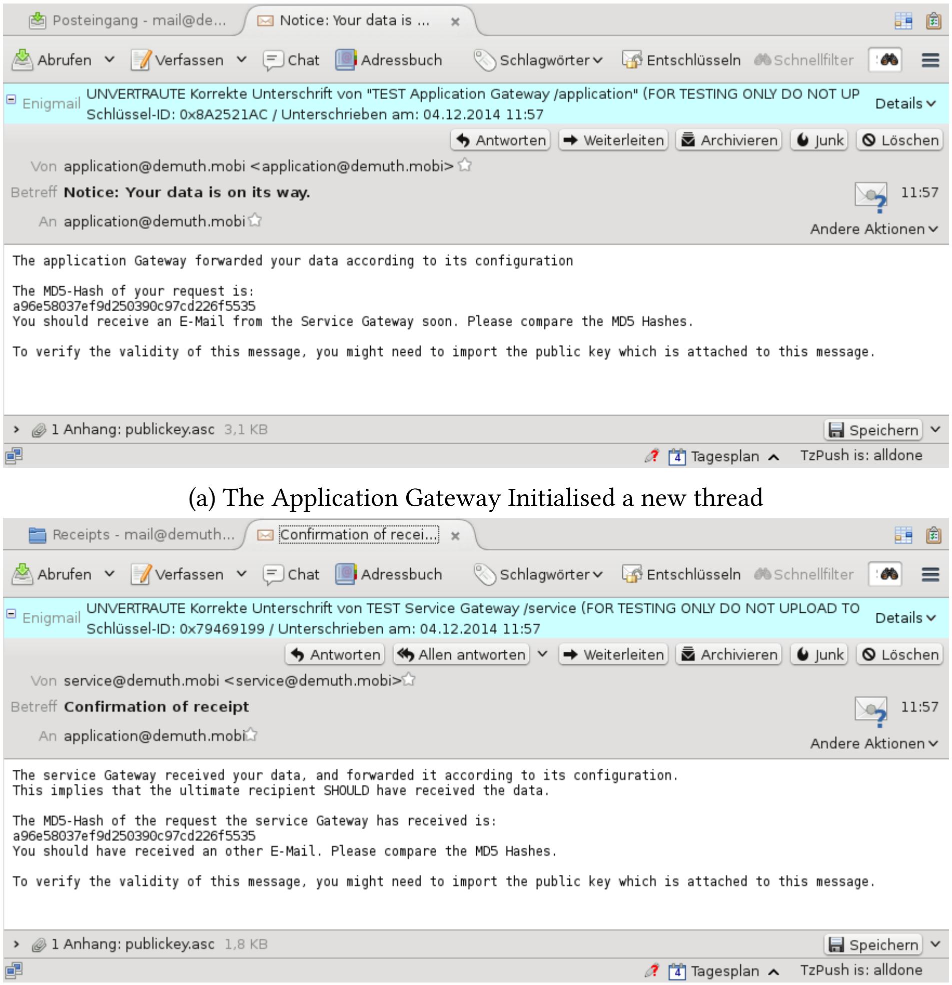
(b) Affected Schools were identified

Integration of geoservices into an e-Government environment for infection reporting

(c) The WPS was used to draw a 200m buffer around the schools

(d) A bus connection could be identified which approaches all affected schools

Figure 5.6: Steps of the analysis process (Background map is courtesy of GeoBasis-DE / BKG 2014 WebAtlasDE, Schools and Bus routes are property of the OpenStreetMap Contributers)



Enigmail UNVERTRAUTE Korrekte Unterschrift von "TEST Application Gateway /application" (FOR TESTING ONLY DO NOT UP
Schlüssel-ID: 0x8A2521AC / Unterschrieben am: 04.12.2014 11:57

Von application@demuth.mobi <application@demuth.mobi>
Betreff **Notice: Your data is on its way.** 11:57
An application@demuth.mobi

```
The application Gateway forwarded your data according to its configuration

The MD5-Hash of your request is:
a96e58037ef9d250390c97cd226f5535
You should receive an E-Mail from the Service Gateway soon. Please compare the MD5 Hashes.

To verify the validity of this message, you might need to import the public key which is attached to this message.
```

1 Anhang: publickey.asc 3,1 KB

(a) The Application Gateway Initialised a new thread

Enigmail UNVERTRAUTE Korrekte Unterschrift von TEST Service Gateway /service (FOR TESTING ONLY DO NOT UPLOAD TO
Schlüssel-ID: 0x79469199 / Unterschrieben am: 04.12.2014 11:57

