Master Thesis

im Rahmen des Universitätslehrganges
„Geographical Information Science & Systems“
(UNIGIS MSc) am Zentrum für GeoInformatik (Z_GIS)
der Paris Lodron-Universität Salzburg

zum Thema

Konzeption eines Sicherheitsframeworks für eine Open Source-basierte Geodateninfrastruktur

vorgelegt von

Dipl. Ing. FH Rolf Mühlemann
U1219, UNIGIS MSc Jahrgang 2005

Zur Erlangung des Grades
„Master of Science (Geographical Information Science & Systems) - Sc(GIS)”

Gutachter:
Ao. Univ. Prof. Dr. Josef Strobl

Basel, 18. Juli 2007

Danksagung

Diese Arbeit stellt den Abschluss des Master Studiengangs „Geographical Information Science and Systems“ an der Paris Lodron-Universität Salzburg dar. An dieser Stelle möchte ich mich bei allen bedanken die mich vor und während den Arbeiten zu dieser Master Thesis unterstützt haben.

Ein besonderer Dank geht dabei an Dr. Martin Huber, der mich bei der Ideenfindung, Konzeption und Umsetzung dieser Arbeit unterstützt und beraten hat. Durch seine zahlreichen konstruktiven und kritischen Anregungen hat er massgeblich zum Ergebnis dieser Arbeit beigetragen.

Im Weiteren möchte ich mich bei Hannes Eugster und Tobias Henz für die redaktionelle und fachliche Durchsicht dieser Arbeit und die guten Hinweise bedanken.

Ein Dank geht auch an Fabio Di Pietro (GIS-Fachstelle des Kantons Basel-Landschaft) und Horst Düster (Amt für Geoinformation des Kantons Solothurn) für ihre Bereitschaft in der Anfangsphase dieser Arbeit die Anforderungen und Bedürfnisse im Umfeld von GDIs zu diskutieren.

Zuletzt möchte ich mich bei meiner Familie und bei meiner Freundin Ines bedanken, die mich in den letzten zwei Jahren - und im Speziellen in den letzten paar Wochen - trotz zahlreicher Entbehrungen immer wieder motiviert und unterstützt haben.

Eigenständigkeitserklärung

Ich versichere, diese Master Thesis ohne fremde Hilfe und ohne Verwendung anderer als der angeführten Quellen angefertigt zu haben, und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat. Alle Ausführungen der Arbeit die wörtlich oder sinngemäss übernommen wurden sind als solche gekennzeichnet.

Basel, 18. Juli 2007

Rolf Mühlemann

Anmerkung:

Aus Gründen der Übersichtlichkeit und Lesbarkeit wurde in dieser Arbeit auf eine geschlechterspezifische Schreibweise verzichtet. Die gewählte männliche respektive weibliche Formulierung ist in diesem Sinne geschlechtsneutral zu verstehen.

Zusammenfassung

In den letzten Jahren haben viele private und öffentliche Institutionen und Körperschaften ihre Geodaten in Form von einfachen Web Services oder umfangreichen Geodateninfrastrukturen (GDIs) veröffentlicht. Die Sicherheit dieser Dienstleistungen stellt eine wesentliche Grundanforderung für deren kommerzielle Nutzung in verteilten Infrastrukturen dar. Im Rahmen von GDIs werden diese Aspekte jedoch oft vernachlässigt, da es an übergeordneten Konzepten fehlt, um eine durchgehende Sicherheit auch mit begrenzten finanziellen Mitteln gewährleisten zu können. Im Rahmen dieser Arbeit wird mit der Konzeption eines Sicherheits-frameworks gezeigt, welche Standards und Spezifikationen im Bereich von GDIs und Web Services derzeit existieren, welche Sicherheitsaspekte diese abdecken und wie sie in einen Gesamtkontext eingeordnet werden können. Im Zentrum stehen dabei die Nutzung von offenen und etablierten Standards aus dem IT-Umfeld und die Analyse der bestehenden Spezifikationen aus dem GIS-Umfeld.

Keywords: Sicherheit, Framework, Geodateninfrastruktur, GDI, Web Service

Abstract

In the recent past many private and governmental organizations have started to provide their geodata using simple Geo web services or more complex Spatial Data Infrastructures (SDIs). The security of these services is now recognized as a crucial base requirement for their commercial use. This aspect has often been disregarded due to the lack of an overall concept which guarantees complete security with limited resources. In the scope of this Masters thesis a Security Framework has been drafted in order to illustrate and document the functionality of numerous standards and specifications in the range of SDIs and Geo web services. Based on these cognitions, the relevant standards and specifications have been integrated into an aggregated context. Thereby the focus has been directed to the use of open and established IT standards and existing specifications for the SDI environment.

Keywords: security, framework, spatial geodata infrastructure, SDI, web service

Inhaltsverzeichnis

Abbildungsverzeichnis…….....x
Tabellenverzeichnis……....xii
Abkürzungsverzeichnis…….xiii

1. Einführung 1
1.1 Ausgangslage 1
1.2 Motivation 4
1.3 Thesen 5
1.4 Lösungsansatz 6
1.5 Zielsetzung und Vorgehen 7
1.6 Abgrenzung 8

2. Literaturüberblick 10
2.1 Grundlegende Begriffe 10
2.1.1 Geodateninfrastruktur 10
2.1.2 Interoperabilität 11
2.1.3 Offener Standard 13
2.1.4 Web Service 14
2.1.5 Geo Web Service 16
2.1.6 Framework 18
2.2 Sicherheit in der IT 19
2.2.1 Begriffe und Definitionen 19
2.2.2 Angriffsarten und Bedrohungen 20

2.2.3 Sicherheitsanforderungen aus dem IT-Bereich ... 23
2.2.4 Die OSI-Sicherheitsarchitektur ... 25
2.2.5 Integrierte Sicherheitsarchitektur ... 31
2.3 Sicherheit bei Web Services ... 33
2.3.1 Verschlüsselung ... 33
2.3.2 Transportsicherheit ... 38
2.3.3 Nachrichtensicherheit ... 42
2.3.4 AAA-Verfahren ... 48
2.3.5 Technologien und Standards von AAA-Verfahren ... 50
2.4 Sicherheit im GDI-Umfeld ... 60
2.4.1 WAS ... 60
2.4.2 WSS ... 60
2.4.3 GeoXACML ... 61
2.4.4 GeoDRM ... 63
2.4.5 WPOS / XCPF ... 64
2.5 Aktuelle GDI-Initiativen ... 65
2.5.1 deegree ... 65
2.5.2 52°North ... 67
3. Lösungsansatz ... 69
3.1 Theorieansatz ... 69
3.1.1 ISO/OSI-Sicherheitsarchitektur ... 69
3.1.2 Integrierte Sicherheitsarchitektur ... 70
3.1.3 Sicherheit im GDI-Umfeld ... 71
3.2 Beurteilung ... 72
4. GDI-Sicherheitsframework ... 74
4.1 Sicherheitsaspekte und Massnahmen ... 74
4.2 GDI Konzept ... 75
4.2.1 Verbindungssicherheit ... 76
4.2.2 Anwendungssicherheit ... 77
4.3 Empfehlung ... 81

4.3.1 Verfahren und Standards ... 82
4.3.2 Aufbau und Interaktion ... 85
5. Ergebnisse und Beurteilung ... 87
5.1 Ergebnisse ... 87
5.2 Beurteilung ... 89
5.2.1 Inhaltliche Beurteilung ... 89
5.2.2 Beurteilung der Methodik ... 91
6. Zusammenfassung und Ausblick ... 92
6.1 Zusammenfassung ... 92
6.2 Ausblick ... 93
7. Literaturverzeichnis ... 95
Anhang 1: LDAP ... 104

Abbildungsverzeichnis

Abb. 1: Service-orientierte Architektur (SOA) (Huber, 2006) 2

Abb. 2: Top-Down-Ansatz unterteilt in konzeptionelle, logische und physische Ebene..... 6

Abb. 3: Aufbau und Struktur der Master Thesis 8

Abb. 4: Eigenschaften und Beziehungen von GDI-Komponenten (Rajabifard et al. 2002)..... 11

Abb. 5: Web Service-Architektur: Einheiten und Aktionen (nach Shah, 2007) 15

Abb. 6: Abhören von Nachrichten 21

Abb. 7: Löschen von Nachrichten..... 21

Abb. 8: Verändern von Nachrichten 21

Abb. 9: Einfügen von Nachrichten 21

Abb. 10: Wiederholen von Nachrichten 21

Abb. 11: Bestreiten des Versands oder Empfangs von Nachrichten..... 22

Abb. 12: Vortäuschen einer Identität 22

Abb. 13: ISO/OSI-Referenzmodell..... 27

Abb. 14: Integrierte Sicherheitsarchitektur (nach Abbie, 2003) 32

Abb. 15: Signierung und Verifikation einer Nachricht (nach Muster, 2006) 35

Abb. 16: Indirekter Zugriff auf einen Web Service (nach Mahmoud, 2005)..... 39

Abb. 17: IPSec-Verbindung im Transport-Mode (nach Muster, 2006) 40

Abb. 18: IPSec-Verbindung im Tunnel-Mode (nach Muster, 2006) 41

Abb. 19: Tunneling in VPNs 41

Abb. 20: WS Security Framework (nach IBM, 2002) 47

Abb. 21: Sign-on-Server (Rummeyer et al., 2006) 51

Abb. 22: Circle-of-Trust (Rummeyer et al., 2006) 51

Abb. 23: SAML Konzept (nach OASIS, 2006a) 53

Abb. 24: Nachrichtensicherheit - Zusammenspiel der Standards (nach Hauser et al., 2004) 54

Abb. 25: SAML-Authentifizierung mittels POST-Profil (nach Hey, 2005) 55

Abb. 26: SAML-Authentifizierung mittels Artefact-Profil (nach Hey, 2005) 56

Abb. 27: Ablauf einer XACML-Zugriffsanfrage (nach OASIS, 2005a) 57

Abb. 28: Zusammenspiel von WAS und WSS (nach Drewnak, 2003) 61

Abb. 29: Zugriffseinschränkungen mit GeoXACML (AM Consult, 2005) 62

Abb. 30: GeoXACML Service Infrastruktur (nach AM Consult, 2005) 62

Abb. 31: Aufbau, Interaktion und Kommunikation von deegree 66

Abb. 32: Aufbau, Interaktion und Kommunikation von 52°North 68

Abb. 33: Einordnung der OSI-Sicherheitsdienste in das OSI-Referenzmodell 69

Abb. 34: GDI-Sicherheitsframework 76

Abb. 35: GDI-Sicherheitsframework: Einordnung der Standards und Spezifikationen 81

Abb. 36: Transportsicherheit in Bezug auf das ISO/OSI-Referenzmodell 82

Abb. 37: Empfehlung für die Architektur einer sicheren GDI 85

Abb. 38: Beispiel eines LDAP Verzeichnisbaums (nach Howes et al. 2005) 105

Abb. 39: Verfahren einer typischen LDAP-Anfrage (nach Howes et al. 2005) 105

Tabellenverzeichnis

Tab. 1: Beispielsyntax WSDL-Nachricht (nach W3Schools, 2007) 14

Tab. 2: Vor- und Nachteile von Web Services (nach Hauser et al., 2004) 16

Tab. 3: Klassifikation der OSI-Sicherheitsdienste (nach ISO, 1989) 29

Tab. 4: Beziehung zwischen Sicherheitsdiensten und -mechanismen (nach ISO, 1989)..... 31

Tab. 5: Hashfunktionen und Hashcodes (nach Muster, 2006) 34

Tab. 6: XML-Signature Beispielcode (Beispiel aus W3C, 2002a und IETF, 2002)..... 43

Tab. 7: XML-Encryption Beispielcode (Beispiel aus W3C, 2002b) 44

Tab. 8: UsernameToken (aus OASIS 2006c)..... 45

Tab. 9: BinarySecurityToken mit X.509 Zertifikat (aus OASIS 2006d) 46

Tab. 10: BinarySecurityToken mit Kerberos Ticket (aus OASIS, 2006f) 46

Tab. 11: SAML Token (aus OASIS, 2006e)..... 46

Tab. 12: Beispiel einer SAML Response mit Assertion 55

Tab. 13: Beispiel einer XACML-Anfrage 57

Tab. 14: Pseudocode einer GeoXACML-Anfrage..... 68

Tab. 15: Sicherheitsaspekte im IT-Bereich und die zugehörigen Verfahren 75

Tab. 16: Pseudo-Beispielabfrage OWS + Authentifizierungsinformation..... 83

Tab. 17: Vor- und Nachteile von LDAP 106

Abkürzungsverzeichnis

AAA	Authentifizierung, Autorisierung, Accounting
AES	Advanced Encryption Standard
CA	Certification Authority
CRL	Certificate Revocation List
DES	Data Encryption Standard
DRM	Digital Rights Management
GeoXACML	Geo eXtensible Access Control Markup Language
GDI	Geodateninfrastruktur
GML	Geography Markup Language
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPSec	IP Security
ISO	International Standardization Organization
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
KOGIS	Koordination, Geo-Information und Services (Schweiz)
LDAP	Lightweight Directory Access Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OSI	Open Systems Interconnection
OWS	OGC Web Service
OWL	Web Ontology Language
PKI	Public Key Infrastructures
PAP	Policy Administration Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PDP	Policy Decision Point
RA	Registration Authority

RDF	Resource Description Framework
RSA	Asymmetrisches Kryptografiesystem nach **R**ivest, **S**hamir und **A**dleman
SAML	Security Assertion Markup Language
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
SSO	Single Sign-On
TLS	Transport Layer Security
TSA	Time Stamping Authority
UDDI	Universal Description, Discovery and Integration
VPN	Virtual Private Network
WAS	Web Authentication Service
WPOS	Web Pricing and Ordering Service
WS-Security	Web Service Security
WSC	Web Security Client
WSS	Web Security Service; Web Service Security Committee (OASIS)
WSDL	Web Service Definition Language
W3C	World Wide Web Consortium
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

1. Einführung

Im ersten Kapitel werden die Ausgangslage (Kap 1.1) und die Motivation (Kap. 1.2) zu dieser Arbeit erläutert. Ausgehend von den aufgestellten Thesen (Kap. 1.3) werden der gewählte Lösungsansatz (Kap. 1.4) erklärt und die Zielsetzung (Kap. 1.5) aufgezeigt. Die Beschreibung der thematischen und inhaltlichen Abgrenzung (Kap. 1.6) schliesst dieses erste Kapitel ab.

1.1 Ausgangslage

Die Verfügbarkeit und Aktualität von Geodaten[1] bilden eine massgebliche Grundlage für die Qualität und Transparenz von Entscheidungen in der Verwaltung, Politik und Wirtschaft. Geodaten gelten dabei als Voraussetzung für politische und wirtschaftliche Entscheide, insbesondere für die Sicherung des Grundeigentums und der Versorgungsinfrastruktur. Diese Anforderungen haben in den letzten Jahren dazu geführt, dass viele private und öffentliche Institutionen und Körperschaften ihre Geodaten in Form von einfachen Web Services oder umfangreichen Geodateninfrastrukturen (GDIs) veröffentlicht haben. Diese Entwicklung wurde mitunter durch die Standardisierung im Bereich der Geo Web Services und die zunehmende Verfügbarkeit von frei erhältlichen GDI-Komponenten begünstigt.

[1] Geodaten sind digitale Daten die einen geografischen Raumbezug aufweisen.

Der Geoinformations-Markt hat mittlerweile eine grosse Vielfalt an interoperablen[2], interaktiven Dienstleistungen hervorgebracht, die sich durch standardisierte Schnittstellen in verteilte IT-Infrastrukturen und somit auch in Geschäftsprozesse integrieren lassen. Man spricht hierbei auch von einer serviceorientierten Architektur oder SOA (engl. service oriented architecture). Innerhalb einer SOA stellen Dienste unabhängige Verarbeitungseinheiten dar, die hinsichtlich ihrer Schnittstellen und Funktionen genau definiert sind. Dies ermöglicht eine bessere Verteilung der einzelnen Verarbeitungseinheiten auf mehrere Applikationen, Server oder Organisationen und unterstützt eine flexible Konfiguration und Modifikation von Geschäftsprozessen. Somit können die Anbieter von Geodiensten schneller auf die Bedürfnisse aus dem internen und externen Umfeld (u.a. Organisation, Kunden, Lieferanten etc.) reagieren und ihr Angebot den Anforderungen anpassen. (Huber, 2006).

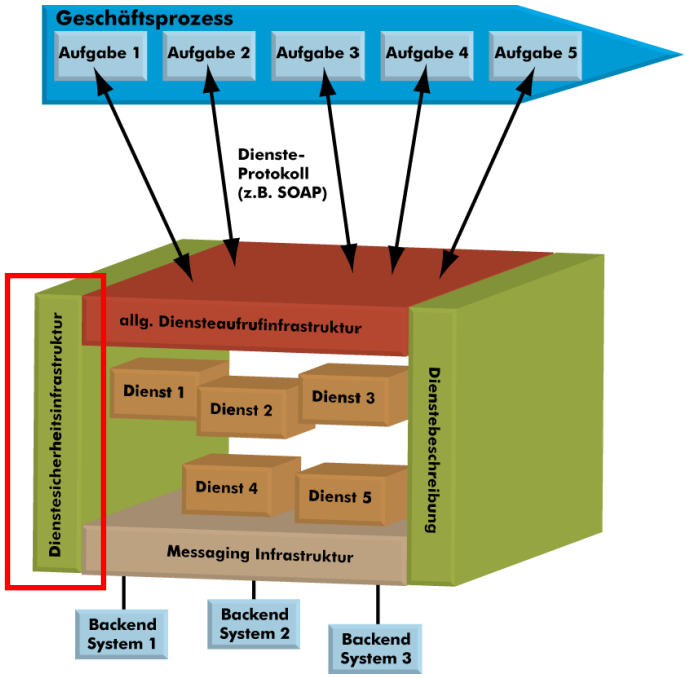

Abb. 1: Service-orientierte Architektur (SOA) (Huber, 2006)

Ein wesentlicher Teil einer solchen SOA bildet die Dienstsicherheitsinfrastruktur (siehe Markierung Abb. 1). Sie sorgt dafür, dass für alle Dienste einer Infrastruktur die folgenden Aspekte gewährleistet werden:

[2] Interoperable Dienstleistungen sind per Definition systemunabhängig und kommunizieren über standardisierte Schnittstellen und Verfahren.

- Korrekte Identifikation der Benutzer (Authentifizierung)
- Einhaltung der Benutzerberechtigungen (Autorisierung, Zugriffssicherheit)
- Sicherung der Verbindungsleitung zwischen Client und Service
- Abwehr von Missbräuchen oder Hacker-Attacken

Sicherheit im Allgemeinen und Informationssicherheit im Speziellen sind Grundanforderungen für die kommerzielle Nutzung von Web Services in verteilten Infrastrukturen. Gleichzeitig sind auch die Sicherheitskonzepte auf dem Gebiet von kommerziellen Web Services soweit gediehen, dass moderne eCommerce-Lösungen (von der E-Banking Plattform bis hin zum E-Payment) eine breite Akzeptanz und Verbreitung erreicht haben.

Geo-räumliche Web Services (Geo Web Services) unterscheiden sich in ihrer Funktionsweise nicht von herkömmlichen Web Services aus dem IT-Bereich. Der Unterschied liegt einzig darin, dass Geo Web Services Inhalte zur Verfügung stellen die einen direkten oder indirekten Raumbezug aufweisen. Dies hat zur Konsequenz, dass auch für die Sicherheit von Geo Web Services die bestehenden Technologien und Standards aus dem allgemeinen IT-Umfeld angewendet werden können. Die geo-räumlichen Zusatzanforderungen sind demzufolge nur dort zu spezifizieren, wo dies die funktionalen Einschränkungen der bestehenden Technologien und Standards erforderlich machen. Dadurch ergeben sich folgende Vorteile:

- Interoperabilität: Die Dienste lassen sich standardisiert untereinander verbinden (Service Chaining), so dass Geschäftsabläufe einfach durch geo-räumliche Dienste erweitert werden können und keine zusätzlichen Schnittstellen für proprietäre Formate entwickelt werden müssen.
- Weiterentwicklung: Die Anpassung der Verfahren und Standards auf die sich stetig verändernden Anforderungen aus dem Sicherheitsumfeld ist sichergestellt.
- Akzeptanz: Der erfolgreiche Einsatz einer Technologie oder eines Standards ist immer auch abhängig von deren Verbreitung und Akzeptanz. Durch minimale geo-räumliche Anpassungen an bereits etablierten Standards lassen sich eine breite Akzeptanz und damit auch eine themenübergreifende Verbreitung bewerkstelligen.

Im IT-Umfeld haben zahlreiche Institutionen wie die W3C[3], IETF[4] oder OASIS[5] Standards und Verfahren für die Sicherheit bei Web Services veröffentlicht. Die Vielfältigkeit und Komplexität dieser Verfahren machen es für den Anbieter nicht einfach die Übersicht über das Gebotene zu behalten, zumal viele der Standards lediglich Teilaspekte der IT-Sicherheit abdecken.

1.2 Motivation

Mit der Veröffentlichung von Geoinformationen im Rahmen von GDIs wird auch die Behandlung von vertraulichen oder kostenpflichtigen Daten zu einem zentralen Thema. Für die Anbieter von Geodateninfrastrukturen ist es wichtig zu wissen, wer auf ihre Dienste zugreift. Dies ist die Voraussetzung um entscheiden zu können, ob der Dienstzugriff gewährt werden soll und ob es sich um einen kostenpflichtigen Zugriff handelt, der entsprechend in Rechnung gestellt werden kann. Die Einführung einer zuverlässigen IT-Sicherheitspolitik ist deshalb unabdingbar, da nur so die Wirtschaftlichkeit und Nachhaltigkeit der Dienste gewahrt bleiben kann.

Auf Grund der gewünschten Offenheit und Interoperabilität ist die Sicherheit im Bereich GDI ein komplexes Problem, das sich auf verschiedenen Ebenen abspielt. In den aktuellen Spezifikationen des OGC[6] und in den Empfehlungen des schweizerischen eGovernment Standards[7] wird der Sicherheitsaspekt noch nicht berücksichtigt. Somit fehlen wichtige Spezifikationen über Verfahren oder Mechanismen durch die der Zugriff auf Daten und Dienste kontrolliert und geschützt werden kann.