Von service@demuth.mobi <service@demuth.mobi>
Betreff **Confirmation of receipt** 11:57
An application@demuth.mobi

```
The service Gateway received your data, and forwarded it according to its configuration.
This implies that the ultimate recipient SHOULD have received the data.

The MD5-Hash of the request the service Gateway has received is:
a96e58037ef9d250390c97cd226f5535
You should have received an other E-Mail. Please compare the MD5 Hashes.

To verify the validity of this message, you might need to import the public key which is attached to this message.
```

1 Anhang: publickey.asc 1,8 KB

(b) The Service Gateway send its reception receipt

Figure 5.7: Visualisation of reception receipts in Mozilla Thunderbird with GPG-extension

5.3.1 Synopsis

In this fictitious scenario, simple geospatial analysis was used to determine the vector of an infection. In real applications the infection-scenarios are far more complex and more sophisticated methods are required to determine the sources and vectors of an infection. Nevertheless, a WPS might be one of the tools which could provide standardised geospatial analysis of infection data. To do so, it requires spatial data important for infection research, such as bus-routes, schools, or public places. Within this simplified scenario, data was not transmitted to the WPS in the format typical for DEMIS, instead standardised Geography Markup Language (GML) was used for the communication with the geospatial service. In an productive environment, the WPS should be capable of processing the data format of DEMIS, thus making the integration of geospatial services into infection reporting systems more easy.

Despite of the successful example, some drawbacks must be considered.

1. The response times of the infrastructure are very long, due to the dispatch of the e-mails.
2. The GIS was not capable of communicating with the WPS, neither directly nor via the OSCI-Mockup, this made the use of the WebFormClient of the WPS necessary.
3. Data received from the WPS could not be processed by the GIS. Additional transformations were necessary to integrate and visualise the data.
4. The GIS is not capable of displaying information on the authenticity / integrity of the received dataset, as it does not have access to the mailbox.
5. Manual validation of the hashes is required.
6. In order to proof that a request / response was performed, both the hash and the request/response need to be archived. The proposed implementation does not include a database which archives the hashes and the data of requests and responses.

Nevertheless, this prototypical and fictitious application showed, that an integration of standardised geospatial service into a infection reporting scenario is possible. The implementation meets geospatial standards as well as the standards of the e-Government domain.

With the help of the receipts in the Application Gateways mailbox, the public health office, which would be conducting the analysis, is capable of proving that they performed an analysis with the help of the WPS. Both Gateways verify the authenticity and integrity of the transferred data. In addition to traceability, authenticity and integrity, all data transferred between Application Gateway and Service Gateway is encrypted so no sensitive information is accessible.

6 Discussion

In this chapter, the findings of this thesis are discussed. First, it is analysed if the proposed solution meets the requirements which were identified in the introduction. After that, the compatibility of the proposed approach to similar solutions is considered briefly. As the results of this thesis were already discussed with experts, the feedback of these discussions is integrated as a third point. This chapter finishes with a conclusion and a brief outlook on future work.

Satisfication of requirements
Chapter 3 deduced five requirements from the use-cases. The prototypical implementation of this thesis satisfies four of them. The *assurance of confidentiality* is met by the use of encryption between Application and Service Gateway. Digital signatures allow an *assurance of integrity* and an *assurance of authenticity* of the transported dataset. An *assurance of traceability* is given with the help of reception and delivery receipts. The assurance which cannot be satisfied by the prototype is the *assurance of legally binding* communication. This is due to the fact, that the chosen encryption and signature method GPG is not compliant to the German law for digital signatures [20].

Compatibility to existing approaches
Security concepts, as well as access control concepts of OSCI are closely related to those proposed as solutions for the ARe3NA AAA project [43]. ARe3NA AAA, did only take care of authentication and authorisation. A solution which is using protocols like OSCI could also take care of aspects of accountability, for instance by generating invoices from reception receipts and associated log-files. This could create additional legal security, as an invoice is only created in cases when the user confirmed the receipt of a dataset.

When considering authentication and authorisation both, OSCI and ARe3NA AAA, make use of access federations, which provide a scalable solution for access control. Also both approaches make use of the same subset of technical standards, which should make both approaches compatible. This possible compatibility is interesting, as it might provide the opportunity to use OSCI-enabled services with authentication and authorisation federations of other European member states. Such a use would enable legally binding communication between OSCI-enabled applications and services, and authentication and authorisation control with applications which are not capable of OSCI. To determine in how far OSCI is compatible to the concepts of the ARe3NA AAA project, further work is required.

Feedback

The proposed solution of this work was presented on a workshop of the GDI-DE initiative[1], which focussed on the architecture of the federal SDI and especially on access control aspects. Findings and solutions of this thesis received positive feedback from the attending experts, which were representatives from several German member-states and federal offices. According to them, the topic is of significance, as legally binding communication was not yet considered for a German SDI, and the collaboration of SDI with other e-Government applications is one of the future tasks. Current services within the German SDIs claim that the provided data might not be correct or complete[2], hence it is impossible to provide legally binding data by using these services.

Participants of the workshop stated, that use-cases which require a sophisticated access control framework that allows cross-border access control in Germany, are unknown. Nevertheless, most of them doubt such use-cases would not exist. The use-cases of chapter 3 did not take cross-border applications into account, still these might happen, for instance in planning processes for large projects, like pipelines or highways or electrical power lines, or in jurisdiction, when cases span across multiple regions.

Anyhow, the proposal has given an impulse to consider the already existing solutions of non-spatial e-Government environments, for example access management and control, as well as other requirements of these environments, like legally binding communication, which have to be met to successfully integrate the German SDI into non-spatial e-Government environments.

In addition to the workshop, the topic was proposed for discussion on the 14th IT-Security Congress of the BSI in 2015 [53]. Unfortunately the proposal was not accepted.

Conclusion

This work analysed and showed which technical requirements have to be met by

[1] Workshop "Zugriffskontrolle GDI-DE", Federal Agency for Cartography and Geodesy, Frankfurt (Main), 2014-11-13

[2] URL: http://www.geoportal.bayern.de/geoportalbayern/seiten/nutzungsbedingungen (Retr.: 2014-11-27)

geospatial data services of an SDI in order to integrate them into e-Government infrastructures. Integration was achieved by using and applying the transport protocol OSCI, which is common in the non-spatial e-Government domain, as a transport mechanism between e-Government applications and geospatial data services. The proposed approach keeps standards of both domains intact, thus it does not harm the compatibility of neither e-Government application nor geospatial data service with already existing applications.

By interviewing experts from the geospatial, as well as the e-Health domain, some use cases have been identified which would emerge from a collaboration of SDI and non-spatial e-Government environments. Possible use-cases are manifold, but they share a subset of requirements which have to be met. The identified requirements are the five core features, *user authentication*, *integrity*, *confidentiality*, *traceable* and *legally binding* communication. Those have to be provided by geospatial data services in order to enable a sufficient integration of them into non-spatial e-Government environments. To meet these requirements it is reasonable to use standards which are well-distributed and wide-spread within Germany.
The protocol OSCI is such a standard. OSCI applications can be implemented as a gateway in order to enable legally binding information exchange, authentication and authorisation, as well as the proof of integrity and authenticity, and preservation of confidentiality in SDIs.

Due to the complexity of OSCI, and the high requirements of security, an integration and adaptation for SDI is challenging. The high implementation efforts which would have been necessary to adapt existing OSCI implementations and the resulting rejection of those, during the implementation within this thesis, were a setback. This setback could be successfully circumvented with a mockup implementation. The mockup implements three of the five core concepts of OSCI and uses a simplified data format to transport the information between the applications. Nevertheless a real implementation of OSCI into SDI can be achieved within a manageable time, when source-code becomes available, or developers and companies which are familiar with the protocol take over the work. In this case, the communication and transport protocol between the OSCI gateways, which was simplified in the mockup, can also remain untouched.

By using the mockup to augment the features and the communication process of OSCI, it was shown that the concepts of secure communication of typical e-Government applications are also applicable to geospatial data services, whilst keeping the existing geospatial standards intact.

In cases when geospatial data services provide an OSCI interface, applications from the e-Government domain, which require this transport technology, can connect to these geospatial data services. Thus, the geospatial services can be integrated into the e-Government applications. Nevertheless, the e-Government application still needs to be capable of processing geospatial data. This issue was not addressed in this work and would require further research.