Gleichzeitig wachsen die Anforderungen an die Entscheidungsträger im GIS-Bereich, sich vermehrt auch ein detailliertes Wissen über Lösungsarchitekturen und Sicherheitsmethoden in verteilten GDIs anzueignen. Um diesen Anforderungen auch bei beschränkten finanziellen und

[3] World Wide Web Consortium: http://www.w3.org (30.06.2007)

[4] Internet Engineering Task Force: http://www.ietf.org (30.06.2007)

[5] Organization for the Advancement of Structured Information Standards: http://www.oasis-open.org (30.06.2007)

[6] Open Geospatial Consortium: http://www.opengeospatial.org (30.06.2007)

[7] Anwendungsprofil Geodienste (Stark et al. 2006)

personellen Ressourcen gerecht zu werden, bedarf es eines unterstützenden Konzepts, wie die Sicherheit innerhalb einer GDI umfassend gewährleistet werden kann.

Die Motivation dieser Arbeit besteht darin, mit der Konzeption eines Sicherheitsframeworks die zentralen Sicherheitsaspekte einer GDI zu identifizieren und Massnahmen vorzuschlagen, wie diese in verteilten IT-Systemen durchgesetzt werden können. Bei der Konzeption gilt es folgende Rahmenbedingungen zu beachten:

- Die bestehenden Sicherheitsstandards aus dem allgemeinen IT-Umfeld sollen soweit als möglich auch für die Dienste einer GDI genutzt werden können. Die spezifischen Erweiterungen für den GIS-Bereich (räumliche Zugriffseinschränkung) sollten minimal gehalten werden.
- Die getroffenen Sicherheitsmassnahmen dürfen die Interoperabilität nicht einschränken und müssen die Nutzung der bestehenden OGC-Standards ohne Modifikationen gewährleisten können.
- Die Sicherheitsmassnahmen müssen sowohl für zentralisierte als auch für dezentrale GDI-Architekturen anwendbar sein.
- Die Sicherheitsmassnahmen dürfen den Benutzungskomfort der GDI-Komponenten nicht eingrenzen und müssen die Sicherheit von Dienstanbieter UND Dienstnutzer gewährleisten.

1.3 Thesen

Aus den oben genannten Rahmenbedingungen lassen sich für die Konzeption der Arbeit folgende Thesen aufstellen:

1. Zur ganzheitlichen Betrachtung der relevanten Sicherheitsaspekte ist ein übergeordnetes GDI-Sicherheitskonzepts erforderlich.
2. Die zur Verfügung stehenden Standards und Spezifikationen aus dem allgemeinen IT-Sicherheitsumfeld decken die Grundbedürfnisse für die Absicherung einer GDI weitestgehend ab. Die geo-spezifischen Zusatzanforderungen werden nur wo zwingend erforderlich durch ergänzende Spezifikationen vervollständigt.

3. Im GDI-Umfeld sind feingranulare, rollenbasierte Kontrollmechanismen erforderlich damit eine thematische, zeitliche und räumliche Zugriffsbeschränkung garantiert werden kann.
4. Auch bei frei verfügbaren Geodatenbeständen die im Rahmen von GDIs veröffentlicht werden, sind Sicherheitsmassnahmen sinnvoll und generieren einen Mehrnutzen.

1.4 Lösungsansatz

Der Lösungsansatz basiert auf einem Top-Down-Vorgehen (Abb. 2). Dabei wird versucht die bestehenden und bereits etablierten Sicherheitsstandards aus dem IT-Umfeld so weit als möglich auch für das Geo-Umfeld übernehmen zu können. Die Aspekte des räumlichen Bezugs verstehen sich somit als Spezialisierung der IT-Gesamtkonzepte.

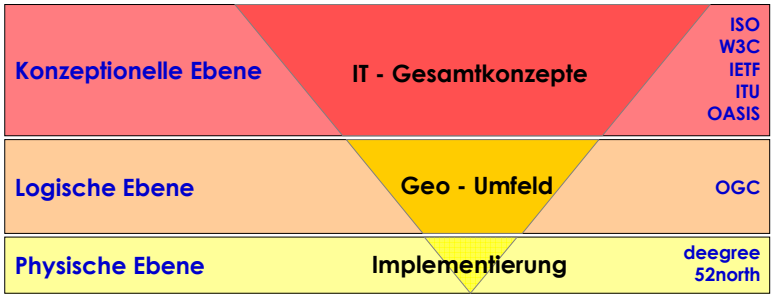

Abb. 2: Top-Down-Ansatz unterteilt in konzeptionelle, logische und physische Ebene

Ausgehend von den allgemeinen Sicherheitsanforderungen aus dem IT-Umfeld (konzeptionelle Ebene) werden die für die Sicherheit von Web Services und verteilten Geodateninfrastrukturen relevanten Gesamtkonzepte herausgearbeitet. Im Fokus stehen dabei die massgebenden IT-Spezifikationen der internationalen Standardisierungsinstitutionen wie ISO[8], IETF, ITU[9], W3C oder OASIS. Die Ansätze der konzeptionellen Ebene werden auf der logischen Ebene mit den Anforderungen aus dem Geo-Umfeld verglichen und die räumlichen Zusatzanforderungen identifiziert. In diesem Schritt gilt es vor allem die Standardisierungsbestrebungen des OGC zu betrachten. In einem dritten Schritt wird auf der physischen Ebene analysiert, wie sich die

[8] International Standardization Organization: http://www.iso.org (30.06.2007)

[9] International Telecommunication Union: http://www.itu.int (30.06.2007)

verschiedenen Sicherheitsstandards implementieren und zu einem Framework zusammenfügen lassen. Dabei stehen insbesondere die bestehenden Implementierungen von deegree[10] und 52°North[11] im Fokus des Interesses.

1.5 Zielsetzung und Vorgehen

Ziel der Arbeit ist es, ein Framework zu konzipieren, das - basierend auf den grundlegenden Sicherheitsaspekten aus dem IT-Umfeld - eine ganzheitliche und übergeordnete Sicht auf die für die Gewährleistung der Sicherheit erforderlichen Komponenten einer GDI vermittelt. Dazu sollen die derzeit bestehenden Sicherheitslösungen aus dem allgemeinen IT-Umfeld dokumentiert und mit dem Stand der Standardisierungsbemühungen aus dem GDI-Bereich verglichen werden. Ein wesentlicher Teil der Aufgabe ist es dabei, die relevanten Verfahren, Spezifikationen und Standards in diesen Bereichen herauszufiltern, zu analysieren und in einen Gesamtkontext einzuordnen.

Mit dem resultierenden GDI-Sicherheitsframework soll ein grundsätzliches Konzept geschaffen werden, das es Entscheidungsträgern ermöglicht, die wesentlichen „Bestandteile“ einer sicheren GDI zu kennen und entsprechende Massnahmen einordnen und beurteilen zu können. Ziel des Frameworks ist es, auf einer konzeptionellen Ebene eine strukturierte Sichtweise auf die Abhängigkeiten und Interaktionen zwischen den wesentlichen Sicherheitskomponenten einer GDI darzustellen. Die Art und Weise der Implementierung soll dabei grundsätzlich offen gelassen werden. Im Rahmen einer Empfehlung wird dennoch versucht eine mögliche Open Source[12]-basierte Lösungsarchitektur aufzuzeigen.

Die nachfolgende Grafik (Abb. 3) zeigt einerseits das gewählte Top-Down-Vorgehen und verdeutlicht die verwendete Methodik. Andererseits wird mit dieser Grafik auch die Struktur der weiteren Kapitel dieser Master Thesis illustriert. Der Aufbau der Unterkapitel wird jeweils Anfangs des Kapitels erläutert.

[10] Degree Initiative - Free Software for Spatial Data Infrastructures (degree, 2007)

[11] 52°North - Geospatial Open Source Software GmbH (52°north, 2007)

[12] Eine nach den Richtlinien der Open Source-Initiative erstellte Software, deren Quellcode zugänglich ist und beliebig kopiert, verändert oder weiter genutzt werden darf. http://www.opensource.org (30.06.2007).

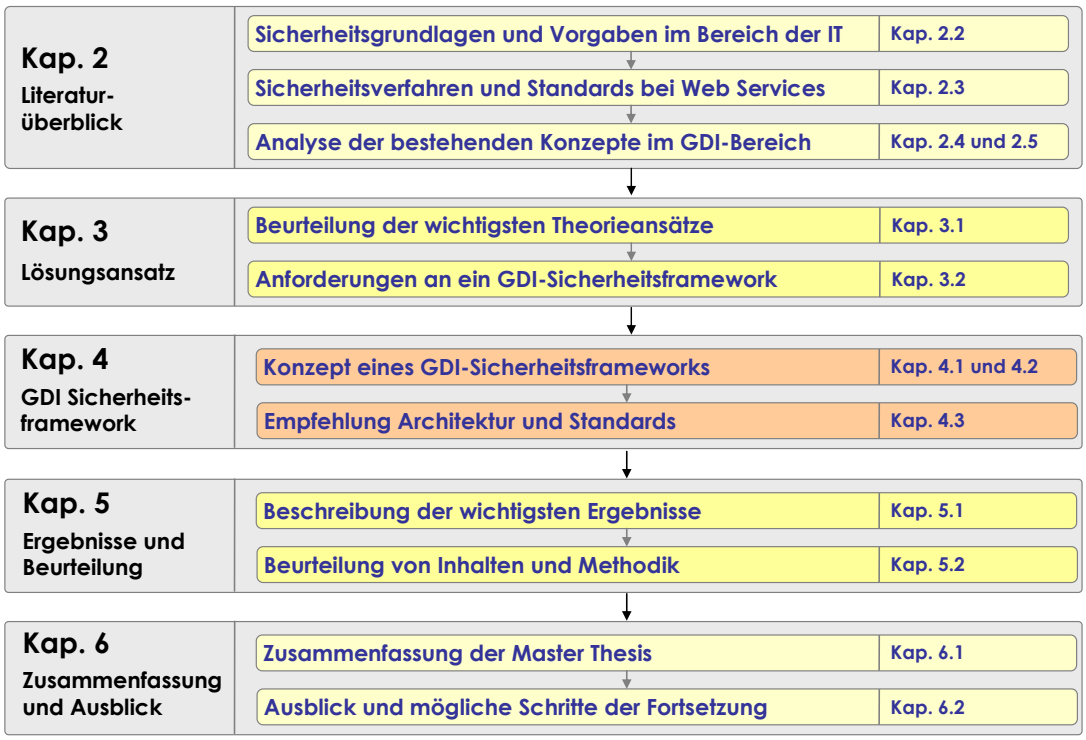

Abb. 3: Aufbau und Struktur der Master Thesis

1.6 Abgrenzung

Im Open Source-Bereich haben in den letzten Jahren einige Initiativen (u.a. deegree, 52°North) Lösungen für die fehlenden Sicherheitsmechanismen entwickelt und diese im Rahmen von GDI-Projekten im produktiven Einsatz erprobt. Einzelne Teilkomponenten wurden bereits als OGC Discussion Papers veröffentlicht, haben es aber bis dato noch nicht bis zum Spezifikationsstatus geschafft. Die Betrachtung dieser Initiativen wird im Rahmen dieser Arbeit nur auf einer konzeptionellen Ebene erfolgen.

Das OGC hat im Juni 2006 eine Arbeitsgruppe Sicherheit[13] ins Leben gerufen, deren Ziel es ist, ein interoperables Sicherheitsframework für OpenGIS Web Services zu etablieren. Diese Bemühungen seitens des OGC zeigen den Bedarf nach Sicherheit für Geo Web Services und die Relevanz des Themas. Bis zum Abschluss dieser Arbeit wurden von der Security WG des OGC

[13] OGC Security Working Group (OGC, 2007b)

keine Spezifikationen oder Discussion Papers verabschiedet, die für die Konzeption eines Sicherheitsframeworks hätten beigezogen werden können.

Folgende Themenbereiche liegen nicht im Fokus dieser Arbeit und werden im Rahmen des Berichts nicht behandelt:

- Wissenschaftliche Auseinandersetzung mit erweiterten Rahmenbedingungen im Umfeld einer GDI und im Speziellen mit den politischen, rechtlichen, organisatorischen und wirtschaftlichen Umwelten.
- Methodische Evaluation und Bewertung von frei verfügbaren Software-Komponenten für die Umsetzung der betrachteten Sicherheitsspezifikationen.
- Methodische Evaluation aller derzeit verfügbaren GDI-Sicherheitslösungen. Im Rahmen der Arbeit werden ausschliesslich deegree und 52°North betrachtet.
- Realisierung und Implementierung von einzelnen Sicherheitskomponenten oder prototypische Umsetzung der vorgestellten Konzepte.
- Detaillierte Betrachtung der Verfahren zur Bestellung und Bezahlung von Web Services (Pricing und Ordering Services).

Diese Master Thesis wurde im Rahmen einer Studienarbeit der Firma Condesys Consulting GmbH erstellt und von Dr. Martin Huber fachlich begleitet. Das Thema steht in thematischer Nähe zu der Abschlussarbeit von Pascal Imoberdorf (U1217), die sich eingehend mit der Konzeption eines Metamodells zur Konfiguration und Steuerung von Komponenten einer GDI auseinandersetzt. Diese Aspekte einer GDI stehen nicht im Fokus dieser Arbeit und werden inhaltlich nicht tangiert. Die einleitenden Kapitel wurden in einer Anfangsphase teilweise gemeinsam erarbeitet und können daher ähnliche Formulierungen enthalten.

2. Literaturüberblick

Zu Beginn dieses Kapitels werden die wichtigsten Begriffe im Umfeld von Geodateninfrastrukturen eingeführt (Kap. 2.1). Die drei folgenden Abschnitte befassen sich mit den wichtigsten Literaturgrundlagen zu den grundlegenden Themenbereichen der IT-Sicherheit (Kap. 2.2), der Sicherheit im Rahmen von Web Services (Kap. 2.3) und den spezifischen Aspekten der Sicherheit im GDI-Umfeld (Kap. 2.4). Dabei werden die wichtigsten Standards und Verfahren vorgestellt und die bestehenden Spezifikationen und Sicherheitskonzepte einer Geodateninfrastruktur an Hand der aktuellen GDI-Initiativen (Kap. 2.5) aufgezeigt.

2.1 Grundlegende Begriffe

2.1.1 Geodateninfrastruktur

Wie im ersten Kapitel dieses Berichts bereits erwähnt, bilden Geodateninfrastrukturen (GDIs) eigentliche Plattformen für heterogene, verteilte Geodaten und Dienste. Im deutschen Sprachgebrauch wird der Begriff Geodateninfrastruktur synonym zum englischen Begriff Spatial Data Infrastructure (SDI) gebraucht und als solcher auch im Rahmen dieser Arbeit verwendet.

In der Literatur gibt es verschiedene Ansätze eine Geodateninfrastruktur zu definieren, wobei sich die Unterschiede vor allem auf die Betrachtungsweise beziehen. Eine allgemeine Definition liefert das Schweizerische Koordinationsorgan für Geoinformation und geografische Informationssysteme des Bundes (KOGIS), das eine GDI als „[…] ein allgemein verfügbares System von Verfahren, institutionellen Einrichtungen, Technologien, Daten und Personen, die

den gemeinsamen Austausch und die effiziente Nutzung geografischer Daten ermöglichen“ beschreibt (KOGIS, 2006).

In einer prozessorientierten Sichtweise besteht die GDI aus Regeln, Netzwerk, Standards, Nutzern und Daten (vgl. Abb. 4). Die Interaktion zwischen Nutzern und Daten ist die fundamentale Basis die durch die technologischen Komponenten (Regeln, Netzwerk und Standards) verbunden werden (Rajabifard et al. 2002).

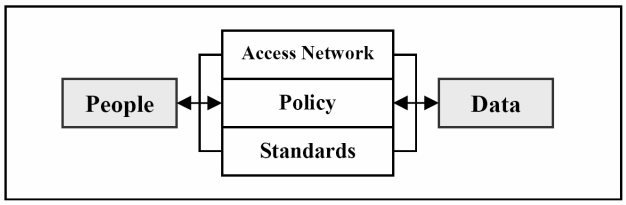

Abb. 4: Eigenschaften und Beziehungen von GDI-Komponenten (Rajabifard et al. 2002)

Aus betriebsorientierter Sicht sind bei der Definition einer GDI noch weitere Aspekte von Bedeutung. Die Definition von Groot und McLaughlin (Groot et al., 2000) nennt zusätzlich zu den bereits erwähnten Komponenten der Verwaltung und Vernetzung von Geodaten auch die Bereiche der institutionellen, organisatorischen, technologischen und wirtschaftlichen Ressourcen. Dabei gehören auch die Entwicklung und Pflege der GDI, sowie der **verantwortungsvolle Umgang** mit den darin zur Verfügung stehenden Geoinformationen zu den wesentlichen Bereichen (Bernhard et al. 2002).

Zusammenfassend lässt sich festhalten, dass für eine Geodateninfrastruktur neben Geodaten, Diensten und Nutzern auch das Netzwerk und die Aspekte der Interoperabilität (Regeln und Standards) wichtig sind. Für die Entwicklung und den Betrieb einer GDI ist zudem der verantwortungsvolle Umgang mit Geodaten von Bedeutung.

2.1.2 Interoperabilität

Der Begriff Interoperabilität bezeichnet die Möglichkeit einer systemunabhängigen Kommunikation zwischen verschiedenen Informationssystemen über standardisierte Schnittstellen und Verfahren (SOGI, 2003). In der Betrachtungsweise des OGC wird Interoperabilität als die Möglichkeit des Austausches von Daten und Anweisungen lokal verwalteter, unterschiedlicher Systeme zur Unterstützung von Services (Computing- und Web Services) verstanden (OGC, 2007a). Die Herausforderung besteht darin, die von den Nutzern gewünschte Austauschbarkeit der Daten und Dienste (engl. compatibility) mit der

Eigenständigkeit (engl. autonomy) und Heterogenität (engl. heterogenity) der interagierenden Systeme in Einklang zu bringen (OGC, 2007a).

Im Umfeld einer GDI lassen sich unterschiedliche Arten von Interoperabilität definieren (Matheus, 2005):

- Die **Interoperabilität von Geodaten** respektive Geodatenmodellen erlaubt eine eigentliche Kombination von unterschiedlichen Formaten und Standards. Dies umfasst neben den Standardformaten aus den verschiedenen IT-Bereichen auch die auf die Anforderungen des Raumbezugs angepassten Formate. Dieser Aspekt der Interoperabilität wird im GIS-Bereich mit der Schaffung von OGC-Standards (z.B. GML[14]) erfüllt.
- Die **Interoperabilität der Services** erlaubt eine standardisierte Abfrage der zur Verfügung stehenden Funktionen und Methoden, sowie der unterstützten Ein- und Ausgabeformate eines Web Services. Neben den Standards aus der IT (z.B. LDAP[15]), sind im Rahmen einer GDI auch hier vor allem die Standards des OGC (z.B. WMS) von Bedeutung (vgl. Kap. 2.1.5).
- Die **Interoperabilität der Semantik** hilft einer Anwendung selber festzustellen, welcher Service zur Erreichung des gesetzten Ziels genutzt werden kann. Insbesondere bei einer Automatisierung der Dienstnutzung ist es notwendig eine Semantikbeschreibungen in maschinenverarbeitbarer Form bereitzustellen und gemeinsam mit dem Dienst anzubieten (Dostal et al., 2004). Zu erwähnen sind in diesem Zusammenhang die Konzepte des Semantic Web und dessen erste Ausprägungen wie RDF[16] oder OWL[17].
- Die **Sicherheitsinteroperabilität** ermöglicht einen sicheren Zugriff auf geschützte und verteilte Daten einer GDI. Dieser Zugriff respektive die entsprechenden Zugriffsrechte müssen auch über verteilte Systeme hinweg durchgesetzt werden können. Es gilt dabei zu beachten, dass durch die Anforderungen der Sicherheit die standardisierten Zugriffsverfahren (z.B. WMS-Aufruf) nicht verändert oder eingeschränkt werden dürfen. Zudem müssen die Sicherheitsmassnahmen über unterschiedliche Netzinfrastrukturen

[14] Geography Markup Language: http://www.opengeospatial.org/standards/gml (30.06.2007)

[15] Lightweight Directory Access Protocol: http://www.ietf.org/rfc/rfc4511.txt (30.06.2007) und Anhang 1: LDAP

[16] Resource Description Framework: http://www.w3.org/TR/1999/REC-rdf-syntax-19990222 (30.06.2007)

[17] Web Ontology Language: http://www.w3.org/TR/2004/REC-owl-features-20040210 (30.06.2007)

(Intranet, Internet, VPN etc.) sichergestellt werden können. In diesem Bereich gibt es vom OGC derzeit noch keine standardisierten Verfahren für die GIS-spezifischen Zusatzanforderungen (z.B. räumliche Zugriffskontrolle).

Grundsätzlich geht es beim Begriff Interoperabilität um die semantisch, konzeptuell und physisch eindeutige Definition von Schnittstellen, so dass diese im Rahmen einer verteilten Systemarchitektur genutzt werden können. Was dabei hinter der Schnittstelle abläuft, liegt im Ermessen des Anbieters oder Systemintegrators (Huber, 2006). Für die weiteren Betrachtungen dieser Arbeit steht die Interoperabilität der Sicherheit im Fokus des Interesses.

2.1.3 Offener Standard

Unter dem Begriff „Offener Standard“ wird eine frei verfügbare Spezifikation[18] verstanden, die eine allgemeine Methode zur Erledigung einer bestimmten Aufgabe zur Verfügung stellt (Wikipedia, 2007). Das Ziel von offenen Standards ist es, die Verfügbarkeit und Unabhängigkeit von Spezifikationen zu gewährleisten, ohne dass diese durch Nutzungsgebühren oder Urheberrechte eingeschränkt werden können. Ein wesentlicher Vorteil von offenen Standards liegt darin dass,

> „…Software-Unternehmen damit aufhören können, um jeden Preis *ihre* Anschlussvorrichtung für den Feuerwehrhydranten durchzusetzen, und sich statt dessen darauf konzentrieren, bessere Löschschläuche, Pumpen und Feuerwehrautos als ihre Konkurrenten zu bauen.“
>
> *(Friedmann, 2006)*

Als Beispiele von offenen Standards sind unter anderem XML[19] oder SOAP[20] zu nennen. Offene Standards sind eine Grundvoraussetzung für die Interoperabilität von Web Services und daher eine zentrale Anforderung für die Umsetzung von Geodateninfrastrukturen.