When using OSCI as a transport technology between GIS and geoservice, the authenticity and integrity of datasets can be proven between the OSCI gateways. As GIS are not capable of using OSCI natively, this assurance is lost between the gateway and the GIS. This means that secure and legally binding communication only possible between the applications which are capable of processing OSCI. Thus it makes a difference whether the OSCI-Gateway is installed a network appliance, serving multiple users, or as a local service on a desktop machine, serving only one user. In the first case, it can only be assured that an information has been received by a network unaltered, in the second case, this assurance can be extended to the desktop machine and the user.

Future work might extend the OSCI protocol to the desktop GIS. If a GIS becomes capable of using OSCI as a transport technology, it could be able to display and process the information about authenticity and integrity of the geospatial datasets. Authenticity and integrity of a geospatial dataset could be verified in the GIS in this case. Such a communication flow could also work the other way around, for instance in cases when a Transactional Web Feature Service is used and information is sent from the GIS to the geoservice. In such cases, the geoservice would be capable of verifying the authenticity and integrity of the received information.

Bibliography

[1] Cisco, Bearing Point, and SAP. *13. eGovernment-Wettbewerb 2014 - Die Gewinner 2014.* German. 2014. URL: http://www.egovernment-wettbewerb.de/gewinner/gewinner-2014.html.

[2] Glenn Vancauwenberghe, Joep Crompvoets, and Danny Vandenbroucke. "Location Information Strategies: Bringing Location into e-Government". In: *Government e-Strategic Planning and Management.* Ed. by Leonidas G. Anthopoulos and Christopher G. Reddick. Vol. 3. Public Administration and Information Technology. Springer New York, 2014, pp. 65–82.

[3] Mapping Science Committee. *Toward a coordinated spatial data infrastructure for the nation.* National Academies Press, 1993.

[4] Ian Masser. *Building European spatial data infrastructures, Second Edition.* Esri Press, 2010.

[5] H.-G. Pöttering and G. Gloser. *Richtlinie 2007/2/EG des Europapäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE).* German. Amtsblatt der Europäischen Union. Europäische Union, 2007.

[6] Bundesministerium des Innerern. *3.Geo-Fortschrittsbericht der Bundesregierung.* German. 2012.

[7] Arbeitskreis Architektur. *Architektur der Geodateninfrastruktur Deutschland.* German. Tech. rep. Arbeitskreis Architektur, 2014.

[8] Bundesrepublik Deutschland. *Gesetz über den Zugang zu digitalen Geodaten (GeoZG).* German. BGBl. Geodatenzugangsgesetz vom 10. Februar 2009 (BGBl. I S. 278), das durch Artikel 1 des Gesetzes vom 7. November 2012 geändert worden ist. Feb. 2009.

[9] Lars Bernard and Ulrich Streit. "Geodateninfrastrukturen und Geoinformationsdienste: Aktueller Stand und Forschungsprobleme". German. In: *Proceedings of the 22. Wissenschaftlich-Technische Jahrestagung der DGPF" Zu neuen Märkten-auf neuen Wegen-mit neuer Technik", Neubrandenburg, Publikationen der Deutschen Gesellschaft für Photogrammetrie und Fernerkundung (DGPF)* (2002), pp. 11–20.

[10] Andreas Claßen. “Ein Schaufenster für Geodaten einrichten”. German. In: *Städte- und Gemeinderat* 3/2013 (2013).

[11] Lutz Rabe. “Langer Weg zum einheitlichen Format”. German. In: *Städte- und Gemeinderat* 3/2013 (2013).

[12] Abbas Rajabifard. “Beyond spatial enablement: engaging government, industry and citizens”. In: *International Conference on Sharing Geospatial Technology, Experience, Knowledge Smart Geospatial Expo 2012*. 2012.

[13] European Commission. *About INSPIRE*. URL: http://inspire.ec.europa.eu/index.cfm/pageid/48.

[14] Jörn von Lucke and Heinrich Reinermann. *Speyerer Definition von Electronic Government*. German. Online-Publikation. June 2000.

[15] European Commission. *The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government*. 2010.

[16] Ministers for e-Government in the Memberstates of the European Union. *Ministerial Declaration on eGovernment*. aka. Malmö Declaration. 2009.

[17] Claudia Gallo et al. *Study on eGovernment and the Reduction of Administrative Burden*. Tech. rep. European Commission, 2014.

[18] European Commission. *EUROPE 2020 - A strategy for smart, sustainable and inclusive growth*. Mar. 2010.

[19] Thomas Zefferer. *E-Government-Dienste in Europa – ein Vergleich von sieben Ländern*. German. Tech. rep. Vodafone Institut für Gesellschaft und Kommunikation GmbH, 2014.

[20] Bundesrepublik Deutschland. *Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG)*. German. BGBl. Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist. May 2001.

[21] Die Bundesregierung der Bundesrepublik Deutschland. *BundOnline 2005 - Umsetzungsplan für die eGovernment-Initiative*. German.

[22] OSCI Leitstelle. *Projektauftrag "OSCI—Transport: Version 1.2"*. German. 2002.

[23] Die Beauftragte der Bundesregierung für Informationstechnik. *SAGA-Modul Technische Spezifikationen - de.bund 5.0.0*. German. 2011.

[24] Manuel Antonio Aldana. “Sicherer Dokumentenaustausch im E-Government mit OSCI und Acrobat/PDF”. German. MA thesis. Technische Universität Berlin Fakultät IV für Elektrotechnik und Informatik, 2007.

[25] OSCI Leitstelle. *OSCI-Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und -mechanismen –*. German. 2002.

[26] Internet Engineering Task Force. *rfc5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Internet Engineering Task Force.

[27] OSCI Leitstelle. *OSCI 2 - Technical Features Overview*. 2009.

[28] OSCI Leitstelle. *OSCI-Transport 1.2 – Spezifikation –*. 2002.

[29] Justus Benzler. "DEMIS - Deutsches Elektronisches Meldesystem für Infektionsschutz". German. In: *Beiträge zum Projekttreffen der epidemologischen und molekularbiologischen Surveillance von HIV in Deutschland*. Robert Koch-Institut, Berlin, 2013.

[30] Tatjana Rubinstein, Jürgen Baum, and Jan Gottschick. *P23R: Spezifikation des P23R-Protokolls*. German. Tech. rep. Ein Ergebnisdokument des Projekts P23R | Prozess-Daten-Beschleuniger im Auftrag des Bundesministeriums des Innern. Fraunhofer ISST, 2012.

[31] Bundesrepublik Deutschland. *Grundgesetz für die Bundesrepublik Deutschland (GG)*. German. BGBl. Vom 23.05.1949 (BGBl. I S. 1) zuletzt geändert durch Gesetz vom 11.07.2012 (BGBl. I S. 1478) m.W.v. 17.07.2012. May 1949.

[32] IT-Planungsrat. *Nationale E-Government Strategie*. German. 2010.

[33] Bundesamt für Informationssicherheit. *Leitfaden Informationssicherheit*. Feb. 2012.

[34] R. Shirey. *rfc2828 - Internet Security Glossary*. May 2000.

[35] W. Diffie and M. Hellman. "New Directions in Cryptography". In: *IEEE Trans. Inf. Theor.* 22.6 (Sept. 2006), pp. 644–654.

[36] *The GNU Privacy Handbook*. The Free Software Foundation. 1999.

[37] Bundesrepublik Deutschland. *Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (IfsG)*. German. BGBl. Infektionsschutzgesetz vom 20. Juli 2000 (BGBl. I S. 1045), das zuletzt durch Artikel 2 Absatz 36 u. Artikel 4 Absatz 21 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist. June 2000.

[38] Justus Benzler. *DEMIS Deutsches Elektronisches Meldesystem für Infektionsschutz*. German. Robert Koch Institut. 2013. URL: https://www.lzg.gc.nrw.de/_media/pdf/service/veranstaltungen/130410_nrw-dialog_11/benzler_DEMIS_10-04-2013_dortmund.pdf.

[39] Rüdiger Gartmann and Felix Jungermann. *Zugriffskontrolle in Geodateninfrastrukturen: Der Web Authentication and Authorization Service (WAAS).* German. Tech. rep. 2003.

[40] Jan Drewnak and Rüdiger Gartmann. "Zugriffkontrolle in Geodateninfrastrukturen: Web Authentication Service (WAS) und Web Security Service (WSS)". German. In: *Geodaten- und Geodienste-Infrastrukturen - von der Forschung zur praktischen Anwendung*. Ed. by Kristian Senkler Lars Bernard Adam Sliwinski. Institut für Geoinformatik Universität Münster. June 2003.

[41] Andreas Matheus and Chris Higgins. "A Shibboleth Service Provider for OGC Web Map Services". In: *CCS'09* (2009).