[18] Eine Spezifikation bezeichnet eine veröffentlichte Technologiebeschreibung und wird nur dann als Standard bezeichnet, wenn sie sich in einem spezifischen Technologiebereich durchgesetzt hat und von einer Standardisierungsinstanz administriert wird (Hauser et al., 2004).

[19] eXtensible Markup Language: http://www.xml.org (30.06.2007)

[20] Simple Object Access Protocol - Standard Version 1.2: http://www.w3.org/TR/soap (30.06.2007)

2.1.4 Web Service

Web Services sind Funktionen oder Methoden die über einen Webserver publiziert werden und aus dem verteilten Intranet oder Internet mit Hilfe von XML-basierten Standards wie WSDL[21], UDDI[22] und SOAP aufgerufen werden können (Shah, 2007). Vereinfacht lassen sich bei der Web Service-Technologie die drei Einheiten Konsument (engl. web service consumer), Anbieter (engl. web service supplier) und Registrierungsinstitution (engl. universal business registry, UBR) definieren. Die gesamte Kommunikation zwischen diesen Akteuren wird über die Standards UDDI, WSDL und SOAP übermittelt. Zum Verständnis des allgemeinen Ablaufs einer Serviceanfrage werden an dieser Stelle kurz die oben erwähnten Standards erläutert.

- **SOAP** ist ein Kommunikationsprotokoll des W3C, das auf HTTP/HTTPS aufsetzt und den Zugriff auf Services, Objekte und Server ermöglicht.
- **UDDI** ist ein auf SOAP basierendes Verzeichnis von Serviceangeboten.
- **WSDL** ist ein XML-basiertes Format zur Beschreibung von Eigenschaften (engl. capabilities) von Web Services. Ein WSDL Dokument enthält folgende Informationen:

  `<types>` Die Datentypen die der Web Service verarbeiten kann (Zeile 4-7).

  `<message>` Die Nachrichten die der Web Service verwendet (Zeile 8-11).

  `<portType>` Die Operationen die vom Web Service angeboten werden (Zeile 12-15).

  `<binding>` Die Protokolle die der Web Service unterstützt (Zeile 16-20).

```
 1  <wsdl:definitions name="nmtoken"? targetNamespace="uri">
 2      <import namespace="uri" location="uri"/> *
 3      <wsdl:documentation .... /> ?
 4      <wsdl:types> ?
 5          <wsdl:documentation .... /> ?
 6          <xsd:schema .... /> *
 7      </wsdl:types>
 8      <wsdl:message name="ncname"> *
 9          <wsdl:documentation .... /> ?
10          <part name="ncname" element="qname"? type="qname"?/> *
11      </wsdl:message>
12      <wsdl:portType name="ncname"> *
13          <wsdl:documentation .... /> ?
14          <wsdl:operation name="ncname"> .... </wsdl:operation>
15      </wsdl:portType>
16      <wsdl:binding name="ncname" type="qname"> *
17          <wsdl:documentation .... /> ?
18          <-- binding details --> *
19          <wsdl:operation name="ncname"> .... </wsdl:operation>
20      </wsdl:binding>
21  </wsdl:definitions>
```

Tab. 1: Beispielsyntax WSDL-Nachricht (nach W3Schools, 2007)

[21] Web Services Description Language: http://www.w3.org/TR/wsdl (30.06.2007)

[22] Universal Description, Discovery and Integration: http://www.uddi.org (30.06.2007)

Der Ablauf einer solchen Serviceinteraktion (Abb. 5) gestaltet sich wie folgt:

1. Der Web Service Konsument sucht bei der Registrierungsinstitution (UBR) Services, die seinen Anforderungen entsprechen.
2. Die UBR liefert dem Konsumenten eine Liste mit möglichen Services, wovon der Konsument einen oder mehrere auswählen kann. Diese Auswahl erhält der Konsument in Form eines WSDL Dokuments mit der genauen Beschreibung der Aufrufssyntax.
3. Der Web Service Konsument verlangt bei der UBR die Zugangsinformationen (IP-Adresse) zu den ausgewählten Services, die er von der Registrierungsinstitution entsprechend zugestellt erhält.
4. Der Web Service Konsument verbindet sich über die erhaltenen Zugangsinformationen mit dem Host des Web Service-Anbieters und greift auf diesen zu. Dabei verwendet er die in der Servicebeschreibung (WSDL) spezifizierte Syntax. Mit dieser Beschreibung kann ein generischer Client[23] des Serviceanbieters dem Benutzer die in der Servicebeschreibung (UDDI) vorgefundenen Aufrufe vorlegen. Der Web Service Konsument wählt einen Aufruf, liefert die in der Servicebeschreibung geforderten Parameter und sendet den Aufruf an den Serviceanbieter.

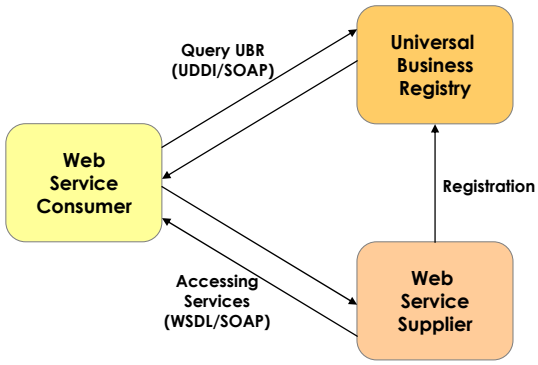

Abb. 5: Web Service-Architektur: Einheiten und Aktionen (nach Shah, 2007)

Im Unterschied zum bisherigen Web-Ansatz wo der Benutzer direkt die Daten und Funktionen eines Webservers bezieht, ermöglichen Web Services auch einen Informationsaustausch zwischen Maschinen. Die weiteren Vor- und Nachteile von Web Services sind in der nachfolgenden Tabelle zusammengefasst (Hauser et al., 2004):

[23] Ein generischer Client verwendet strukturell einheitliche und allgemeingültige Schnittestellen.

Vorteile	Nachteile
▪ Web Services sind im Gegensatz zu den alternativen Verfahren (CORBA[24] und DCOM[25]) sehr einfach zu handhaben. ▪ Web Services basieren in ihrer Grundfunktionalität auf anerkannten IT-Standards (SOAP, WSDL, UDDI). ▪ Web Services haben eine breite Akzeptanz in der Software-Industrie. Viele grosse Software-Hersteller (u.a. Microsoft, Sun, IBM) setzen auf Web Services. ▪ In fast allen Programmierumgebungen stehen Implementierungen für die Unterstützung der Protokolle und Standards von Web Services zur Verfügung. ▪ Die Standards zur Verwendung von Web Services basieren auf XML und haben die Vorteile, dass sie von Menschen lesbar sind und für die Realisierung vielfältige und offene Standards zur Verfügung stehen.	▪ Für einige Bereiche wie Sicherheit, Prozesse und Transaktion gibt es zwar viele Spezifikationen aber derzeit noch keine Standards. ▪ Web Services erfordern für einige Bereiche neue Technologien. Zum Beispiel im Sicherheitsbereich: Da Web Services über das HTTP respektive HTTPS-Protokoll kommunizieren, passieren sie Firewalls problemlos. Zur Absicherung müssen also auch Sicherheitsmechanismen angeboten werden, die Web Service Aufrufe untersuchen und gegebenenfalls sperren können (SOAP-Firewall). ▪ Web Services sind oft nicht die leistungsfähigste Lösung, da die Informationen in Textform (XML) verschickt werden. Dies bringt gegenüber einer Datenübermittlung in binärer Form Geschwindigkeitseinbussen mit sich.

Tab. 2: Vor- und Nachteile von Web Services (nach Hauser et al., 2004)

2.1.5 Geo Web Service

Geo Web Services unterscheiden sich nur in einem wesentlichen Punkt von herkömmlichen Web Services - dem geografischen Raumbezug. Dem Gesetzesentwurf für das schweizerische Geoinformationsgesetz des Bundes (GeoIG[26]) ist zu entnehmen, dass es sich bei Geo Web Services um vernetzbare Anwendungen handelt, „[…] welche die Nutzung von elektronischen Dienstleistungen im Bereich der Geodaten vereinfachen und Geodaten in strukturierter Form zugänglich machen“. Dem Endanwender soll dadurch die Nutzung von Geoinformation

[24] Common Object Request Broker Architecture: http://www.corba.org (30.06.2007)

[25] Distributed Component Object Model: http://www.microsoft.com/com/ (30.06.2007)

[26] Entwurf für das Bundesgesetz über Geoinformation (GeoIG); Art.3 (Stand April 2007)

erleichtert werden. Gleichzeitig soll aber auch die Interaktion von Geo Web Services untereinander (Service Chaining) verbessert werden.

Das OGC ist massgeblich an der Strukturierung der Geodaten und Geo Web Services beteiligt und bietet mit zahlreichen Standards die Grundlage für eine interoperable Nutzung von Geodaten im Internet. Basierend auf GML, einer XML-basierten Sprache für die Codierung von Geodaten, hat das OGC zahlreiche weitere Standards hervorgebracht. Die für eine GDI wichtigsten Standards (nach Nebert et al., 2006) sind nachfolgend aufgeführt:

- Ein **Web Map Service** (WMS) unterstützt den Aufruf und die Auslieferung von Karten eines Map Services. Die geforderten Kartenausschnitte werden in Form von Bildern (z.B. TIFF, JPEG) von einem oder mehreren WMS geliefert und in der gewünschten Endanwendung überlagert und kombiniert (OGC, 2006a).
- Ein **Web Feature Service** (WFS) ermöglicht einem Client einen GML-basierten Zugriff (Abfrage- und Manipulationsoperatoren) auf räumlichen Vektordaten. Die gewünschten Daten werden von einem oder mehreren Services im GML-Format bereitgestellt und in der gewünschten Endanwendung kombiniert (OGC, 2005a).
- **Filter Encoding** (FE) definiert eine XML-basierte Abfragesprache für Filterausdrücke (Queries). Damit lassen sich Teilbereiche von Objektgruppen von unterschiedlichen Services (CSW, WFS, WFS-G, WFS-GC) selektieren. Beispielsweise kann Filter Encoding in Kombination mit WFS über den GetFeature-Befehl logische, mathematische, geometrische und arithmetische Abfrageregeln (query constraints) definieren (OGC, 2005b).
- Ein **Web Coverage Service** (WCS) unterstützt die themenspezifische Extraktion flächenhafter Bereiche (engl. Coverages) von Raster- und Vektordaten. Die resultierenden Coverages können für die Weiterverarbeitung mit WMS oder WFS verwendet werden (OGC, 2006b).
- Ein **Catalogue Service** (CSW) ermöglicht die Suche, Ermittlung und Abfrage von Metadaten über Geodaten, Geodienste und Geoanwendungen in verteilten heterogenen Katalogservern (OGC, 2005c).
- Ein **Web Processing Service** (WPS) stellt GIS-Berechnungsfunktionen für raumbezogene Daten (Raster- und Vektordaten) über ein Netzwerk zur Verfügung. Die Spezifikation beschreibt die dazu erforderlichen Prozesse der Identifikation und Initiierung der Berechnung, sowie das Management der resultierenden Daten. WPS hat derzeit den Status eines OGC Discussion Papers (OGC, 2005d).

2.1.6 Framework

Ein Framework ist eine logische Grundstruktur zur Einordnung und Organisation von komplexen Informationen. Es bildet eine Art „Setzkasten“, bei dem alle relevanten Aspekte eines a priori komplexen Themas strukturiert eingeordnet werden können (Wikipedia, 2007). Das angestrebte Sicherheitsframework soll die Architektur von sicheren Anwendungen aufzeigen und die Bausteine für die Entwicklung einer sicheren GDI identifizieren.

2.2 Sicherheit in der IT

2.2.1 Begriffe und Definitionen

2.2.1.1. IT-System

Ein informationstechnisches System - kurz IT-System - ist ein geschlossenes oder offenes, dynamisches System, das die Fähigkeit besitzt Informationen zu speichern und zu verarbeiten (Eckert, 2006).

2.2.1.2. Sicherheit

Sicherheit ist ein oft verwendeter Begriff in unserem Alltag, der in den verschiedensten Bereichen zur Anwendung kommt und per Definition einen Zustand frei von Gefahr beschreibt. Dieser Definition steht die Aussage von Anton Pawlowitsch Tschechow gegenüber:

> „Es gibt keine Sicherheit, nur verschiedene Grade der Unsicherheit."
>
> *Anton Pawlowitsch Tschechow (1860 - 1904)*

Da es eine vollkommene Sicherheit nicht zu geben scheint, lässt sich Sicherheit realistischerweise wohl eher als ein relativer Zustand der Gefahrenfreiheit, bezogen auf eine bestimmte Situation, einen bestimmten Zeitraum und bestimmte Rahmenbedingungen definieren (Schmidt 2006).

2.2.1.3. IT-Sicherheit

Im IT-Umfeld wird Sicherheit oft allgemein als ein Zustand der voraussichtlich störungs- und gefahrenfreien Funktion eines Systems beschrieben (Wikipedia, 2007). Eine ähnliche Definition für den Begriff „security" liefert auch das Internet Security Glossary (Shirey, 2000), das den Sicherheitsbegriff durch folgende Eigenschaften charakterisiert:

1. Massnahmen zum Schutz eines Systems.
2. Zustand eines Systems, der aus der Einrichtung und Aufrechterhaltung von Schutzmassnahmen resultiert.

3. Zustand von Systemressourcen die frei sind von unautorisiertem Zugriff und keine unautorisierte oder unbeabsichtigte Veränderung, Zerstörung und keinen Verlust zulassen.

Im Wissen, dass es eine absolute Sicherheit nicht geben kann, muss es das Ziel sein, durch geeignete Schutzmassnahmen eine passgenaue Sicherheit für das jeweilige System zu gewährleisten (Schmidt 2006). Die Sicherstellung dieser Massnahmen ist ein stetiger Prozess, bei dem es neben den technischen auch die wirtschaftlichen Aspekte zu berücksichtigen gilt, um den dynamischen Änderungen des Systems und dessen Umgebung Rechnung zu tragen.

Um den Begriff Sicherheit und dessen Teilbereiche im Umfeld der IT etwas besser verstehen zu können, werden nachfolgend die wichtigen Sicherheitsbegriffe erläutert (Eckert, 2006).

- **Informationssicherheit** (engl. security) ist die Eigenschaft eines Systems, keine unautorisierte Veränderung oder Gewinnung von Systeminformationen zuzulassen.
- **Datenschutz** (engl. privacy) ist die Eigenschaft eines Systems, die Haltung und Weitergabe persönlicher Daten[27] zu kontrollieren.
- **Datensicherheit** (engl. protection) ist die Eigenschaft eines Systems, Zustände zu verhindern, die zu unautorisiertem Zugriff auf Systemressourcen oder Daten führen.
- **Funktionssicherheit** (engl. safety) ist der Zustand eines Systems, indem die realisierte Ist-Funktionalität mit der spezifizierten Soll-Funktionalität übereinstimmt und das System somit keinen unzulässigen Zustand annehmen kann.

Für die weiteren Betrachtungen im Rahmen dieser Master Thesis sind insbesondere die Informationssicherheit, der Datenschutz und die Datensicherheit von zentraler Bedeutung.

2.2.2 Angriffsarten und Bedrohungen

2.2.2.1. Angriffsklassen

Eine wesentliche Voraussetzung bei der Definition von Sicherheit ist das Wissen über die existierenden Angriffs- oder Bedrohungsarten einer IT-Infrastruktur. Die Kenntnis der möglichen Gefahren ist eine essentielle Voraussetzung für die Deklaration und Beurteilung einer massgeschneiderten Sicherheitskonzeption. Die Angriffsarten lassen sich dabei in folgende Angriffsmuster, respektive -klassen unterteilen (nach Muster, 2006):

[27] Persönliche Daten sind gemäss Bundesgesetz über den Datenschutz (DSG): „[…]alle Angaben die sich auf eine bestimmte oder bestimmbare Person beziehen[…]“ Art.3, (Stand 20. Juni 2006)

Abhören (engl. eavesdropping): Die Nachricht wird auf dem Weg zwischen den beiden Kommunikationspartnern (blau) von einer unberechtigten Drittperson (rot) abgehört oder eingesehen (Man-in-the-middle-Angriff).

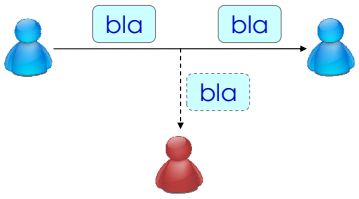

Abb. 6: Abhören von Nachrichten

Löschen (engl. deletion): Die Nachricht oder ein Teilbereich der Nachricht wird auf dem Weg zwischen den beiden Kommunikationspartnern (blau) von einer unberechtigten Drittperson (rot) ungewollt oder vorsätzlich entfernt oder gelöscht (Man-in-the-middle-Angriff).

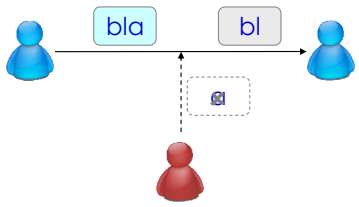

Abb. 7: Löschen von Nachrichten

Verändern (engl. manipulation): Die Nachricht wird auf dem Weg zwischen den beiden Kommunikationspartnern (blau) von einer unberechtigten Drittperson (rot) verändert oder manipuliert, sodass die veränderte Nachricht nicht mehr mit der ursprünglichen Nachricht entspricht (Man-in-the-middle-Angriff).

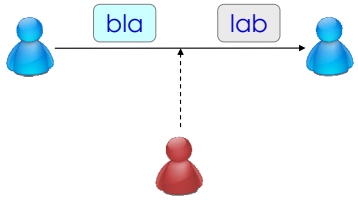

Abb. 8: Verändern von Nachrichten

Einfügen (engl. insertion): In den Nachrichtenaustausch zwischen den beiden Kommunikationspartnern (blau) wird von einer unberechtigten Drittperson (rot) eine Nachricht eingefügt, die von beiden Kommunikationspartnern nicht gewünscht wird (Man-in-the-middle-Angriff).

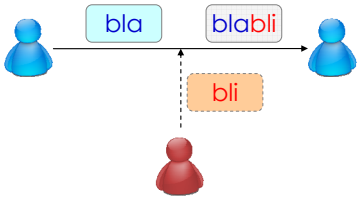

Abb. 9: Einfügen von Nachrichten

Wiederholen (engl. replay): In den Nachrichtenaustausch zwischen den beiden Kommunikationspartnern (blau) wird von einer unberechtigten Drittperson (rot) eine bereits versandte Nachricht unerwünschter Weise erneut in die Kommunikation eingefügt (Man-in-the-middle-Angriff).

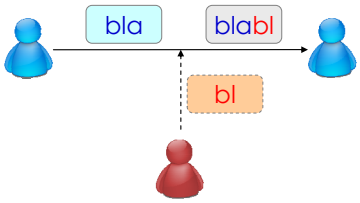

Abb. 10: Wiederholen von Nachrichten

Bestreiten (engl. non-repudiation): Der Nachrichtenaustausch zwischen den beiden Kommunikationspartnern (rot und blau) wird bestritten: Der Nachrichtenempfänger bestreitet die Nachricht erhalten zu haben oder der Nachrichtensender bestreitet die Nachricht gesendet zu haben.

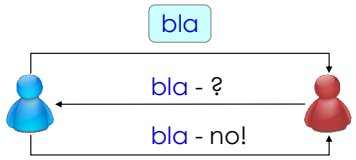

Abb. 11: Bestreiten des Versands oder Empfangs von Nachrichten

Vortäuschen (engl. masquerade oder spoofing): Eine Person (rot) gibt mittels falscher Identität vor ein vertrauenswürdiger Kommunikationspartner (blau) zu sein. Spoofing ist eine Grundvoraussetzung für weitere Manipulationsmechanismen wie Phising (Abhören von sensiblen Daten durch gefälschten Nachrichtenversand).

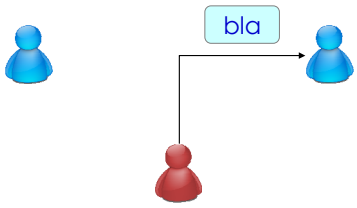

Abb. 12: Vortäuschen einer Identität

2.2.2.2. Bedrohungen

Die oben erwähnten Angriffsklassen werden von Angreifern einzeln oder in kombinierter Form eingesetzt. Es ergeben sich dadurch unter anderem die folgenden Arten der Bedrohung für Web Services (Saraha et al., 2006):

- **DoS-Angriff** (engl. denial-of-service attack): Dabei wird vom Angreifer versucht die Verfügbarkeit eines Web Services so einzuschränken, dass ein autorisierter Nutzer den Dienst nicht erreichen kann. Dies kann durch eine grosse Anzahl von „sinnlosen" Serviceanfragen erfolgen, was zu einer Überlastung der Systemressourcen führen kann.
- **Mann-in-der-Mitte-Angriff** (engl. man-in-the-middle attack): Der Angreifer versucht den Kommunikationskanal unter seine Kontrolle zu bringen um Zugriff zu vertraulichen Informationen zu erlangen oder den Datenverkehr manipulieren zu können.
- **Wiedereinspielungs-Angriff** (engl. replay attack): Der Angreifer versucht einen alten Authentifizierungsnachweis zu nutzen um sich unberechtigt Zugriff auf die Informationen zu verschaffen.
- **XML-Angriff** (engl. XML poisoning): Da Web Services über XML-Protokolle miteinander kommunizieren, kann ein Angreifer ein XML-Angriffsdokument mit sehr grosser Tiefe (sehr viele Unterklassen und Attribute) und Grösse an den Service senden.

Wenn der Service über einen DOM-Parser[28] verfügt, wird versucht das gesamte Dokument beim Parsen in den Arbeitsspeicher zu schreiben, was zu einer Überlastung der Ressourcen (vgl. DoS-Angriff) führen kann. Weniger kritisch sind diese Attacken bei einem SAX-Parser[29], da dieser pro Schritt jeweils nur eine Linie parst und interpretiert. Aber auch bei der Verwendung eines SAX-Parsers kann ein Angreifer bei fehlender Werteprüfung mittels eines mehrdeutigen Attributs eine Inkonsistenz provozieren, was zu ungewünschten Ergebnissen führen kann.