[42] Jan M. Herrmann. "Zugriffskontrolle in serviceorientierten Architekturen am Beispiel von Geodateninfrastrukturen". German. PhD thesis. Technische Universität München – Forschungs- und Lehreinheit XI – Angewandte Informatik / Kooperative Systeme, 2011.

[43] Ann Crabbé et al. *ARE3NA (D1.1.1 & D1.2.1) Authentication, Authorization and Accounting for Data and Services in EU Public Administrations: Analysing standards and technologies for AAA*. Tech. rep. For Review only. Joint Research Centre, 2014.

[44] Harlan J Onsrud. "Evidence generated from GIS". In: *GIS Law* 1.3 (1992), pp. 1–9.

[45] Sally Speers Dischinger and Lyle A. Wallace. "Geographic Information Systems: Coming to a Courtroom Near You". In: *The Colorado Lawyer* Vol. 34.4 (Apr. 2005), pp. 11–23.

[46] Ronald J. Rychlak, Joanne Irene Gabrynowicz, and Rick Crowsey. "Legal Certification of Digital Data: The Earth Resources Observation and Science Data Center Project". In: *Journal of Space Law* 33.1 (2007), pp. 195–219.

[47] Thomas Hoeren. "Beweiswert Digitaler Dokumente - Eine EU-Perspektive". German. In: *Internet-Recht und Digitale Signaturen*. Ed. by Simon Schlauri, Florian S. Jörg, and Oliver Arter. Vol. 6. Stämpfli Verlag AG, 2005, pp. 83–101.

[48] Bundesrepublik Deutschland. *Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERVGerFöG)*. BGBL. Oct. 2013.

[49] Morgan Peck. *Algorithm Detected Ebola Outbreak Before Official Alerts.* 2014. URL: spectrum.ieee.org/tech-talk/biomedical/diagnostics/healthmap-algorithm-ebola-outbreak.

[50] OSCI Leitstelle. *OSCI-Transport, Version 2 – Funktionale Anforderungen und Entwurfsziele –*. June 2009.

[51] Network Working Group. *rfc4880 - OpenPGP Message Standard.* 2007.

[52] Don Davis. “Defective Sign &; Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML”. In: *Proceedings of the General Track: 2002 USENIX Annual Technical Conference.* Berkeley, CA, USA: USENIX Association, 2001, pp. 65–78.

[53] Dustin Demuth. “Integration standardkonformer Geodatendienste in sichere e-Government Infrastrukturen”. German. Kurzfassung - Einreichung für 14. Deutscher IT-Sicherheitskongress. Aug. 2014.

Appendix

List of Figures

List of Tables

List of Abbreviations

AAA	Authentication, Authorisation, Accountability
AES	Advanced Encryption Standard
BOS	Bremen Online Services (The Company was renamed to Governikus GmbH & Co. KG)
BSI	Federal Office for Information Security (Ger: Bundesamt für Informationssicherheit)
CAD	Computer Aided Design
CIT	cit GmbH
DEHSt	German Emissions Trading Authority (Ger: Deutsche Emissionshandelsstelle)
DEMIS	German electronic system for infection reporting (Ger: Deutsches elektronisches Meldesystem für Infektionsschutz)
DOI	Germany Online Infrastructure (Ger: Deutschland Online Infastruktur
EC	European Commission

EOD	Explosive Ordnance Disposal
EROS	Earth Resources Observation and Science
FOSS	Free Open Source Software
FTP	File Transfer Protocol
GIS	Geographic Information System
GML	Geography Markup Language
GPG	GNU Privacy Guard
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
INSPIRE	Infrastructure for Spatial Information in the European Community
IT	Information Technologies
KoSIT	Coordinating Office for IT-Standards (Ger: Koordinierungsstelle für IT-Standards)
LGPL	Lesser General Public License
MEP	Message Exchange Pattern
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OSCI	Online Services Computer Interface
PDF	Portable Document Format
PHP	PHP: Hypertext Preprocessor originally: Personal Home Page
PKI	Public Key Infrastructure
REST	Representational state transfer
RKI	Robert Koch-Institute
SAGA	Standards and Architectures for e-Government Applications (Ger: Standards und Architekturen für e-Government-Anwendungen)
SDI	Spatial Data Infrastructure