- **Falsche Parameterangabe :** Wenn bei einem Web Service nicht alle Parameter der Anfrage auf deren Gültigkeit hin getestet werden, kann ein Angreifer versuchen, durch die Übergabe eines ungültigen Parameters den Service lahm zu legen (vgl. DoS-Angriff) oder ein unerwünschtes Verhalten zu verursachen.

Die Auflistung der oben beschriebenen Angriffsarten und Bedrohungen ist mit Sicherheit nicht abschliessend, zeigt aber eine Auswahl von möglichen Angriffen. Es gilt jedoch anzumerken, dass diese Angriffe meist aus einer Kombination von verschiedenen Angriffsarten bestehen und damit eine grosse Herausforderung für die Sicherheitsvorkehrungen einer Service-Infrastruktur bedeuten. Beim Einsatz von immer neuen und besseren Sicherheitstechnologien wird immer auch mit einer Vielzahl neuer und versierter Angriffsszenarien respektive Angriffs-kombinationen zu rechnen sein. Für eine detaillierte Einsicht in die Themen Hacking und Serviceangriffe sei auf das Buch „Hacking Web Services“ (Shah, 2006) verwiesen.

2.2.3 Sicherheitsanforderungen aus dem IT-Bereich

Aus der allgemeinen Definition von Sicherheit lassen sich die relevanten Kriterien für ein IT-System ableiten. Dies setzt voraus, dass bekannt ist welche Objekte[30] vor unberechtigten Zugriffen der Subjekte[31] geschützt werden müssen. Dabei ist es essentiell, dass die sicherheitsrelevanten Informationen sowohl vor, als auch während und nach der Verarbeitung vor Beeinträchtigung und Verlust der **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** bewahrt werden. In offenen und verteilten Netzen (z.B. Internet) muss darüber hinaus auch die **Authentizität** von Benutzern und die **Verbindlichkeit** von Kommunikationsbeziehungen

[28] Document Object Model-Parser

[29] Simple API for XML-Parser

[30] Daten- oder Datenobjekte, die Informationen speichern oder verarbeiten können, wie z.B. Dateien, Dienste, Prozesse, etc. (Eckert, 2006)

[31] Benutzer und von Benutzern aktivierte Objekte, wie z.B. Prozesse, Server, etc. (Eckert, 2006)

gewährleistet sein (Flückiger et al., 2004). Nachfolgend sollen diese grundlegenden Sicherheitskriterien erläutert werden (nach Eckert 2006 und Schmidt 2006):

2.2.3.1. Vertraulichkeit

In einer Organisation gibt es viele Informationen, die nur einem bestimmten Personenkreis zugänglich sein dürfen und auf Grund ihres Inhalts als vertraulich einzustufen sind. Geraten solche Informationen in falsche Hände kann daraus ein grosser Schaden entstehen. Ein IT-System wird dann als vertrauenswürdig eingestuft, wenn es keine unautorisierte Informationsgewinnung zulässt. Dies setzt voraus, dass Berechtigungen festgelegt und diese beim Zugriff überprüft und durchgesetzt werden können. Die Feststellung des Informationsflusses zwischen den Subjekten stellt sicher, dass Subjekte weder absichtlich noch unabsichtlich Kenntnis von Informationen erlangen, für die sie nicht autorisiert sind.

2.2.3.2. Integrität

Für den Aspekt der Integrität (engl. integrity) ist es zentral, dass Informationen nicht unbefugt und unbemerkt verändert werden dürfen. Die Integrität eines Systems ist dann gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Integrität beinhaltet zum einen die Festlegung von Nutzungsrechten an Objekten (z.B. Lese- oder Schreibrecht) oder Eigenschaften von Objekten (z.B. Methode, Funktionen), so dass der Zugriff und die Manipulationsmöglichkeiten bereits entsprechend eingeschränkt sind. Zum anderen sind die Nutzungsrechte an Subjekte zu vergeben, so dass diese autorisiert sind den vorgesehenen Zugriff (und nur diesen) durchzuführen. Ein weiterer Bestandteil von Integrität ist es, die im Vornherein nicht verhinderbaren unautorisierten Manipulationen erkennen und nachvollziehen zu können.

2.2.3.3. Verfügbarkeit

In vielen Geschäftsprozessen ist die Verwendung von IT-Diensten so zentral, dass durch einen Ausfall eines Dienstes die gesamte Prozesskette unterbrochen wird und die unternehmerische Tätigkeit nicht mehr zu erbringen ist. Die Verfügbarkeit (engl. availability) ist demzufolge die Wahrscheinlichkeit, dass ein Subjekt das IT-System zu einem bestimmten Zeitpunkt als funktionsfähig wahrnimmt und entsprechend seinen Rechten nutzen kann. Diese Anforderung ist vor allem aus Sicht der Dienstadministration von Bedeutung und für die weiteren Betrachtungen der allgemeinen Sicherheitsüberlegungen im Rahmen dieser Arbeit nicht relevant.

2.2.3.4. Authentizität

Wie auch bei der Manipulation kann die Falscheinspielung von Daten für eine Organisation verheerende Folgen haben. Authentizität (engl. authenticity) ist hierbei ein wichtiger Aspekt, der mit Hilfe einer eindeutigen Identität oder charakteristischen Eigenschaft die Echtheit und Glaubwürdigkeit eines Subjekts (respektive Objekts) überprüfbar macht. Basierend auf einer eindeutigen Erkennung des Subjekts (z.B. mittels Benutzername) wird durch die Angabe einer charakterisierenden Eigenschaft (z.B. Passwort, Chipkarte, biometrisches Merkmal) dessen Identität nachgewiesen. Solche Identitätsnachweise werden häufig als „Credentials“ bezeichnet.

2.2.3.5. Verbindlichkeit

Die Verbindlichkeit bzw. Nicht-Abstreitbarkeit (engl. non-repudiation) setzt sich aus den beiden oben genannten Kriterien der Authentizität und Integrität zusammen und ist vor allem in den Bereichen eCommerce und eBusiness von grosser Bedeutung. Ein IT-System gilt dann als verbindlich, wenn ein Subjekt die Durchführung einer in Anspruch genommen Dienstnutzung im Nachhinein nicht abstreiten kann. In diesem Zusammenhang ist auch die Anrechenbarkeit (engl. accountability) zu nennen, da sie die Verbindlichkeit durch Überwachungs- und Protokollierungsmechanismen ergänzt.

Für die Evaluation eines umfassenden Sicherheitskonzepts sind diese fünf Anforderungen von zentraler Bedeutung. Sie bilden die Grundlage für die Konzeption des Sicherheitsframeworks.

2.2.4 Die OSI-Sicherheitsarchitektur

2.2.4.1. Bedeutung

Die OSI-Sicherheitsarchitektur ist ein internationaler Standard der ISO[32] und der ITU[33] für die Spezifikation von Sicherheitsdiensten (engl. security service) und Sicherheitsmechanismen (engl. security mechanism) in offenen Kommunikationssystemen. Im Rahmen des Standards werden allgemeine Begriffe und Dienste im Sicherheitsumfeld beschrieben. Die OSI-Sicherheitsarchitektur basiert auf der Struktur des ISO/OSI-Referenzmodells und zeigt, auf welchen Ebenen des Referenzmodells die jeweiligen Sicherheitsmassnahmen einzusetzen sind. Sie dient damit als Grundlage für die einheitliche und systemunabhängige Beschreibung von

[32] ISO 7498-2, ISO 10181-1 bis ISO 10181-7: http://www.iso.org (30.06.2007)

[33] ITU-T X.800 bis X.830: http://www.itu.int (30.06.2007)

sicheren Verbindungen zwischen Clients und Web Services respektive service-orientierten Architekturen.

2.2.4.2. ISO/OSI Referenzmodell

Das ISO/OSI-Referenzmodell[34] ist ein Standard für die Architektur von offenen Kommunikationssystemen und beschreibt alle Ebenen der Informationsübermittlung von der physikalischen Datenübertragung bis hin zur Applikationsschicht. Das ISO-Schichtenmodell umfasst folgende sieben Schichten:

1. Bitübertragungsschicht (engl. physical layer): Übertragung eines Datenstroms über ein Trägermedium (elektrische oder optische Signale, elektromagnetische Wellen oder Schallwellen).
2. Sicherungsschicht (engl. data link layer): Die gesicherte und fehlerfreie Datenübertragung von Daten zwischen zwei Stationen (z.B. Paketaufteilung, Prüfsumme).
3. Netzwerkschicht (engl. network layer): Die effiziente Datenübertragung zwischen zwei Rechnern (Paketrouting und Adressierung).
4. Transportschicht (engl. transport layer). Die gesicherte Datenübertragung zwischen zwei Diensten bzw. Prozessen (End-to-End-Communication).
5. Sitzungsschicht (engl. session layer): Die Synchronisationsfunktionen bei der Übertragung von Daten zwischen zwei Diensten bzw. Prozessen.
6. Präsentationsschicht (engl. presentation layer): Die Anpassung der gesendeten Datenstruktur an die verlangte Datenstruktur (Datenformat, Datenkompression).
7. Anwendungsschicht (engl. application layer): Die Nutzung des Datenstroms in Form einer Anwendung oder Applikation als Schnittstelle zum Benutzer.

In einer vernetzten Infrastruktur werden neben den Endsystemen (Rechner A und B) auch Vermittlungsrechner (Router, Gateways etc.) eingesetzt, die die Daten an den gewünschten Ort weiterleiten. Diese Vermittlungsrechner verwenden die Informationen aus den ersten drei Schichten (Schicht 1-3) dem sogenannten Kommunikations-Subsystem, wie aus der nachfolgenden Grafik (Abb. 13) hervorgeht (Eckert, 2006).

[34] OSI Basic Reference Model ISO/IEC 7498-1: http://www.iso.org (30.06.2007)

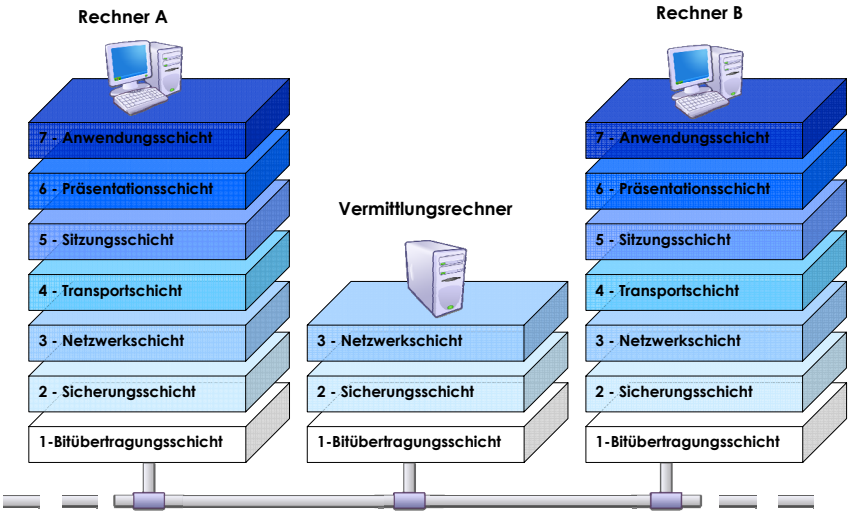

Abb. 13: ISO/OSI-Referenzmodell

Das ISO/OSI Referenzmodell legt keine Dienste, Protokolle oder Implementierungshinweise für die jeweiligen Schichten fest. Es beschreibt lediglich, welche Funktionalität die jeweilige Schicht zur Verfügung stellen soll (funktionaler Design-Ansatz).

2.2.4.3. Sicherheitsdienste

Die OSI-Sicherheitsarchitektur unterscheidet fünf Klassen von Sicherheitsdiensten. Die Aufgaben der jeweiligen Sicherheitsdienste und die Empfehlungen auf welcher Ebene sie anzusiedeln sind werden nachfolgend beschrieben (Eckert, 2006).

1. **Authentifizierung** (engl. authentication): Authentifizierungsdienste haben die Aufgabe, jede Entität (Datenpaket) zweifelsfrei zu identifizieren. Es wird zwischen einseitiger und wechselseitiger Kommunikation zwischen Endpunkten unterschieden. Bei der einseitigen Authentifizierung (engl. data origin) geht es darum, den Sender bzw. Autor einer Nachricht eindeutig identifizieren zu können. Bei einer wechselseitigen Kommunikation (engl. peer entity) authentifizieren sich die Kommunikationspartner gegenseitig. Authentifizierungsdienste sind gemäss der Empfehlung der OSI auf der Anwendungsschicht (Schicht 7) einzusetzen. Einzelne Grundfunktionalitäten der Authentifizierung werden auch auf den Ebenen der Transport- und Netzwerkschicht (Schichten 3 und 4) angewendet.
2. **Zugriffskontrolle** (engl. access control): Die Dienste zur Zugriffskontrolle verhindern eine unautorisierte Nutzung von Systemressourcen. Als solche Ressourcen werden Informationen (Dateien, Datenbanken etc.), Dienste (Prozesse, Funktionen) und auch

die Kommunikation als solche (Pakete, Ports etc.) verstanden. Zugriffskontrolldienste können bereits auf unteren Anwendungsschichten (Schichten 3 und 4) zum Einsatz kommen, wobei es sich hier vor allem um Firewall-Funktionalitäten handelt (Bridges, Router etc.). Die gezieltesten Kontrollen lassen sich auch hier auf der obersten Schicht (Schicht 7) des ISO-Referenzmodells durchführen.

3. **Vertraulichkeit** (engl. confidentiality): Vertraulichkeitsdienste schützen die Daten vor einer unberechtigten Offenlegung, wobei sich vier verschiedene Sicherungsmassnahmen unterscheiden lassen. Verbindungsorientierte Vertraulichkeitsdienste (engl. connection) betrachten die Verbindung zwischen den Kommunikationspartnern als eine Einheit und wenden für alle Datenpakete, die über die jeweilige Verbindung übertragen werden, die gleichen Verfahren und Schlüssel an. Bei verbindungslosen Diensten (engl. connectionless) werden einzelne Datenpakete als Einheiten betrachtet und jeweils individuell abgesichert. Gleiches gilt auch für die dritte Art von Vertraulichkeitsdiensten, bei denen die Vertraulichkeit nur für einzelne Datenfelder (engl. selective fields) gebraucht wird. Mit dem Dienst zur Sicherstellung der Vertraulichkeit von Verkehrsdaten (engl. traffic flow) wird eine Verkehrsflussanalyse verhindert. Damit soll es potentiellen Angreifern verunmöglicht werden herauszufinden, wer mit wem, in welchem Umfang und zu welcher Zeit kommuniziert. Für die Vertraulichkeitsdienste werden die Schichten 4, 6 und 7 empfohlen - es können aber auch Dienste auf tieferen Schichten (1 bis 4) implementiert werden (z.B. IPSec). Auch hier gilt, dass die oberste Schicht die adäquatesten Absicherungsmöglichkeiten bietet, die beispielsweise für die vertrauliche Behandlung von einzelnen Datenfeldern zwingend erforderlich sind.

4. **Integrität** (engl. integrity): Datenintegritätsdienste sollen das unautorisierte Manipulieren von Daten (Modifizieren, Einfügen, Löschen, Umordnen, Duplizieren, Wiedereinspielen) erkennen. Mit der Recovery-Fähigkeit ist es möglich die Manipulationen nicht nur zu erkennen, sondern auch abzuwehren (z.B. durch erneuten Versand des Datenpakets oder durch Einsatz eines fehlerkorrigierenden Codes). Analog zu Vertraulichkeitsdiensten ist es auch möglich, Massnahmen zur Gewährleistung der Integrität nur für ausgewählte Datenfelder (engl. selective field) oder Datenpakete (engl. connectionless) zu überprüfen. Für den Einsatz von Integritätsdiensten gilt gleiches wie für die Vertraulichkeitsdienste, sie werden am Besten auf den Schichten 3, 4 und 7 integriert.

5. **Verbindlichkeit** (engl. non-repudiation): Verbindlichkeitsdienste stellen sicher, dass keiner der beteiligten Kommunikationspartner die Beteiligung im Nachhinein leugnen kann (Nicht-Abstreitbarkeit). Durch einen Nachweis über Nachrichtenursprung und Inhalt des Datenpakets (engl. proof of origin) kann der Empfänger den Erhalt der Nachricht nicht abstreiten und der Absender kann beweisen, dass das Paket auch wirklich von ihm übermittelt wurde. Andererseits muss auch der Empfang der Nachricht bestätigt werden, so dass der Empfänger den Erhalt eines Datenpakets nicht abstreiten kann und der Absender den Versand beweisen kann (engl. proof of delivery). Verbindlichkeitsdienste sind sehr stark von der jeweiligen Anwendung abhängig, so dass deren Integration auf der obersten Schicht (Schicht 7) vorzunehmen ist.

Die nachfolgende Zusammenstellung (Tab. 3) soll einen Überblick über die oben genannten Klassen der OSI-Sicherheitsdienste vermitteln.

#	Description	
1.1	Authentication	Peer Entity
1.2		Data Origin
2.1	Access Control	
3.1	Confidentiality	Connection
3.2		Connectionless
3.3		Selective Field
3.4		Traffic Flow
4.1	Integrity	Connection with Recovery
4.2		Connection without Recovery
4.3		Connectionless
4.4		Selective Field
5.1	Non-Repudiation	Proof-of-origin
5.2		Proof-of-delivery

Tab. 3: Klassifikation der OSI-Sicherheitsdienste (nach ISO, 1989)

2.2.4.4. Sicherheitsmechanismen

Neben den erwähnten Sicherheitsdiensten sind in der OSI-Sicherheitsarchitektur auch Mechanismen definiert, mit denen sich IT-Systeme absichern lassen. Man unterscheidet zwischen spezifischen (engl. specific) und durchgängigen (engl. pervasive) Mechanismen. Durchgehende Mechanismen gehören in das Aufgabengebiet eines Sicherheitsmanagements (Ereigniserkennung, Sicherheitsaufzeichnung) und sind für die Betrachtung im Rahmen dieser Arbeit nicht relevant. Interessant in Zusammenhang mit den zu planenden Massnahmen sind

jedoch die spezifischen Mechanismen. Die folgenden Verfahren werden von der OSI-Sicherheitsarchitektur benannt:

A. **Kryptografische Verfahren** (engl. encipherment) dienen zur Sicherstellung der Vertraulichkeit für Nutzerdaten und Verkehrsinformationen. Zu diesen Verfahren zählen symmetrische und asymmetrische Verschlüsselungsverfahren (vgl. Kap. 2.3.1)

B. **Digitale Signaturen** (engl. digital signature) bilden das Pendant zu handschriftlichen Unterschriften und dienen als Beweis für die Überprüfung von Datenpaketen oder deren Hashwerte durch eine Notariatsinstanz (vgl. Kap. 2.3.1.2).

C. **Zugriffskontrollmechanismen** (engl. access control) beinhalten die Verwaltung der Rechte und Kontrolle von Zugriffen auf ein System (vgl. Kap. 2.3.4.2).

D. **Datenintegritätsmechanismen** (engl. data integrity mechanisms) dienen zur Sicherstellung der Integrität, d.h. um unautorisierte Datenmanipulationen zu verhindern.

E. **Mechanismen zum Austausch von Authentizitätsinformationen** (engl. authentication exchange) ermöglichen die Identifikation von Subjekten entweder durch Wissen, durch Besitz oder durch ein persönliches Merkmal (vgl. Kap. 2.3.4.1).

F. Mit der **Verschleierung oder Anonymisierung von Verkehrsdaten** (engl. traffic padding mechanisms) soll eine Verkehrsflussanalyse verhindert werden. Dies kann unter anderem durch den Aufbau von zusätzlichen Dummy-Verbindungen oder durch den Versand zusätzlicher Informationen (z.B. Dummy-Datenpaket oder Fülldaten in einem regulären Datenpaket) erreicht werden.

G. **Mechanismen zu Kontrolle der Wegewahl** (engl. routing control) haben durch explizite Routing-Entscheide die Möglichkeit, Informationen auf sicherem Weg an ihr Ziel zu bringen. Dabei werden Datenpakete die eine Sicherheitsklassifikation (engl. labeling) tragen so weitergeleitet, dass sie nur von Vermittlungsrechnern (Router, Hubs etc.) bearbeitet werden dürfen, die eine entsprechende Sicherheitseinstufung besitzen.

H. **Notariatsmechanismen** (engl. notarization mechanisms) ermöglichen eine sichere Zuweisung von spezifischen Eigenschaften der übermittelten Datenpakete wie z.B. Erzeugungsdatum, Ursprung und Ziel (vgl. Kap. 2.3.1.2).

Die nachfolgende Tabelle (Tab. 4) zeigt auf, welche der genannten Mechanismen einzeln oder gemeinsam mit anderen die Anforderungen der Sicherheitsdienste abdecken können. Ein Mechanismus wird auch dann als geeignet (✓) eingestuft, wenn er mehr als die zur Erfüllung der Dienstanforderung notwendigen Eigenschaften bietet.

Security mechanisms / Security service			A. Encipherment	B. Dig. Signature	C. Access Control	D. Data Integrity	E. Authentication	F. Traffic Padding	G. Routing Control	H. Notarization
1.1	Authentication	Peer Entity	✓	✓	×	×	✓	×	×	×
1.2		Data Origin	✓	✓	×	×	×	×	×	×
2.1	Access Control		×	×	✓	×	×	×	×	×
3.1	Confidentiality	Connection	✓	×	×	×	×	×	✓	×
3.2		Connectionless	✓	×	×	×	×	×	✓	×
3.3		Selective Field	✓	×	×	×	×	×	×	×
3.4		Traffic Flow	✓	×	×	×	×	✓	✓	×
4.1	Integrity	With Recovery	✓	×	×	✓	×	×	×	×
4.2		Without Recovery	✓	×	×	✓	×	×	×	×
4.3		Connectionless	✓	✓	×	✓	×	×	×	×
4.4		Selective Field	✓	✓	×	✓	×	×	×	×
5.1	Non-	Proof-of-origin	×	✓	×	✓	×	×	×	✓
5.2	Repudiation	Proof-of-delivery	×	✓	×	✓	×	×	×	✓

Tab. 4: Beziehung zwischen Sicherheitsdiensten und -mechanismen (nach ISO, 1989)

Die Vorgaben der OSI-Sicherheitsarchitektur hinsichtlich der erforderlichen Dienste und Mechanismen gilt es bei der Konzeption einer sicheren GDI zu beachten. Diesem Sachverhalt wird im Rahmen des Lösungsansatzes (Kap. 3) Rechnung getragen.

2.2.5 Integrierte Sicherheitsarchitektur

Ein anderer Ansatz um das Thema Sicherheit in einer verteilten Infrastruktur zu definieren, basiert auf dem Konzept einer integrierten Sicherheitsarchitektur (Abbie, 2003). Dabei wird die Sicherheit von Web Services als Bestandteil eines übergeordneten, institutions- respektive abteilungsweiten Sicherheitskonzepts verstanden. Sicherheit definiert innerhalb dieses Konzepts den Prozess zur Absicherung aller System-, Netzwerk- und Applikationsressourcen. Die Sicherheitsarchitektur soll das Management von Sicherheitsrichtlinien unterstützen und basiert auf den folgenden Grundprinzipien (Abbie, 2003):

- Eine mehrschichtige Sicherheit (engl. multi-layer security) definiert Schutzfunktionen für die drei wesentlichen Ebenen der Architektur:
    1. Netzwerkebene (OSI-Schichten 1 bis 3)

2. Netzwerkunterstützende Ebene (OSI-Schichten 4 bis7)
3. Applikationsebene (OSI-Schicht 7)

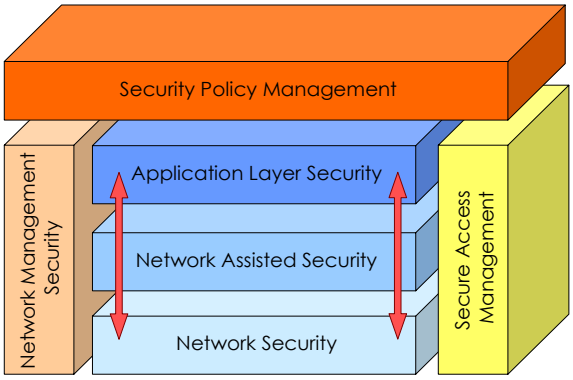

Abb. 14: Integrierte Sicherheitsarchitektur (nach Abbie, 2003)

- Durch ein einheitliches Rechtemanagement (engl. security policy management) können die definierten Sicherheitsmassnahmen auf Applikations- und Netzwerkebene konfiguriert und durchgesetzt werden.
- Ein einheitliches Zugriffsmanagement (engl. secure access management) ermöglicht neben der Authentifizierung und Verwaltung der User auch eine rollenbasierte Zugriffskontrolle auf alle angebotenen Ressourcen einer Institution.
- Mit einem sicheren Netzwerkmanagement (engl. network management security) werden geeignete Operationen für die Erfassung und Überprüfung von Nutzerdaten und Zugriffsverhalten innerhalb des Systems zur Verfügung gestellt.

Der Ansatz der integrierten Sicherheitsarchitektur fasst die sieben Ebenen des OSI-Schichtenmodells auf drei, für die Gewährleistung der Sicherheit relevante, Ebenen zusammen. In einer eher konzeptuellen Betrachtungsweise werden bei der integrierten Sicherheits-architektur die Grundprinzipien eines Sicherheitsframeworks aufgezeigt. Diese Anforderungen gilt es beim Entwurf des Sicherheitskonzeptes (Kap. 3) zu berücksichtigen.

2.3 Sicherheit bei Web Services

Die allgemeinen IT-Sicherheitsanforderungen haben auch im Bereich der Web Services ihre Gültigkeit und werden durch unterschiedliche Standards oder Spezifikationen abgedeckt. Die nachfolgende Zusammenstellung soll die relevanten Sicherheitsverfahren im Bereich der Web Services aufzeigen.

2.3.1 Verschlüsselung

Die Verschlüsselung[35] (engl. encryption) oder Kryptografie bietet Methoden, wie der Inhalt einer Nachricht gegenüber unberechtigter Einsicht von Dritten geschützt werden kann. Das Verschlüsseln oder Signieren von Nachrichten ist deshalb eine wesentliche Voraussetzung für die Vertraulichkeit von Nachrichten. Man unterscheidet gemeinhin zwischen symmetrischer und asymmetrischer Verschlüsselung (Muster, 2006).

- Bei der symmetrischen Verschlüsselung (Secret-Key Verfahren) wird für die Verschlüsselung der Nachricht und für die Entschlüsselung der Nachricht derselbe Schlüssel verwendet. Die bekanntesten Verfahren für die symmetrische Verschlüsselung sind DES[36] und Triple-DES[37] sowie IDEA[38].
- Bei der asymmetrischen Verschlüsselung (Public-Key Verfahren) sind die Verschlüsselungsschlüssel und die Entschlüsselungsschlüssel verschieden. Das gebräuchlichste Verfahren für die asymmetrische Verschlüsselung ist RSA[39].

Asymmetrische Verfahren sind auf Grund der grösseren Schlüssellängen in der Regel rechenintensiver als symmetrische Verfahren. Sie sind aber auch entsprechend sicherer. Im Internet wird zur Verschlüsselung von Nachrichten häufig eine Kombination aus symmetrischen und asymmetrischen Verfahren angewendet. Bei diesen Hybridverfahren wird der Schlüssel

[35] Die Verschlüsselung stellt im Grunde eine Thematik der allgemeinen IT-Sicherheit dar und ist keine Web Service spezifische Anforderung. Der Fokus im Rahmen der nachfolgenden Betrachtung lag vor allem auf den für Web Services relevanten Teilbereichen.

[36] Data Encryption Standard Verschlüsselungsalgorithmus mit einer Schlüssellänge von 56 Bits (FIPS, 1999)

[37] Triple-Data Encryption Standard Verschlüsselungsalgorithmen mit einer Schlüssellänge 168 Bits (FIPS, 1999)

[38] International Data Encryption Algorithm mit einer Schlüssellänge von 128 Bit (IDEA, 2005)

[39] Kryptografie-Standard nach Rivest, Shamir und Adleman mit einer variablen Schlüssellänge; Gebräuchliche RSA-Verfahren verwenden derzeit Schlüssellängen von 1024 Bit (RSA, 2002)

eines symmetrischen Verfahrens (z.B. DES oder IDEA) mit Hilfe eines asymmetrischen Verfahrens (z.B. RSA) ausgetauscht. Die weitere Kommunikation wird dann aber auf Basis der symmetrischen Verschlüsselung durchgeführt.

Bei beiden Verfahren wird in der Regel nicht nur die gesamte Nachricht verschlüsselt, sondern auch eine aus der Nachricht resultierende kryptografische Prüfsumme - der so genannte Hashcode. Der Hashcode ist eine Bitfolge von bestimmter Länge, der die Nachricht eindeutig repräsentiert (Signatur) und mit Hilfe einer Hashfunktion erstellt wird. Die Sicherheit einer Hashfunktion ist stark von der Länge der Hashcodes (Länge der Prüfsumme) abhängig. Hashfunktionen mit einem Hashcode von kleiner als 160 Bit gelten in der Praxis als unsicher, falls die Sicherheit über eine grössere Dauer gewährt sein soll (Muster, 2006). Die nachfolgende Tabelle zeigt eine Übersicht über die in der Praxis verwendeten Hashfunktionen und deren Hashcodelängen.

Hashfunktion	Länge des Hashcodes
SHA / SHA-1	160 Bit
SHA 256	256 Bit
SHA 384	384 Bit
SHA 512	512 Bit
RIPEMD-160	160 Bit

Tab. 5: Hashfunktionen und Hashcodes (nach Muster, 2006)

2.3.1.1. Elektronische Signatur

Die elektronische oder digitale Signatur basiert auf der Technik der asymmetrischen Verschlüsselung und unterscheidet zwei Arten von kryptografischen Schlüsseln. Zum einen den privaten Schlüssel (engl. private key), der geheim bleiben muss und zum anderen sein Gegenstück, den öffentlichen Schlüssel (engl. public key), der bekannt gegeben werden kann. Mit dem privaten Schlüssel (oder Signaturschlüssel) wird eine elektronische Nachricht signiert, während der öffentliche Schlüssel (oder Signaturprüfschlüssel) dem Empfänger erlaubt, die elektronische Signatur des Absenders zu überprüfen. Ist das Ergebnis dieser Überprüfung positiv, ist der Empfänger sicher, dass der Inhalt bei der Dateiübermittlung nicht geändert wurde.

Der öffentliche Schlüssel befindet sich in einem elektronischen Zertifikat, das von einer vertrauenswürdigen dritten Stelle, der Zertifizierungsstelle (engl. certification authority oder Trust Center) ausgestellt wird. Die Hauptfunktion des elektronischen Zertifikats besteht darin,

einen öffentlichen Schlüssel einer bestimmten Person oder Organisation (Subjekt) zuzuordnen, die bei der Ausgabe des Schlüssels mit Hilfe eines eindeutigen Merkmals identifiziert wurde. Im Gegenzug dazu erhält das Subjekt von der Zertifizierungsstelle ein Zertifikat, das ihm und allen anderen bescheinigt, dass sein öffentlicher Signierschlüssel eindeutig seiner Identität zugeordnet werden kann. Der Empfänger der elektronisch signierten Nachricht kann sich bei der Zertifizierungsstelle über die Identität des Absenders informieren und „kennt“ dadurch seinen Kommunikationspartner (Bakom, 2004a).

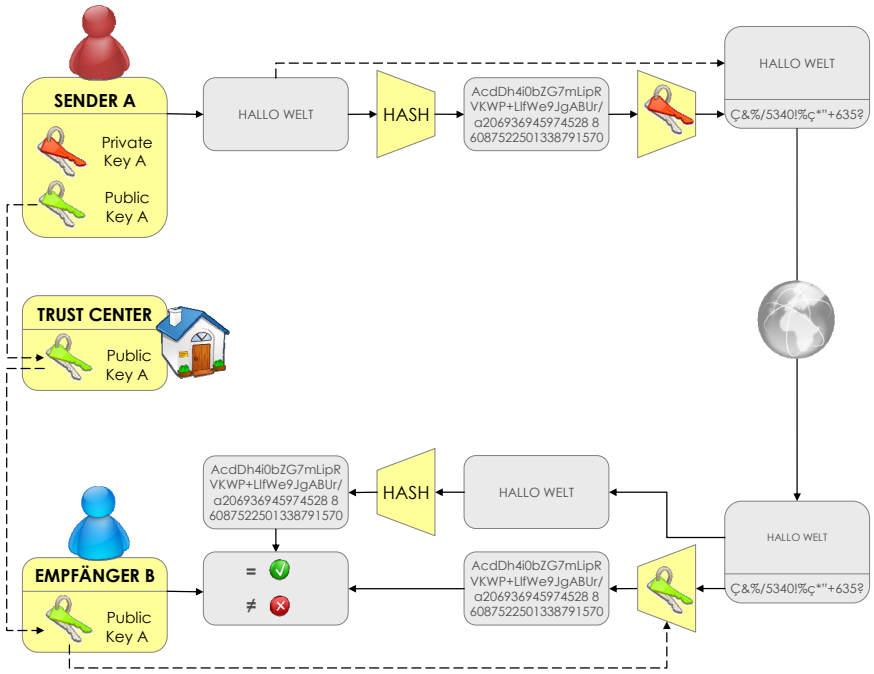

Abb. 15: Signierung und Verifikation einer Nachricht (nach Muster, 2006)

Das Verfahren für den Austausch einer Nachricht könnte wie folgt ablaufen (Muster, 2006):

1. Sender A möchte eine Nachricht an Empfänger B versenden. Dazu veröffentlicht er seinen öffentlichen Schlüssel in einem Trust Center, wo auch B Zugriff hat.
2. Sender A generiert nun aus der Kopie seiner Nachricht mit Hilfe eines Hashverfahrens einen Hashcode (Bitstring) und verschlüsselt diesen mit seinem privaten Schlüssel. Die dadurch entstandene Signatur hängt Sender A nun an die Nachricht und sendet sie über das Netzwerk (z.B. Internet) an Empfänger B.
3. Empfänger B bildet aus der Kopie der erhaltenen Nachricht wiederum einen Hashcode. In einem zweiten Schritt entschlüsselt Empfänger B die erhaltene Signatur mit dem öffentlichen Schlüssel von Sender A, den er aus dem Trust Center bezogen hat, und generiert dadurch einen zweiten Hashcode.

4. Empfänger B vergleicht nun die beiden Hashcodes und kann bei deren Gleichheit sicher sein, dass die Nachricht von niemandem unterwegs verändert wurde.
5. Das Trust Center kann Empfänger B bestätigen, dass der öffentliche Schlüssel A auch wirklich Sender A gehört.

Ein weit verbreitetes Verfahren für den Austausch von Zertifikaten definiert der X.509 Standard[40] der ITU. Ein X.509-Zertifkat enthält neben den Informationen, die für eine Identifizierung eines Nutzers benötigt werden (Benutzername, öffentlicher Schlüssel) auch die Angaben über die Zertifizierungsinstanz (Name, öffentlicher Schlüssel, Seriennummer) und die Beschreibung der zur Signierung des Zertifikats verwendeten Algorithmen und Parameter. Jedes Zertifikat hat eine Gültigkeitsdauer die durch eine Anfangs- und einen Endpunkt definiert ist. Zu beachten ist aber, dass ein Zertifikat weder eine Aussage über den Inhalt des signierten Dokuments noch über die Vertrauenswürdigkeit der signierenden Person machen kann (Eckert, 2006). Die Qualität des Zertifikats hängt davon ab, wie sorgfältig der Anbieter von Zertifizierungsdiensten die Identität des Zertifikatinhabers überprüft hat. Es liegt in der Verantwortlichkeit der ausstellenden Zertifizierungsstelle sicher zu stellen, dass kein Zertifikat oder dessen Seriennummer mehrfach ausgestellt werden.

Seit Inkrafttreten der entsprechenden Gesetze und Verordnungen (ZertES[41], VZertES[42] und TAV[43]) am 1.1.2005 kann in der Schweiz im privaten Geschäftsverkehr elektronisch signiert werden. Mit der neuen Gesetzgebung werden die elektronische Signatur und die handschriftliche Unterschrift unter bestimmten Bedingungen als gleichwertig betrachtet. Dies betrifft vor allem Rechtsgeschäfte im privaten Geschäftsverkehr, wo eine einfache Schriftlichkeit gefordert ist. Der Geschäftsverkehr mit den Behörden wurde in diesem Gesetz nicht geregelt (Muster, 2006).

2.3.1.2. PKI

Der Einsatz von digitalen Signaturen setzt zwingend gewisse technische und organisatorische Rahmenbedingungen voraus, die unter dem Begriff Public Key Infrastruktur (PKI)

[40] X.509 ist ein ITU-T-Standard für digitale Zertifikate (ITU-T, 2005)

[41] Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bakom, 2003)

[42] Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bakom, 2004b)

[43] Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bakom, 2006)

zusammengefasst sind. Ziel einer PKI ist es, Inhalt und Herkunft von elektronischen Nachrichten zwischen zwei oder mehreren meist unbekannten Subjekten sicher auszutauschen ohne dass sich diese direkt gegenseitig zu kennen brauchen. PKIs werden in den Bereichen eCommerce (zwischen Unternehmen oder zwischen Unternehmen und Einzelpersonen) und eGovernment (zwischen Behörden oder zwischen Behörden und Bürgern) aber auch für die Benutzeridentifikation innerhalb von Grossfirmen eingesetzt. Für die Gewährleistung der Authentizität und Verbindlichkeit in diesen Bereichen sind verschiedene PKI-Komponenten erforderlich:

- Zertifizierungsstelle (engl. certification authority - CA): Stellt Zertifikate aus und signiert diese, veröffentlicht aktuelle Zertifikate und erstellt und veröffentlicht Listen von ungültigen Zertifikaten (engl. certificate revocation list - CRL).
- Registrierungsstelle (engl. registration authority - RA): unterstützt die CA und bürgt für die Verbindung zwischen öffentlichem Schlüssel und Identitäten der Zertifikatsinhaber.
- Verzeichnisdienst (engl. directories): LDAP[44], Verteilung der Zertifikate und CRLs.
- Zeitstempeldienst (engl. time stamping authority -TSA): erstellt signierte Zeitstempel mit Gültigkeitsdauer eines Zertifikats.

Der Aufbau einer PKI und insbesondere einer Zertifizierungsstelle ist aufwendig und muss aus Sicht des Nutzers von einer vertrauenswürdigen Stelle betrieben werden. In der Schweiz ist es privaten Anbietern möglich, sich als Zertifizierungsdienstanbieter (engl. certification service provider - CSP) von der Anerkennungsstelle (engl. certification body) registrieren zu lassen. Die Anerkennungsstellen selbst werden von der Schweizerischen Akkreditierungsstelle (SAS[45]) mit der Anerkennung von Zertifizierungsdiensten beauftragt. Es gibt derzeit schweizweit eine Anerkennunkstelle (KPMG Fides Peat) und drei Zertifizierungsdienstanbieter (Swisscom Solutions AG, QuoVadis Trustlink AG, Die Schweizerische Post - SwissSign AG).

[44] Siehe auch Anhang 1: LDAP

[45] SAS ist Teil des Staatssekretariats für Wirtschaft (SECO): http://www.sas.ch/DE/pki_isms/pki.html (30.06.2007)

2.3.2 Transportsicherheit

2.3.2.1. SSL / TLS

Das SSL[46]-Protokoll ist ein De-facto-Internet-Standard für eine sichere HTTP-Verbindung auf der Transportschicht (Schicht 4 des OSI-Schichtenmodells). SSL ist im Gegensatz zu HTTP ein zustandsbehaftetes Protokoll, dass es erlaubt Sitzungen zwischen den Kommunikationspartner aufzubauen. Ein Client kann zu einem Zeitpunkt mehrere Sitzungen zu verschiedenen Servern unterhalten. Dabei gehört die Authentifizierung von Kommunikationspartnern, der Aufbau einer vertraulichen Ende-zu-Ende Datenübertragung und die Sicherstellung der Integrität der transportierten Nachrichten zu den Hauptaufgaben von SSL. Dazu verwendet SSL eine Kombination aus symmetrischen und asymmetrischen Verschlüsselungsverfahren, wobei versucht wird, beim Verbindungsaufbau (engl. Handshake) möglichst wenig geheime Informationen über das Internet zu transportieren (Eckert, 2006).

Basierend auf SSL wurde das TLS[47]-Protokoll entwickelt, dass sich als Internetstandard durchgesetzt hat. TLS hat in seiner Definition nur geringfügige Unterschiede zu SSL erfahren. So wurden unter anderem die Verfahren zur Schlüsselerzeugung, Verschlüsselung und kryptografischen Hashwertberechnung optimiert. Die Sicherheit von SSL/TLS ist massgeblich von der der Güte der kryptografischen Verfahren abhängig, die die Kommunikationspartner beim Handshake miteinander vereinbaren. Deshalb werden zur Verschlüsselung von SSL/TLS vor allem HMAC[48]-Verfahren angewendet.

Die wohl verbreitetste Ausprägung von SSL/TLS ist die Kombination mit HTTP - besser bekannt als HTTPS. Bei HTTPS wird von einem HTTP-Client ein SSL-basierter Kanal zu einem Server aufgebaut, über den die Daten sicher, vertraulich und vor unbefugten Modifikationen geschützt transferiert werden können. HTTPS hat im Bereich des elektronischen Datenverkehrs eine weite Verbreitung, was vor allem auf die einfache Implementierung auf verschiedenste Systemumgebungen zurückzuführen ist.

Im Hinblick auf die Absicherung von Web Services zeigen sich aber auch die Grenzen von SSL/TLS. Hält man sich vor Augen, dass ein Web Service meist indirekt über einen Service Provider zur Verfügung gestellt wird, zeigt sich der Nachteil einer Ende-zu-Ende Verbindung

[46] Secure Sockets Layer (IETF, 1996a)

[47] Transport Layer Security (IETF, 1999a)

[48] Kryptografisch sicheres Verfahren zur Berechung von MAC-Werten der Kommunikationssysteme.

wie HTTPS. Die Verbindung zwischen Client und Service Provider (Sicherheitskontext 1; vgl. Abb. 16) kann mittels HTTPS abgesichert werden. Der Datenaustausch zwischen Service Provider und Web Service (Sicherheitskontext 2; vgl. Abb. 16) findet jedoch über SOAP statt. Somit endet aus Sicht des Clients die sichere Datenübertragung bei der ersten „Endstelle“, dem Service Provider. Der Client hat damit keine Gewähr, dass bei der Nutzung des Web Services die vertraulichen Daten zwischen dem Service Provider und dem Web Service über eine sichere Verbindung weitergegeben werden (Mahmoud, 2005).

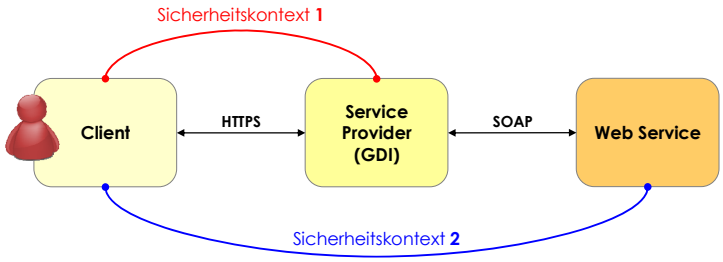

Abb. 16: Indirekter Zugriff auf einen Web Service (nach Mahmoud, 2005)

Im Zusammenhang mit Web Services hat SSL/TLS weitere Nachteile (Mahmoud, 2005):

- SSL/TLS funktioniert wie erwähnt auf der Transportschicht. Daraus folgt, dass die Nachrichten nur während der Dauer des Transports geschützt sind. Somit kann eine Nachricht nicht gespeichert werden, um zu einem späteren Zeitpunkt zu beweisen, dass sie nicht modifiziert wurde.
- SSL/TLS unterstützt keine Vertraulichkeit (Nicht-Abstreitbarkeit). Aus Sicht des Clients lässt es sich nicht nachvollziehen, auf welchem Weg seine Anfrage zwischen Service Provider und Web Service weitergeleitet wurde. Aus Sicht des Web Service Betreibers kann er die Nutzung seines Dienstes nur bis zum Service Provider, nicht aber bis zum Client zurückverfolgen.
- Mit SSL/TLS ist es nicht möglich nur einzelne Elemente einer Nachricht (z.B. Kreditkarteninformation) zu verschlüsseln. Bei grösseren XML-Dokumenten kann dies die Kommunikation unnötig verlangsamen.