SOAP	Simple Object Access Protocol / Service Oriented Architecture Protocol (These terms are not used anymore. Today SOAP is not being used as an acronym, but as a name on its own)
SSH	Secure Shell
USGS	United States Geological Survey
W3C	World Wide Web Consortium
WFS-T	Transactional Web Feature Service
WLAN	Wireless Local Area Network
WMS	Web Map Service
WOT	Web of Trust
WPA	Wi-Fi Protection Access
WPS	Web Processing Service
WSC	Web Security Client
WSDL	Web Service Description Language
WS-I	Web Services Interoperability Organization
WSS	Web Security Service
XML	Extensible Markup Language
XÖV	XML in public administration (Ger: XML in der öffentlichen Verwaltung)

Evaluation of efforts

Component	**Task**	**Subtask**	**Min Effort**	**Max Effort**
Take infrastructure into operation				
	Geoservice			
		Installation	1	2
		Encryption	1	2
		Make data available	1	2
	GIS	Installation	0.5	1
	Gateway 1			
		Installation	1	2
		Configuration	1	2
	Gateway 2			
		Installation	1	2
		Configuration	1	2
	Server 1 (C. GW)	Installation	0.5	1
	Server 2 (S. GW)	Installation	0.5	1
	Server 3 (GS)	Installation	0.5	1
Implementation				
OSCI-Gateway Application-Gateway				
	Offer HTTP Server Endpoint	--	5	10
	Receive HTTP Request	--	1	2
	Configuration of Application Endpoint	--		
		Create configuration schema	1	2
		Read configuration	0.5	1
		Apply configuration	10	15
	Send a synchronous OSCI-Message	--		
		Identification of the partner endpoint	0.5	1
		Convert request to Base64	0.5	1
		Signature	2	OSCI
		Encryption	2	OSCI
		Dispatch	2	OSCI
	Receive a synchronous OSCI-Message	--		
		Wait for OSCI-Response	1	OSCI
		Decryption	1	OSCI
		Signaturechecks	1	OSCI
		Decode Response from Base64	0.5	1
	Forward HTTP Response to the GIS	--	1	2

Evaluation of efforts

Component	**Task**	**Subtask**	**Min Effort**	**Max Effort**	
OSCI-Gateway Service-Gateway					
	Configuration of Service Endpoint	--			
		Create configuration schema	1	2	
		Read configuration	0.5	1	
		Apply configuration	10	15	
	Receive a synchronous OSCI-Message	--			
		Offer a Serverendpoints for OSCI	?	?	
		Decryption	1	OSCI	
		Signaturechecks	1	OSCI	
		Decode Response from Base64	1	OSCI	
	Act as a HTTP-Client	--			
		Forward OSCI-Message content as a HTTP request	1	2	
		Receive the response of the geoservice	1	2	
	Send a synchronous OSCI-Message	--			
		Identification of the partner endpoint	5	10	
		Convert request to Base64	0.5	1	
		Signature	1	OSCI	
		Encryption	1	OSCI	
		Dispatch	1	OSCI	
	Define Testcases		1	2	
	Apply Tests		2	3	
	Evaluate Tests		2	3	
Documentation					
	Architecture		2	4	
	Manual		7	12	
	Provide FOSS Code online		0.5	1	
					Mean
Sum			**77.5**	**111**	**94.25**

License

Graphics, figures and texts of this work, which are not marked as third-party content, trademarks or quotes are licensed under the Creative Commons Namensnennung 3.0 Deutschland License.

Program sources of the Application and Service Gateway which are described in this work are licensed under the MIT License. Application and Service Gateway make use of third party libraries. Those are:

httpful - a library to make http-requests and process the response, licensed under MIT License
phpmailer - a library to send e-mails with PHP, licensed under LGPL 3
Crypt_GPG - a library to interact with GPG, licensed under LGPL 2.1

Sourcecode

The sourcecode for the implementation of this work can be downloaded at:
https://github.com/dmth/php-gpg-gateway

Plagiarism statement

Hiermit versichere ich, dass die vorliegende Arbeit über *Integration of geospatial services into e-Government applications based on e-Government and SDI standards* selbstständig verfasst worden ist, dass keine anderen Quellen und Hilfsmittel als die angegebenen benutzt worden sind und dass die Stellen der Arbeit, die anderen Werken – auch elektronischen Medien – dem Wortlaut oder Sinn nach entnommen wurden, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht worden sind.

Münster, 22. Dezember 2014 ______________________________