2.3.2.2. IPSec

IPSec[49] ist ein Standard der IETF und definiert eine Sicherheitsarchitektur für das Internetprotokoll (IPv4, IPv6). Die Spezifikation von IPSec behandelt den vertraulichen und

[49] Sicherheitsarchitektur für das Internet Protokoll (IETF, 1998)

authentifizierten Transport von IP-Datenpaketen auf der Netzwerkschicht (Schicht 3 des OSI-Schichtenmodells) und legt die kryptografischen Verfahren fest, die jedes IPSec-System anbieten muss (Eckert, 2006). Aufgrund der Tatsache, dass IPSec bereits auf der Netzwerkebene einsetzt, ist es sehr flexibel und kann sowohl TCP- als auch UDP-basierte Protokolle unterstützen. Die hohe Flexibilität bringt aber auch eine Zunahme an Komplexität und Bearbeitungsaufwand mit sich. IPSec wird vor allem für die Verbindung zwischen räumlich verteilten Unternehmensnetzen eingesetzt und dient, wie es der Namen bereits vermuten lässt, zur Absicherung von IP-Paketen. Bevor aber ein sicherer Austausch von IP-Paketen zu Stande kommen kann, müssen sich die Kommunikationspartner über ein genau definiertes Protokoll authentifizieren und sich auf ein Geheimelement einigen (Muster, 2006). Dies kann entweder mittels Signatur (explizierte Authentifizierung) oder mittels Public Key Encryption (implizite Authentifizierung) geschehen. Die Übermittlung des Geheimelements wird durch das Diffie Hellman[50]-Verfahren verschlüsselt. Wenn sich die Kommunikationspartner erfolgreich authentifiziert haben, werden die Session Keys erzeugt, mit denen alle Datenpakete des eröffneten IPSec-Kanals geschützt werden. Für den Austausch der IP-Pakete wird zwischen dem Tunnel- und Transport-Mode unterschieden (Muster, 2006).

- Im Transport-Mode wird der Inhalt eines IP-Pakets geschützt, nicht aber dessen Bestimmungsadressen (IP-Adresse des Ursprung- und Zielorts). Somit kann der Transport-Mode nur dann angewendet werden, wenn der Ursprung des Pakets mit dem Ort der Verschlüsselung und der Zielort des Pakets mit dem Ort der Entschlüsselung übereinstimmt (vgl. Abb. 17).

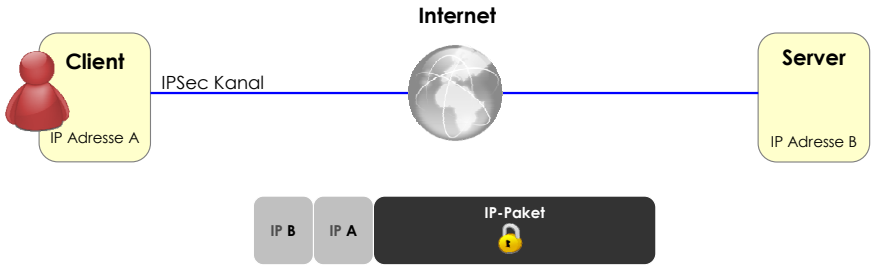

Abb. 17: IPSec-Verbindung im Transport-Mode (nach Muster, 2006)

- Im Tunnel Mode werden Inhalt und Bestimmungsadressen des IP-Pakets verschlüsselt. Dieses Verfahren wird dann angewendet, wenn mindestens eine der beiden oben genannten Bedingungen nicht zutrifft (vgl. Abb. 18).

[50] Kryptografie-Protokoll zur symmetrischen Verschlüsselung (IETF, 1999b)

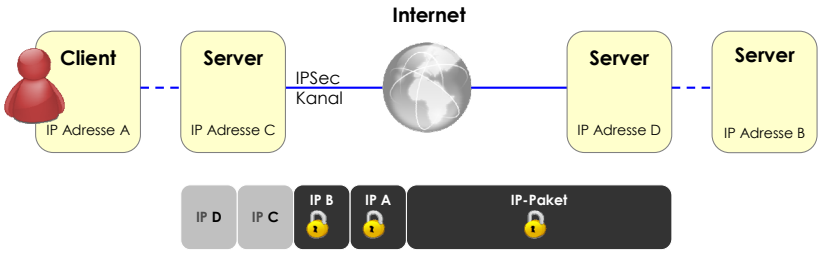

Abb. 18: IPSec-Verbindung im Tunnel-Mode (nach Muster, 2006)

2.3.2.3. VPN

VPN[51] definiert eine Netzinfrastruktur bei der Komponenten eines privaten Netzwerks (z.B. eines LANs) über ein öffentliches Netzwerk (z.B. das Internet) miteinander kommunizieren, wobei ihnen die Kommunikationsverbindung als dedizierte, private Verbindung erscheint.

Mittels einer VPN-Verbindung lassen sich geschützte entfernte Zugriffe von autorisierten Benutzern auf ein Unternehmensnetz realisieren. Dazu muss sowohl auf dem Client- als auch auf dem Serverrechner ein VPN-Modul (VPN-Gateway) installiert sein. Dieses VPN-Gateway linkt sich beim Zustandekommen einer Verbindung in den jeweiligen Protokollstack des Betriebssystems und führen die notwendigen Verschlüsselungs- und Authentifizierungsaufgaben durch. Ein VPN hat somit die Aufgabe, die Benutzer des Netzes zu authentifizieren, die Vertraulichkeit der übertragenen Daten zu garantieren, die erforderlichen Schlüssel zu erzeugen und diese regelmässig zu erneuern (Eckert, 2006).

VPN bedient sich dazu einer Tunneltechnik (engl. tunneling). Beim Tunneling werden die übertragenen Datenpakete durch einen zusätzlichen Header gekapselt, der die Routinginformationen des Empfängers am anderen Tunnelende enthält. Beim Empfänger werden die Datenpakete von der Firewall „empfangen“, durch das VPN-Gateway entkapselt und über das private Netz an die Zieldestination (Benutzer im Netzwerk VPN 2) weitergeleitet.

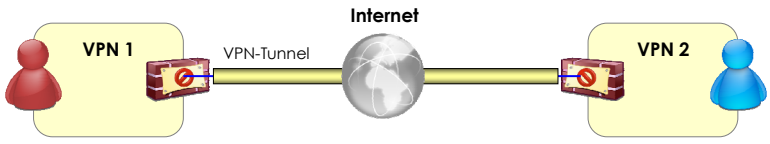

Abb. 19: Tunneling in VPNs

[51] Virtual Private Network

VPNs werden oft für die Einbindung externer Zugriffe auf ein Firmennetzwerk eingesetzt (z.B. für Telearbeitsplätze). Der Einsatz von VPNs setzt aber voraus, dass sich beide Kommunikationspartner bereits kennen und vertrauen müssen. Für die erfolgreiche Anwendung von VPNs in offenen und verteilten Systemen muss daher neben geeigneten Authentifizierungsverfahren auch die Verfügbarkeit des entsprechenden VPN-Gateways gewährleistet sein. Zudem müssen beide Kommunikationspartner über einen vorinstallierten VPN-Gateway verfügen. VPN kann sowohl mit SSL/TLS als auch mit IPSec kombiniert zum Einsatz kommen. Aufgrund der Tatsache, dass die VPN-Technologie eine sichere Verbindung in mitten eines potenziell unsicheren Netzwerks (Internet) bietet, ist sie Bestandteil vieler Sicherheitsprodukte und teilweise bereits auf Betriebssystemebene enthalten. Daraus ergibt sich aber auch gleichzeitig, dass VPN-Gateways häufig ein Ziel für Eindringversuche aus dem Internet darstellen. Dies hat zur Folge, dass für die Authentifizierung eines Users ein einfaches Verfahren wie Username und Passwort nicht ausreicht. In der Praxis werden daher meist Token- oder SmartCard-Verfahren wie sie z.B. SecurId[52] oder ActivCard[53] eingesetzt (Eckert, 2006).

2.3.3 Nachrichtensicherheit

2.3.3.1. XML-Signature

XML-Signature[54] entstand aus einer Arbeitsgruppe des W3C und der IETF und beschreibt eine digitale Signatur in XML. Eine digitale Signatur dient dazu, eine signierte Nachricht - oder ein signierter Teil einer Nachricht - eindeutig zu identifizieren und zuordnen zu können. Die XML-Signature-Spezifikation schreibt den Aufbau einer digitalen Signatur vor und gibt Empfehlungen welche Verschlüsselungsverfahren eingesetzt werden können. Mit XML-Signature können wahlweise die gesamte XML-Nachricht oder beliebige Teile einer XML-Nachricht signiert werden. Nachfolgend soll anhand eines Codebeispiels (Tab. 6) die Struktur von XML-Signature kurz erläutert werden (Beschreibung nach Hauser et al., 2004):

```
1  <Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
2    <SignedInfo>
3      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
4  20010315"/>
5      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
6      <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
7        <Transforms>
```

[52] RSA Security Inc.: http://www.rsa.com (30.06.2007)

[53] ActivIdentity Corp.: http://www.actividentity.com (30.06.2007)

[54] XML-Signature Recommendation (W3C, 2002a) und XML-Signature Standard (IETF, 2002)

```
 8          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 9        </Transforms>
10        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
11        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
12      </Reference>
13    </SignedInfo>
14    <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
15    <KeyInfo>
16      <KeyValue>
17        <DSAKeyValue>
18          <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
19        </DSAKeyValue>
20      </KeyValue>
21    </KeyInfo>
22  </Signature>
```

Tab. 6: XML-Signature Beispielcode (Beispiel aus W3C, 2002a und IETF, 2002).

- `Signature` (Zeile 1) ist das obligatorische Wurzelelement und enthält alle weiteren Elemente.
- `SignedInfo` (2) enthält Informationen über die verwendeten Signatur-Algorithmen.
- `CanonicalizationMethod` (3) ist eine Methode um die digitale XML-Signatur in eine standardisierte Form zu bringen (z.B. Elimination der Leerzeichen) in der ihr ein XML-Parser nichts mehr anhaben kann.
- `SignatureMethod` (5) beschreibt den Verschlüsselungsalgorithmus mit dem die Signatur ausgetauscht wird.
- `Reference` (6) beschreibt den Transformationsalgorithmus (8), die `DigestMethod`[55] (10) und den `DigestValue` (11) und liefert damit die Informationen, wie das Datenobjekt signiert wurde.
- `SignatureValue` (14) enthält die eigentliche Signatur in Form von Base64[56]-kodierten Binärdaten.
- `KeyInfo` (15) dient dazu, die Informationen, die zur Überprüfung der Signatur gebraucht werden zu transportieren. Dies sind unter anderem Schlüssel, Namen oder Zertifikate.

2.3.3.2. XML-Encryption

XML-Encryption[57] ist ein Standard des W3C zur Verschlüsselung von XML-Daten. Die Spezifikation beinhaltet die Mechanismen um sowohl ganze XML-Dokumente als auch

[55] Ein Digest ist die Kurzzusammenfassung der zu verschlüsselnden XML-Daten.

[56] Base64-Content-Transfer-Encoding (IETF, 1996b)

[57] XML Encryption Recommendation (W3C, 2002b)

Elemente oder Inhalte von Elementen zu verschlüsseln. Die Struktur für die Verschlüsselung ist in der Spezifikation vorgegeben und soll mit Hilfe des folgenden Codebeispiels (Tab. 7) erläutert werden (Beschreibung nach Hauser et al., 2004):

```
 1  <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#
 2  'Type='http://www.w3.org/2001/04/xmlenc#Element'/>
 3    <EncryptionMethod Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'/>
 4    <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
 5      <ds:KeyName>John Smith</ds:KeyName>
 6    </ds:KeyInfo>
 7    <CipherData>
 8      <CipherValue>DEADBEEF</CipherValue>
 9    </CipherData>
10  </EncryptedData>
```

Tab. 7: XML-Encryption Beispielcode (Beispiel aus W3C, 2002b)

- `EncryptedData` (Zeile 1) ist das Wurzelelement und beinhaltet Angaben zu Art der verschlüsselten Daten und zu deren Darstellung (Encoding).
- `EncryptionMethod` (3) enthält die Informationen zum Verschlüsselungsalgorithmus und ist optional. Wird dieses Element nicht verwendet, muss der Verschlüsselungs-algorithmus für den Empfänger erkennbar oder bekannt sein.
- `KeyInfo` (4) Element ist ein optionales Element und von XML-Signature abgeleitet (vgl. Namespace ds). Es enthält zusätzliche Angaben zum Schlüssel mit dem verschlüsselt wurde.
- `CipherData` (7) enthält die verschlüsselten Daten, die entweder als `CipherValue`-Element abgelegt werden oder als `CipherReference`-Element referenziert werden. Die Daten müssen in Form von Base64[58]-kodierten Binärdaten vorliegen.
- Mit Hilfe des `EncryptionProperties`-Elements können zusätzliche Informationen über die verschlüsselten Daten und Schlüssel ausgetauscht werden (z.B. Zeitstempel oder Seriennummer der Verschlüsselungshardware).

2.3.3.3. WS-Security

WS-Security[59] ist ein erweiterbarer Standard des Web Service Security Committee (WSS) der OASIS. Der Standard dient als Basis für die Absicherung von Web Services. WS-Security verbindet eine Vielzahl der vorgängig vorgestellten Sicherheitsmodelle wie z.B. PKI, SSL/TLS

[58] Base64-Content-Transfer-Encoding (IETF, 1996b)

[59] Web Services Security (OASIS, 2006b)

oder Kerberos[60]. Ziel ist es, die Integrität und Zuverlässigkeit von SOAP-Nachrichten garantieren zu können.

Das eigentliche Grundelement von WS-Security ist ein XML-basiertes Sicherheitsmerkmal - ein so genanntes Sicherheitstoken. Ein solches Token kann in signierter (z.B. X.509 Zertifikat, Kerberos-Ticket) oder unsignierter (z.B. Username, Passwort) Form vorliegen. Mit Hilfe von WS-Security kann beispielsweise aus der Kombination von XML-Signature (zum Signieren, vgl. Kap. 2.3.3.1), XML-Encryption (zum Verschlüsseln, vgl. Kap. 2.3.3.2) und Sicherheitstoken (UsernameToken oder BinarySecurityToken) ein vollständiges Authentifizierungssystem erstellt werden (Hauser et al., 2004). WS-Security beinhaltet im eigentlichen Sinn selber keine Sicherheitsmechanismen, es bietet vielmehr eine erweiterbare SOAP-Grundlage um verschiedene Sicherheitssysteme miteinander kommunizieren zu lassen. Der WS-Security Standard besteht neben der Kernspezifikation (OASIS, 2006b) aus den oben erwähnten Profilen für die verschiedenen Sicherheitstokens. Man unterscheidet dabei zwischen den nicht-binären Tokens, bei denen einzig das UsernameToken-Profil erwähnt wird, und den binären Tokens wie X.509 Zertifikat, Kerberos-Ticket oder SAML.

A) Nicht-binäre Sicherheits-Tokens: Username Token Profile (OASIS, 2006c) ist das am Häufigsten verwendete Verfahren für die Übergabe von Anmeldeinformationen in Form von Username und Passwort (Tab. 8, Zeile 2 und 3).

```
1  <wsse:UsernameToken wsu:Id="Example-1">
2    <wsse:Username> ... </wsse:Username>
3    <wsse:Password Type="..."> ... </wsse:Password>
4    <wsse:Nonce EncodingType="..."> ... </wsse:Nonce>
5    <wsu:Created> ... </wsu:Created>
6  </wsse:UsernameToken>
7  ...
```

Tab. 8: UsernameToken (aus OASIS 2006c)

B) Binäre Sicherheits-Tokens können sowohl X.509 Zertifikate, SAML Tokens, Kerberos Tickets oder auch andere nicht XML-basierte Sicherheitstokens beinhalten:

- **X.509 Token Profile** (OASIS, 2006d) wird benutzt um die Authentifizierung, Verschlüsselung und Signierung von Nachrichten zu gewährleisten. Das Zertifikat stellt eine Bindung zwischen dem öffentlichen Schlüssel und seinem Besitzer dar und wird in der SOAP-Nachricht mit dem Typ `"X509v3"` (Tab. 9, Zeile 4) definiert.

```
1  <wsse:Security xmlns:wsse="..." xmlns:wsu="...">
2    <wsse:BinarySecurityToken
3      wsu:Id="binarytoken"
```

[60] MIT Kerberos Consortium: http://www.kerberos.org (30.06.2007)

```
4     ValueType="…#X509v3"
5     EncodingType="…#Base64Binary">
6     MIIEZzCCA9CgAwIBAgIQEmtJZc0…
7   </wsse:BinarySecurityToken>
8   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
9     <ds:SignedInfo>…
10      <ds:Reference URI="#body">…</ds:Reference>
11      <ds:Reference URI="#binarytoken">…</ds:Reference>
12    </ds:SignedInfo>
13    <ds:SignatureValue>HFLP…</ds:SignatureValue>
14    <ds:KeyInfo>
15      <wsse:SecurityTokenReference>
16        <wsse:Reference URI="#binarytoken" />
17      </wsse:SecurityTokenReference>
18    </ds:KeyInfo>
19  </ds:Signature>
20 </wsse:Security>
21 ...
```

Tab. 9: BinarySecurityToken mit X.509 Zertifikat (aus OASIS 2006d)

- **Kerberos Token Profile** (OASIS, 2006f) dient der Authentifizierung von Tickets für das SSO von Kerberos. Das Kerberos-Ticket wird in die SOAP-Nachricht mit dem Typ `"Kerberosv5_AP_REQ"` (Tab. 10, Zeile 4) eingebunden.

```
1  <wsse:Security xmlns:wsse="...">
2    <wsse:BinarySecurityToken
3      EncodingType="…#Base64Binary"
4      ValueType="…#Kerberosv5_AP_REQ"
5      wsu:Id="MyToken">boIBxDCCAcCgAwIBBaEDA...
6    </wsse:BinarySecurityToken> ...
7  </wsse:Security>
8  ...
```

Tab. 10: BinarySecurityToken mit Kerberos Ticket (aus OASIS, 2006f)

- **SAML Token Profile** (OASIS, 2006e) dient zur Einbindung von SAML-Assertions in eine SOAP-Nachricht. Dazu muss die SAML-Assertion (Tab. 11, Zeile 2 - 21) oder ihre Referenz in das `<wsse:Security>`−Element eingefügt und mit XML-Signature signiert werden.

```
1  <wsse:Security xmlns:wsse="...">
2    <saml:Assertion xmlns:saml="..."
3      AssertionID=" a75adf55-01d7-40cc-929f-dbd8372ebdfc"
4      IssueInstant="2003-04-17T00:46:02Z"
5      Issuer="www.opensaml.org"
6      MajorVersion="1"
7      MinorVersion="1">
8      <saml:AuthenticationStatement>
9        <saml:Subject>
10         <saml:NameIdentifier
11           NameQualifier=www.example.com
12           ...
13         </saml:NameIdentifier>
14         <saml:SubjectConfirmation>
15           <saml:ConfirmationMethod>
16             urn:oasis:names:tc:SAML:1.0:cm:bearer
17           </saml:ConfirmationMethod>
18         </saml:SubjectConfirmation>
19       </saml:Subject>
20     </saml:AuthenticationStatement>
21   </saml:Assertion>
22 </wsse:Security>
23 ...
```

Tab. 11: SAML Token (aus OASIS, 2006e)

Im Umfeld von WS-Security arbeiten Microsoft, IBM, VeriSign und andere Unternehmen gemeinsam an weiteren Spezifikationen, die sich ebenfalls unter WS-Security einordnen lassen.

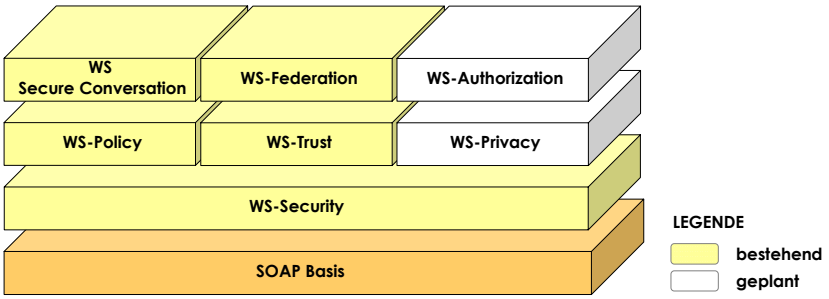

Abb. 20: WS Security Framework (nach IBM, 2002)

- **WS-Policy** (IBM et al., 2006) ist eine Spezifikation die von den Firmen BEA, IBM, Microsoft und SAP entwickelt wird und einen Rahmen für die Definition von Sicherheitsregeln und -eigenschaften darstellt. Ein Web Service kann durch WS-Policy beschreiben, welche Sicherheits-Tokens oder Entschlüsselungsalgorithmen er unterstützt. Mit WS-SecurityPolicy (IBM et al., 2005b) wird die dazu erforderliche Verbindung zwischen WS-Security und WS-Policy sichergestellt.
- **WS-Trust** (IBM et al., 2005a) definiert auf WS-Security basierende SOAP-Erweiterungen, die den Aufbau einer abgesicherten Web Service-Kommunikation innerhalb von Vertrauenszonen ermöglichen.
- **WS-Federation** (IBM et al., 2007) beschreibt Modelle für die firmenweite Verwaltung von Identitäten und greift auf die Tokens von WS-Trust, WS-Policy und das „WS-Security Profil for XML based Tokens“ zu. Das **WS-Security Profile for XML based Tokens** (IBM, 2002) definiert Richtlinien zur Einbindung von XML-basierten Sprachen in WS-Security, wie beispielsweise das SOAP-Binding von SAML.
- **WS-Secure Conversation** (IBM et al., 2005c) stellt Tokens für den sicheren Kontext (engl. context) von Nachrichten zur Verfügung. Dies dient dazu, dass beim Versand von mehreren Nachrichten der Kontext einmalig definiert und für alle nachfolgenden Nachrichten übernommen werden kann.
- **WS-Privacy** ist derzeit noch nicht realisiert, soll aber ein Modell beschreiben, wie Web Services und Anbieter ihre Datenschutz-Richtlinien während der Kommunikation bekannt geben und einhalten können. WS-Privacy wird in Zukunft das Bindeglied zwischen SOAP Message Security, WS-Policy und WS-Trust sein.

- **WS-Authorization** ist derzeit noch nicht umgesetzt. Es soll in Zukunft die Definition liefern, wie Zugriffsrechte auf Web Services zu spezifizieren und zu verwalten sind.

WS-Security kann als umfassende Spezifikation bezeichnet werden, die in Zusammenhang mit XML-Signature, XML-Encryption und SAML (vgl. Kap. 2.3.5.3) alle relevanten Bestandteile für die Sicherung von Integrität und Zuverlässigkeit zur Verfügung stellt (Hauser et al., 2004). Die Ausgangslage für die Verbreitung und Akzeptanz von WS-Security ist auch auf Grund der Erweiterbarkeit von SOAP und der flexiblen Syntax günstig.

2.3.4 AAA-Verfahren

Authentifizierung, Autorisierung und Accounting werden in der Fachliteratur oft als Triple-A Services bezeichnet. Sie bilden das eigentliche Kernstück der Sicherheitsüberlegungen auf Applikationsebene, nämlich die Definition, welches Subjekt auf welches Objekt unter welchen Bedingungen zugreifen darf. Dabei ist insbesondere auch die Aufzeichnung der Interaktion der einzelnen Subjekte von grosser Bedeutung.

2.3.4.1. Authentifizierung

Der Begriff der Authentifizierung beschreibt den Vorgang des sich Identifizierens gegenüber einem Dritten und beinhaltet die Überprüfung und den Nachweis der behaupteten Identität eines Subjekts. Durch geeignete Sicherheitsmassnahmen kann bei der Authentifizierung die Korrektheit einer behaupteten Identität kontrolliert und nachgewiesen werden. Ganz allgemein spricht man in diesem Zusammenhang auch oft von Credentials, die ein Subjekt zum Nachweis seiner Identität vorzulegen hat. Beispiele von solchen Credentials sind Tickets, die von vertrauenswürdiger Stelle ausgestellt werden und die Identität des Besitzers bestätigen. Es lassen sich grundsätzlich drei Arten der Authentifizierung unterscheiden (Eckert, 2006):

- Bei der **Authentifizierung durch Wissen** identifiziert sich ein Subjekt durch die Bekanntgabe eines Geheimnisses, das nur das Subjekt wissen kann. Beispiele für eine solche Art der Authentifizierung sind Verfahren mit Benutzernamen und Passwort, persönlichen Informationen (z.B. Email-Adresse) oder generierten Zahlencodes (PIN).
- Die **Authentifizierung durch Besitz** identifiziert ein Subjekt indem sie von ihm einen bestimmten Gegenstand erhält, der nur im Besitz des jeweiligen Subjektes sein kann. Ein solcher Gegenstand kann beispielsweise eine Smartcard (Chipkarte), ein Ausweis oder eine digitale Signatur sein.

- Die dritte Möglichkeit ist die **Authentifizierung durch ein persönliches Merkmal** des Subjektes. Unter einem solchen Merkmal versteht man physiologische oder verhaltenstypische Eigenschaften einer Person, die diese eindeutig identifizieren. Beispiele für die Authentifizierung durch ein persönliches Merkmal sind biometrische Verfahren wie Fingerabdrücke, Irisscans aber auch Verfahren zur Erkennung von verhaltenstypischen Merkmalen wie Stimme oder Handschrift.

In der Praxis werden die genannten Authentifizierungsverfahren oft kombiniert verwendet. So wird beispielsweise für E-Banking oft die Authentifizierung durch Wissen (Benutzername, Passwort und PIN) mit der Authentifizierung durch Besitz (Code aus der Streichliste) kombiniert. Der Verlust einer der beiden Credential-Informationen alleine würde demzufolge noch keinen Missbrauch zulassen.

2.3.4.2. Autorisierung

Die Autorisierung ist der Prozess der sicher stellt, dass es einem Subjekt erlaubt oder eben nicht erlaubt ist, auf eine Ressource in der gewünschten Art und Weise zuzugreifen (Matheus, 2005). Autorisierung beinhaltet demzufolge die Definition, Zuweisung und Überprüfung von Zugriffsrechten für definierte Subjekte (Rollen) auf die zu verwaltenden Ressourcen (Daten, Web Services, Funktionen). Ein Subjekt gilt als autorisiert, wenn es die Berechtigung zum Zugriff auf eine Information oder ein Datenobjekt besitzt (Eckert, 2006).

Im Verlauf der Arbeit wird in Zusammenhang mit der Autorisierung auch der Begriff des „Zugriffkontrollsystems“ erwähnt. Eine Autorisierung besteht aus der Rechtedurchsetzungs- (Exekutive) und der Zugriffsentscheidungsinstanz (Judikative). Bei der Definition der Zugriffsrechte (Legislative) von herkömmlichen Web Services können thematische, und zeitliche Bedingungen (engl. constraints) unterschieden werden. Es kann also definiert werden auf welche Ressource (z.B. WMS-Layer) wie lange zugegriffen werden kann. Bei der Autorisierung von Geo Web Services kommt zusätzlich der räumliche Aspekt zum tragen, wobei festgelegt werden kann, auf welchen Teilbereich der Ressource (z.B. Gebietsgrenze) zugegriffen werden darf.

2.3.4.3. Accounting

Das Accounting umfasst die systematische Erfassung, Überwachung und Protokollierung der beanspruchten Ressourcen. Im Bereich der Web Services ist damit insbesondere die Feststellung und Dokumentation der Dienstnutzung gemeint die mit der Bereitstellung einer Online-Zahlungsfunktionalität (engl. billing) verbunden sein kann. Der Bereich des Accountings dient

im Rahmen der Sicherheitsüberlegungen vor allem der Gewährleistung der Verbindlichkeit und Nicht-Abstreitbarkeit einer Dienstnutzung.

2.3.5 Technologien und Standards von AAA-Verfahren

Es gibt eine grosse Anzahl an verschiedenen Standards im Bereich der Triple-A Verfahren. Viele dieser Standards decken jeweils einen Teilaspekt des Sicherheitsumfeldes ab. Die nachfolgenden Verfahren und Standards wurden auf Grund ihrer Verbreitung als relevant eingestuft und detaillierter untersucht.

2.3.5.1. Single Sign-On (SSO)

Bei der Authentifizierung ist die Bekanntgabe der Zugriffsinformationen (Credentials) ein Vorgang der grundsätzlich bei jedem Zugriff wiederholt werden muss. Dies wäre aus Sicht des Benutzers störend und gleichzeitig auch ein Sicherheitsproblem. Zur Lösung dieses Problems wurden Verfahren für das Single Sign-On (SSO) entwickelt. Diese ermöglichen es dem Benutzer, nach einer einmaligen Authentifizierung über einen gewissen Zeitraum auf alle für ihn autorisierten Dienste zugreifen zu können ohne sich bei jedem Zugriff erneut authentifizieren zu müssen. Single Sign-On Verfahren bieten neben der grösseren Benutzer-freundlichkeit auch einen Sicherheitsgewinn, da der Benutzer sein Passwort während der Dauer der Interaktion nur einmal übertragen muss.

Ein zentraler Ansatz bei SSO ist der Einsatz von Tickets. Tickets werden bei einer erfolgreichen Anmeldung erzeugt und dienen ab diesem Zeitpunkt dazu, den Anwender zu authentifizieren. Ein Ticket erleichtert zwar die Interaktion, stellt aber ein potenzielles Risiko dar. Gerät ein Ticket in die Hände eines Angreifers stehen diesem Tür und Tor zu allen Diensten des SSO-Bereiches offen. Tickets sollten deshalb mit einer Gültigkeit (Zeitstempel und Gültigkeitsdauer) versehen werden. Um Veränderungen an einem Ticket zu verhindern, sollte ein Ticket zudem verschlüsselt werden. Benutzername und Passwort dürfen aber auf keinen Fall in einem solchen Ticket gespeichert werden (Rummeyer et al., 2006).

Im Bereich des Internets sind zwei Arten von SSO-Verfahren von Bedeutung. Zum einen die Verwendung einer zentralen Instanz (zentraler Sign-on-Server), welche die Anmeldung vornimmt, zum anderen der Aufbau eines Circle-of-Trust, bei der die Anmeldung am Gesamtsystem durch Anmeldung an einem beliebigen System innerhalb des Verbunds erfolgt.

- **Zentraler Sign-on-Server**: Der Benutzer kann sich auf einem zentralen Sign-on-Server einloggen und wird dort authentifiziert. Nach erfolgreicher Authentifizierung wird

server- oder clientseitig ein Cookie erstellt(vgl. Kap. 2.3.5.2), das ihn für die Nutzung der weiteren Web Services des Portals eindeutig ausweist. Ein Beispiel für einen zentralen Sign-on-Server ist Microsoft .NET Passport[61].

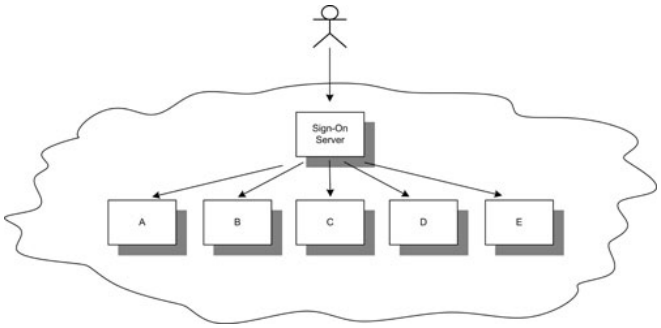

Abb. 21: Sign-on-Server (Rummeyer et al., 2006)

- **Circle-of-Trust**: Bei einem Circle-of-Trust handelt es sich um ein Netz aus vertrauenswürdigen Diensten. Ein Benutzer kann sich an einem beliebigen Dienst anmelden und erhält nach erfolgreicher Authentifizierung ein Ticket, das ihm den Zugriff auf die anderen vertrauenswürdigen Dienste des Circle-of-Trust ermöglicht. Beispiele für diese Systeme sind Kerberos oder das Liberty Alliance Project (vgl. Kap. 2.3.5.5).

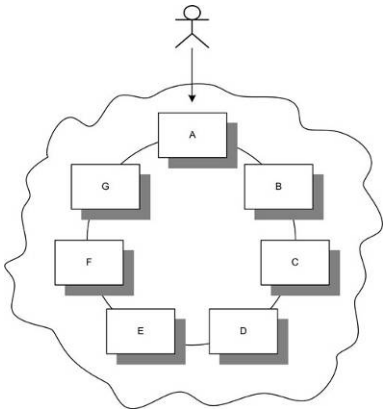

Abb. 22: Circle-of-Trust (Rummeyer et al., 2006)

2.3.5.2. Sessions / Cookies

Ein weiterer wichtiger Aspekt im Zusammenhang mit SSO-Verfahren und Authentifizierung bildet die Session-Technologie. Auf Grund der Tatsache, dass Nachrichten die über das HTTP-Protokoll versandt werden per se keinen Zustand besitzen, müssen alle Anfragen an einen Web

[61] Microsoft .NET Passport speichert die pers. Kenndaten von Besuchen einer Website (Drew, 2004)

Service grundsätzlich als eigenständige Ereignisse betrachtet werden. Dies ist aber meist nicht der Fall, da in der Regel ein Zusammenhang zwischen aufeinander folgenden Anfragen besteht.

Diesem Sachverhalt wird durch die Sessions-Technologie begegnet. Dabei wird beim ersten Zugriff eines Clients auf einen Webserver ein serverseitiges Session-Objekt mit einer eindeutigen Identifikationsnummer (Session-ID) erzeugt. Die Session-ID wird nun während der Interaktion zwischen Client und Webserver bei jeder Nachricht mitgeliefert, so dass der Webserver aufeinander folgende Anfragen vom gleichen Client als solche erkennen kann. Dies ermöglicht es einerseits dem Webserver die Interaktion mit dem Client aufzuzeichnen (Session Tracking, Accounting) und erspart es andererseits dem Client seine Credentials (z.B. Benutzername und Passwort) bei jedem Zugriff auf den Webserver erneut bekannt geben zu müssen.

Die Realisierung von Session-Verfahren wird oft mit Hilfe von Cookies realisiert. Cookies sind vom Server generierte Datenstrukturen, in die der Server Informationen über den zugreifenden Benutzer codiert. Diese Informationen enthalten neben Namen, Wert, Zugriffbeschränkungen und Gültigkeitsdauer[62] des Cookies, auch Angaben über die ausstellende Serverdomäne. In der Regel werden Cookies auf dem Rechner des zugreifenden Clients abgespeichert, was aber je nach Sicherheitsrichtlinie der Client-Domäne oder des Browsers unterbunden sein kann. Da auch hier ein Angreifer die Informationen des Cookies abfangen kann, sollten Cookies über sichere Transportverbindungen (siehe Kap. 2.3.2) ausgetauscht werden (Eckert, 2006).

2.3.5.3. SAML

SAML[63] ist ein Standard der OASIS zum domänenübergreifenden Austausch von Authentifizierungs- und Autorisierungsinformationen. Die Spezifikation von SAML besteht aus einer Reihe von Dokumenten und einer grossen Anzahl an Anwendungsbeispielen in Form von XML-Schemata für unter anderem X509, PGP[64] oder Kerberos (OASIS, 2005b). Im Zentrum von SAML steht das Single Sign-On Verfahren, bei dem ein Identity Provider und ein Service Provider Daten auf der Basis von SOAP über HTTP austauschen. Um diesen Austausch zu ermöglichen bietet SAML vier Kernkomponenten, die in Abbildung (Abb. 23) ersichtlich sind (OASIS, 2006a).

---

[62] Cookies können je nach Anforderung des Servers permanent, auf einen Zeitraum begrenzt oder während der Dauer der Session bestehen bleiben.

[63] Security Assertion Markup Language Standard (OASIS, 2005b)

[64] Petty Good Privacy: http://www.pgp.com (30.06.2007)

- SAML Assertions (OASIS, 2005c) enthalten Angaben über die zum Subjekt gehörenden Aussagen (Statements) wie Authentifizierung, Attribute und Berechtigungsinformationen.
- SAML Protocols (OASIS, 2005c) definieren den Austausch von SAML Assertions zwischen Identity Provider und Service Provider.
- SAML Bindings (OASIS, 2005d) beschreiben die Übersetzungen des SAML Protokolls auf die Standard Nachrichten- und Kommunikationsprotokolle wie SOAP oder HTTP
- SAML Profiles (OASIS, 2005e) legen fest, wie die SAML Assertions und Responses in bestehende Protokolle (z.B. Enhanced Client or Proxy (ECP) Profile, Single Logout Profile oder Web Browser SSO Profile) zu integrieren sind.

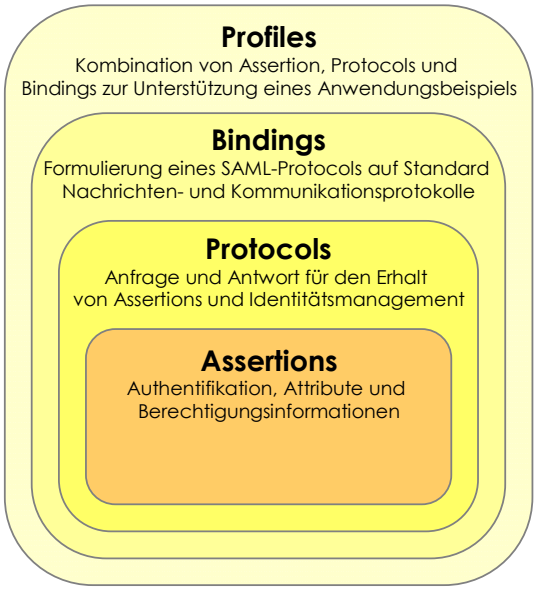

Abb. 23: SAML Konzept (nach OASIS, 2006a)

Neben den oben erwähnten Komponenten umfasst der SAML-Standard auch noch weitere ergänzende Dokumente:

- SAML Glossary (OASIS, 2005f) gibt eine Einführung in die Begriffe und Befehle des SAML-Umfelds
- Authentication Context (OASIS, 2005g) definiert die Syntax für die Definition von Deklarationen und Klassen.
- Security and Privacy Considerations (OASIS, 2005h) bietet einen Überblick über die möglichen Sicherheitsrisiken bei der Verwendung von SAML und definiert mögliche Gegenmassnahmen

- SAML Conformance (OASIS, 2005i) legt die Anforderungen an die Implementierung von SAML fest, damit die Interoperabilität mit SAML gewährleistet werden kann.
- SAML Metadata (OASIS, 2005k) enthält eine standardisierte Beschreibung der Systemeinheiten von SAML-Profilen wie z.B. Identifikatoren, Verbindungstypen, Zertifikate und Schlüssel.

Zum besseren Verständnis der Interaktion zwischen den vorgestellten Standards SOAP, SAML, WS-Security und XML-Signature, illustriert die nachfolgende Grafik exemplarisch den Aufbau einer SOAP-Nachricht und das Zusammenwirken dieser Komponenten.

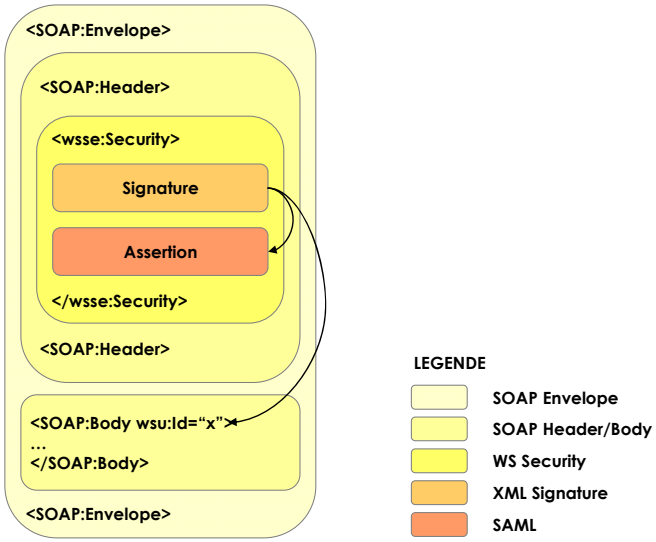

Abb. 24: Nachrichtensicherheit - Zusammenspiel der Standards (nach Hauser et al., 2004)

Nachfolgend ein Codebeispiel einer möglichen SAML-Response die stets auch die angefragte Assertion (Zeile 9-27) enthält. Dem Beispiel zu Folge wurde die Nachricht am 30. Juli 2007 um 23:15 Uhr (3) erstellt und enthält eine Assertion die zwischen 23:30 (15) und 23:59 (16) gültig ist. Die Assertion wurde von „UNIGIS Salzburg“ (11) um 23:10 (12) ausgestellt und bestätigt, dass sich „Rolf Mühlemann“ (24) aus der Domäne „www.unigis.ac.at“ (23) mit seinem Passwort (20) erfolgreich (7) angemeldet hat.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2    <samlp:Response ResponseID="111222333"
3      IssueInstant="2007-06-30T23:15:00Z"
4      InResponseTo="111222333"
5      MajorVersion="2" MinorVersion="0">
6      <samlp: Status>
7        <samlp:StatusCodeValue="samlp:Success"/>
8      </samlp:Status>
9      <saml:Assertion AssertionID="998877"
10       MajorVersion="2" MinorVersion="0"
11       Issuer="UNIGIS Salzburg"
12       IssueInstant="2007-06-30T23:10:00Z"
13       xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
14        <saml:Conditions
15          NotBefore="2007-06-30T23:30:00Z"
16          NotOnOrAfter="2007-07-01T23:59:59Z">
17        </saml:Conditions>
18        <saml:AuthenticationStatement
19          AuthenticationInstant="2007-06-30T23:30:01Z"
20          AuthenticationMethod="urn:oasis:names:tc:SAML:Password">
21          <saml:Subject>
22            <saml:NameIdentifier
23              SecurityDomain=www.unigis.ac.at
24              Name="Rolf Mühlemann">
25          </saml:Subject>
26        </saml:AuthenticationStatement>
27      </saml:Assertion>
28    </samlp: Response>
```

Tab. 12: Beispiel einer SAML Response mit Assertion

SAML bietet für die HTTP-Übertragung und den Austausch der Assertions zwischen Identity Provider und Service Provider zwei mögliche Profile (OASIS, 2005d):

- **POST-Profil**: Nach der Authentifizierung des Clients beim Identity Provider wird beim Identity Provider ein Assertion-Objekt erzeugt. Dieses Assertion-Objekt wird vom Identity Provider an den Client übermittelt, damit sich dieser bei der Anfrage an den Service Provider authentifizieren kann. Der Service Provider kann durch die mitgelieferte Assertion den authentifizierten Client für die gewünschte Servicenutzung autorisieren.

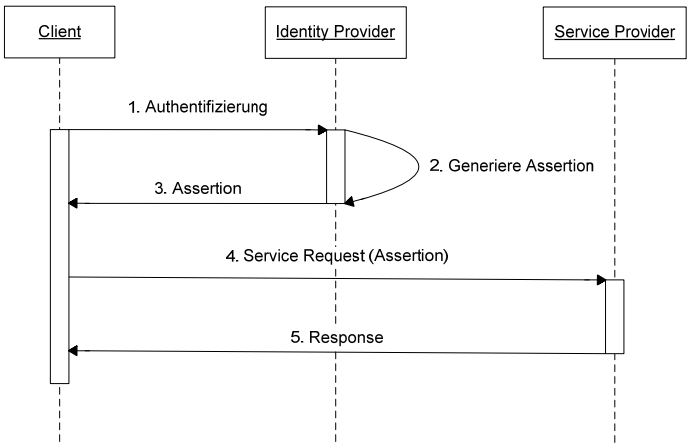

Abb. 25: SAML-Authentifizierung mittels POST-Profil (nach Hey, 2005)

- **Artefact-Profil**: Im Gegensatz zum POST-Profil wird beim Artefact-Profil nur eine Referenz auf das erzeugte Assertion-Objekt (SAML-Artefact) an den Client zurückgegeben. Der Client sendet diesen SAML-Artefact bei der Service-Anfrage an den Service Provider. Der Service Provider kann die im SAML-Artefact enthaltene eindeutige Quelleninformation (SourceID-Element) auflösen und erhält damit die Angabe über den ausstellenden Identity Provider. Stimmt der Eintrag in der Tabelle der vertrauenswürdigen SourceID-Referenzen des Service Providers mit den Angaben aus dem Artefact überein, kann der Service Provider die Authentifizierungsinformationen

beim Identity Provider einsehen und somit den authentifizierten Client für die gewünschte Servicenutzung autorisieren.

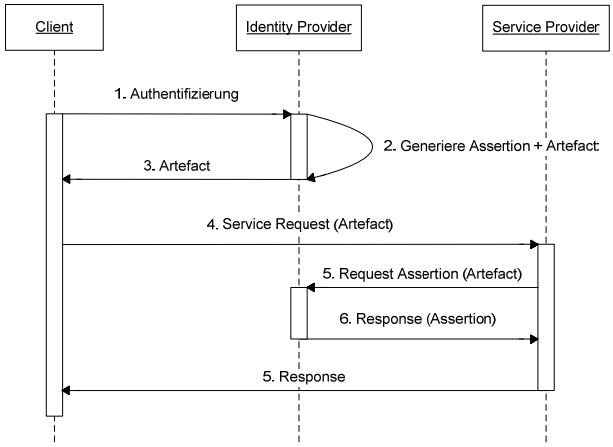

Abb. 26: SAML-Authentifizierung mittels Artefact-Profil (nach Hey, 2005)

2.3.5.4. XACML

XACML[65] ist ein Standard der OASIS der dazu dient, erweiterbare, XML-basierte Sicherheitsregeln und -richtlinien zu beschreiben. Das Kernelement von XACML ist eine Regel (engl. rule), die aus drei Elementen besteht:

- einem Ziel (engl. target),
- einem Effekt (engl. effect) und
- einer Sammlung von Bedingungen (engl. conditions).

Eine Entscheidungsanfrage (engl. decision request) enthält demzufolge die Informationen, auf welches Element man zugreifen möchte, wie man auf das Element zugreifen möchte und unter welchen Bedingungen der Zugriff gewährt werden soll. Neben den Regeln können in XACML auch Regelsammlungen (engl. policies) definiert werden. Diese Policies können dann wieder zu so genannten `PolicySet`-Elementen zusammengefasst werden, wodurch komplexe Regelwerke entstehen können.

Das nachfolgende Codebeispiel enthält mit dem Subjekt (Zeile 3-10), der Ressource (11-26) und den Umgebungsregeln (27-31) die wesentlichen Bestandteile einer XACML-Anfrage. Im Beispiel möchte das Subjekt „Rolf Mühlemann“ (4-6) in der Rolle eines Studenten agierend (7-

[65] Extended Access Control Markup Language (OASIS, 2005a)

9), den Zugriff auf die Ressource FeatureCollection (13-15) eines WFS Services (17-25) beanspruchen und die Operation GetFeature (28-30) ausführen.

```
1  <?xml version="1.0" encoding="ISO-8859-1"?>
2  <Request>
3    <Subject>
4      <Attribute AttributeId="subject-id" DataType="rfc822Name">
5        <AttributeValue>Rolf Muehlemann </AttributeValue>
6      </Attribute>
7      <Attribute AttributeId="role-id" DataType="string">
8        <AttributeValue>Student</AttributeValue>
9      </Attribute>
10   </Subject>
11   <Resource>
12     <ResourceContent>
13       <wfs:FeatureCollection ...>
14         ...
15       </wfs:FeatureCollection>
16     </ResourceContent>
17     <Attribute AttributeId="resource-id" DataType="string">
18       <AttributeValue>/Request/Resource/ResourceContent/</AttributeValue>
19     </Attribute>
20     <Attribute AttributeId="scope" DataType="string">
21       <AttributeValue>Descendants</AttributeValue>
22     </Attribute>
23       <Attribute AttributeId="ServiceName_and_PortId" DataType="string">
24       <AttributeValue>WebFeatureService:port7071</AttributeValue>
25     </Attribute>
26   </Resource>
27   <Action>
28     <Attribute AttributeId="operationId" DataType="string">
29       <AttributeValue>GetFeature</AttributeValue>
30     </Attribute>
31   </Action>
32 </Request>
```

Tab. 13: Beispiel einer XACML-Anfrage

Der Ablauf einer Abfrage innerhalb eines XACML-Zugriffskontrollsystems soll mit Hilfe der untenstehenden Grafik (Abb. 27) und den nachfolgenden Beschreibungen illustriert werden:

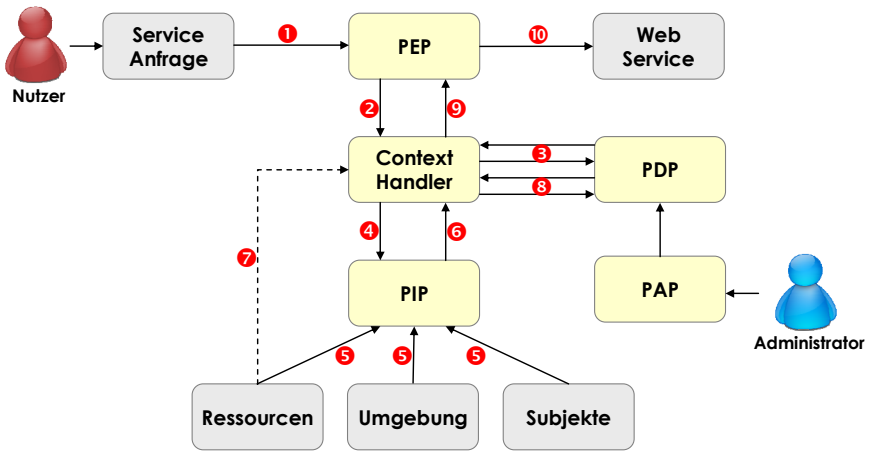

Abb. 27: Ablauf einer XACML-Zugriffsanfrage (nach OASIS, 2005a)

1. Der Nutzer sendet eine Zugriffsanfrage an den PEP (Policy Enforcement Point).
2. Der PEP leitet die Zugriffsanfrage in nativer Form an den Context Handler weiter.

3. Der Context Handler erstellt eine XACML-Kontextanfrage und sendet diese an den PDP (Policy Decision Point). Der PDP ermittelt im PAP (Policy Administration Point) die zur Beantwortung der Zugriffsanfrage erforderlichen Subjekt-, Ressource-, Aktions- und Umgebungsattribute und verlangt diese vom Context Handler.
4. Der Context Handler leitet diese Anfrage an den PIP (Policy Information Point) weiter.
5. Der PIP ermittelt die benötigten Subjekt-, Ressource- und Umgebungsregeln.
6. Der PIP sendet die verlangten Attribute an den Context Handler zurück.
7. Der Context Handler kann weitere Ressourceinformationen in den Kontext integrieren.
8. Der Context Handler sendet die Attribute an den PDP zurück. Dieser wertet die Zugriffsregeln (engl. policies) aus und sendet den Antwortkontext inklusive der jeweiligen Autorisierungsentscheidung (engl. authorization decision) an den Context Handler zurück.
9. Der Context Handler übersetzt den Antwortkontext ins native Format des PEP und sendet die Antwort an den PEP.
10. Der PEP führt die Anfrage an den Web Service durch und liefert dem Nutzer eine der folgenden Antworten zurück:
    - Der Zugriff wird erlaubt (engl. permit).
    - Der Zugriff wird verboten (engl. deny).
    - Die Anfrage ist nicht anwendbar (engl. not applicable) weil keine entsprechende Regel definiert ist.
    - Die Anfrage ist nicht auswertbar oder unbestimmt (engl. indeterminate) wenn ein Fehler bei der Anwendung des Regelwerkes aufgetreten ist.

Zusammenfassend lässt sich festhalten, dass XACML ein leistungsstarker und offener Standard für die Verwaltung und Durchsetzung von Zugriffsrechten auf XML-Daten ist. Sun Microsystems bietet schon seit geraumer Zeit eine als Open Source deklarierte Implementierung von XACML[66]. Der Einsatz von XACML ist aber eng an SAML gekoppelt. Die Verbreitung von XACML ist mitunter auch davon anhängig wie sich dieser Standard gegenüber dem von Microsoft propagierten XrML[67] durchsetzt. (Hauser et al., 2004).

[66] XACML Implementation von Sun Microsystems, Inc.: http://sunxacml.sourceforge.net (30.06.2007)

[67] eXtensible rights Markup Language: http://www.xrml.org (30.06.2007)

2.3.5.5. Liberty Alliance

Unter dem Namen Liberty Alliance Project[68] gründeten namhafte Firmen (unter ihnen Sun, Nokia, VeriSign u.v.m.) im Jahre 2001 eine Initiative zur Schaffung eines industrieweiten Single-Sign-On-Standards[69] für den Aufbau und die Verwaltung von sicheren Web Services und SOAs. Die Spezifikation beschreibt, basierend auf den Standardprotokollen und -diensten im Bereich der Web Services (HTTP, SSL, SOAP und SAML), eine offene und einheitliche Infrastruktur für die Authentifizierung von Nutzern.

Der Fokus von Liberty Alliance liegt im Business-to-Customer-Bereich, wobei die personenbezogenen Daten des Benutzers dezentral gehalten und verwaltet werden sollen. Aufbauend auf dem Konzept des Circle-of-Trust, einer Menge aus Service- und Identitätsbetreibern die untereinander vernetzt sind, werden Geschäftsbeziehungen und Übereinkünfte auf der Liberty Alliance Architektur etabliert. Das persönliche Profil des Benutzers (engl. federated identity), das die verwendete Dienstnutzung, das Einkaufsverhalten und die Zugriffshistorie dokumentiert, kann vom Benutzer selber konfiguriert und verwaltet werden. Es liegt somit im Ermessen des Benutzers, welche persönlichen Informationen er bekannt geben möchte, bei welchen Web Services er diese bekannt geben möchte und welche Web Services, bei denen er eine Kennung besitzt, miteinander verknüpft werden dürfen. Dies ermöglicht es dem Benutzer, nach erfolgreicher Authentifizierung beim Identitäts-Provider, alle an der Föderation (engl. federation) beteiligten Web Services zu nutzen ohne sich erneut anmelden zu müssen. Die Credentials für die Nutzung der Web Services werden im Hintergrund zwischen den an der Föderation beteiligten Web Services weitergereicht. Es handelt sich also um ein SSO-Verfahren in einem vom Benutzer definierten Teilnehmerkreis von Web Services. Gleichzeitig kann wiederum über den Identitäts-Provider ein automatisches Ausloggen des Benutzers (Single Logout) bei allen an der Föderation beteiligten Web Services durchgeführt werden (Eckert, 2006).

[68] Liberty Alliance Project: http://www.projectliberty.org (30.06.2007)

[69] Liberty Alliance Specification (Liberty, 2006)

2.4 Sicherheit im GDI-Umfeld

2.4.1 WAS

Der WAS[70] dient, wie es der Name vermuten lässt, zur Authentifizierung d.h. zur Sicherstellung der Identität eines Benutzers. Der Benutzer kann vor der Nutzung eines Geo Web Services seine Identität gegenüber dem WAS bekannt geben. Der WAS stellt nach erfolgreicher Authentifizierung ein digital signiertes Zertifikat aus, das der Benutzer für die weiteren Zugriffe innerhalb der GDI verwenden kann. Beim Serviceaufruf kann der Benutzer das erhaltene WAS-Zertifikat zusammen mit der regulären OWS-Anfrage dem zugriffsgeschützten Geo Web Service präsentieren. Dieser erhält dadurch die Bestätigung der Identität des Benutzers und muss sich nicht mehr selber um dessen Authentifizierung kümmern.

Dies setzt voraus, dass sich WAS und Web Services kennen und vertrauen. Die Sicherheit des Authentifizierungsvorgangs bei WAS wird durch folgende Massnahmen bewerkstelligt (Drewnak et al., 2005):

- Der Einsatz einer **abgesicherten Verbindung** (wie SSL/TLS) hilft die Entwendung des Zertifikats bei der Übermittlung zu verhindern.
- Die **Signierung des Zertifikats** schützt vor Fälschung oder Falscheinspielung.
- Eine zeitlich begrenzte **Gültigkeitsdauer des Zertifikats** (z.B. auf wenige Minuten) schützt vor dessen Falscheinspielung oder Entwendung.

2.4.2 WSS

Der WSS[71] definiert die Zugriffskontrolle für Geo Web Services, indem er als Sicherheits-Proxy einem zugriffsbeschränkten Geo Web Service vorgeschaltet ist. Dem WSS kommt dabei die Aufgabe zu, die ankommenden Anfragen zu prüfen und autorisierte Anfragen an den OGC Service (z.B. WFS) weiterzuleiten. Für die erfolgreiche Autorisierung einer Anfrage braucht der WSS ein, von einem WAS ausgestelltes Zertifikat, das den Anfrager eindeutig identifiziert. Um den Anforderungen hinsichtlich Interoperabilität gerecht zur werden und auf Grund der Tatsache, dass innerhalb einer GDI auch mehrere WAS-Instanzen Zertifikate ausstellen können,

[70] Web Authentication Service (Drewnak et al., 2005)

[71] Web Security Service (Drewnak et al., 2005)

gibt ein WSS mittels seiner Capabilities bekannt, welche WAS-Instanzen durch ihn akzeptiert werden und welche Authentifizierungsmethoden verwendet werden können. Der Client hat dadurch die Möglichkeit, auf das Angebot des WSS zu reagieren und dem Benutzer die erforderlichen Textfelder anzubieten, die er zur Eingabe der entsprechenden WAS-Authentifizierungsmerkmale benötigt.

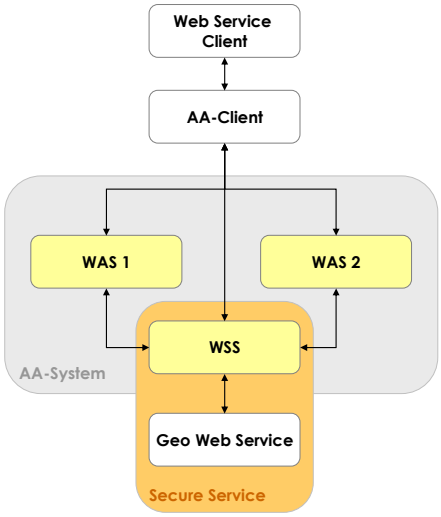

Abb. 28: Zusammenspiel von WAS und WSS (nach Drewnak, 2003)

Die Spezifikation von WSS beinhaltet die Basisfunktionalität der Zugriffskontrolle für Geo Web Services. Im Rahmen von WSS kann die Autorisierungsentscheidung nur grundsätzlich gefällt werden, nämlich ob eine Anfrage an den Service weitergeleitet werden darf oder nicht. Die Anforderung einer feingranularen Zugriffsentscheidung, d.h. welche Funktionen, Features oder Layers ein Benutzer verwenden darf, ist noch nicht umgesetzt.

2.4.3 GeoXACML

GeoXACML[72] basiert auf dem XACML-Standard von OASIS (vgl. Kap. 2.3.5.3) und erweitert diesen um geodaten-spezifische Zugriffsrechte. Zusätzlich zu den nichträumlichen Zugriffsregeln bietet GeoXACML damit auch Zugriffsregeln um Geodatenobjekte (Features) hinsichtlich ihrer räumlichen Lage und Ausdehnung eingrenzen zu können (Matheus, 2005). Damit können mit GeoXACML die folgenden Zugriffsbeschränkungen einzeln oder in Kombination definiert und durchgesetzt werden (vgl. Abb. 29).

[72] Geo eXtensible Access Control Markup Language, OGC Discussion Paper (OGC, 2005e)

- Beschränkung nach Feature-Typ (engl. feature type restriction): Art des Geoobjektes z.B. Zugriff auf Objekte vom Typ “Gebäude”.
- Beschränkung nach Feature (engl. feature instance restriction): Individuelles Attribut oder Eigenschaft eines Geoobjekts z.B. Zugriff auf Objekte mit der Bezeichnung “Bundeshaus”.
- Raumbezogene Beschränkung (engl. spatial restriction): Räumliche Lage und Ausdehnung eines Geoobjekts z.B. Zugriff auf die Objekte im Bereich der Schweiz

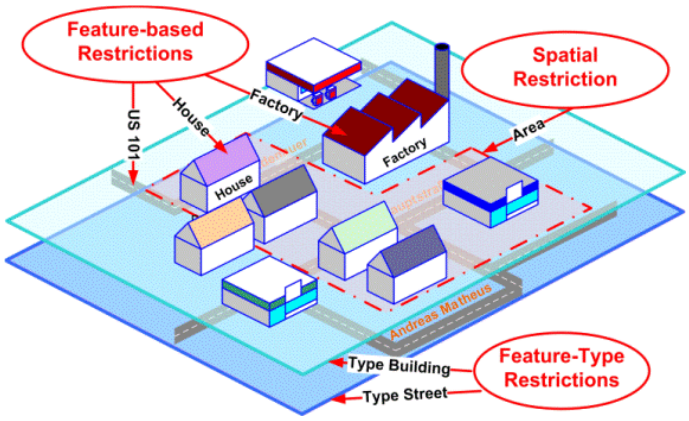

Abb. 29: Zugriffseinschränkungen mit GeoXACML (AM Consult, 2005)

Die Deklaration der Zugriffsbeschränkung mit GeoXACML ist so konzipiert, dass bestehende Geo Web Services (z.B. WMS, WFS) nicht modifiziert werden müssen. Der schematische Aufbau einer GeoXACML Service Infrastruktur zeigt die nachfolgende Grafik (Abb. 30).

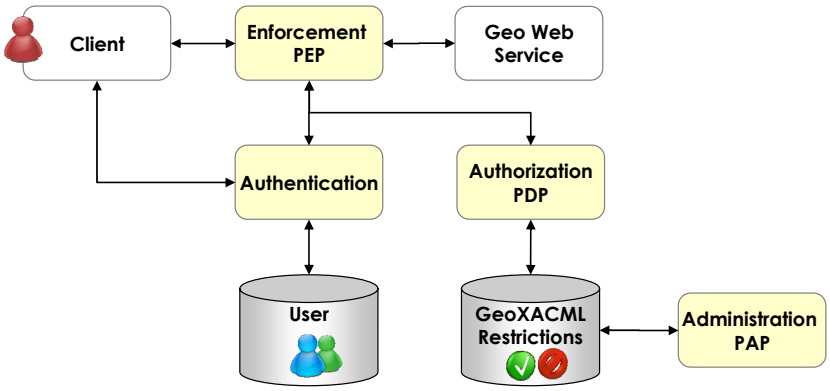

Abb. 30: GeoXACML Service Infrastruktur (nach AM Consult, 2005)

Die Authentifizierung des Clients wird von einem SAML-basierten Service bewerkstelligt und ermöglicht ein SSO. Der Zugriff des Clients auf den Geo Web Service (mit entsprechendem SAML-Ticket) wird über den Policy Enforcement Point (PEP) geleitet. Der PEP ist dem Geo Web Service „vorgeschaltet“ und übernimmt das Management der Service-Anfrage. Er klärt in

einem ersten Schritt die Authentifizierung des Clients ab. In einem zweiten Schritt leitet er die Anfrage an den Policy Decision Point (PDP) weiter, der dann gemäss den definierten Zugriffsregeln (GeoXACML-Restrictions) entscheidet, ob und in welchem Ausmass die Anfrage von Geo Web Service beantwortet werden soll. Der PDP entscheidet, welcher User, respektive welche Rolle auf welche Ressource in welchem geografischen Gebiet zugreifen darf. Die Administration dieser Zugriffsrechte geschieht über den Policy Administration Point (PAP). Mit der Information aus dem Rechte-Repository kann der PEP in einem dritten Schritt die Anfrage an den Geo Web Service weiterleiten und dem Client die entsprechenden Geodaten aushändigen.

2.4.4 GeoDRM

Eine weitere Möglichkeit den Zugriff auf Geodaten sicher zu stellen, bieten die Konzepte des Digital Rights Management (DRM) und dessen Erweiterung für geo-räumliche Daten GeoDRM. Mittels DRM werden die Dateninhalte (z.B. Musik, Texte oder Bilder) vor der Auslieferung verschlüsselt und damit vor unberechtigtem Zugriff geschützt. Der Empfänger der Daten kann beim Anbieter eine Nutzungslizenz beantragen und erhält damit den entsprechenden Schlüssel zur Entschlüsselung der Daten. Eine sichere Datenverschlüsselung vorausgesetzt, kann damit die Zugriffskontrolle über die Vergabe der Nutzungslizenzen geregelt werden. Die Art und Weise der Zugriffsbeschränkung liegt dabei vollständig beim Eigentümer der Daten, unabhängig von den vertraglichen Abmachungen mit den Beteiligten. DRM kann damit sowohl für frei zugängliche als auch für kommerziell genutzte Daten angewendet werden.

GeoDRM[73] ist eine OGC Abstract Specification. Es soll sicher stellen, dass standard-basierte Industrielösungen des Digital Rights Managements (DRM) mit den OGC Web Services kompatibel sind. GeoDRM definiert ein Framework für die zukünftige GeoDRM Implementation Standards der verschiedenen Geo Web Services und widmet sich folgenden Aspekten (OGC, 2006c):

- Das Rechtemodell für räumliche Geodaten berücksichtigt die unterschiedlichsten Arten von Geschäftsbeziehungen und beschreibt die entsprechenden Rollen und Verantwortlichkeiten. GeoDRM bietet die Möglichkeit der direkten Lizenzierung als auch der Lizenzierung über eine dritte Partei (Sub-Licensing) für die Geschäfts-

[73] Geo Digital Rights Management, OGC Abstract Specification (OGC, 2006c)

beziehungen zwischen Anbietern (B2B) und zwischen Anbietern und Endkunden (B2C).

- Die Lizenzierung unterstützt verschiedenste Arten von digitalen Geodaten die von unterschiedlichen Ressourcen stammen können. Diese Ressourcen können statische Offline-Produkte (z.B. DVD mit Navigationsdaten) oder auch dynamische Online-Angebote (z.B. Geo Web Services) darstellen. Das Rechtemodell von GeoDRM stellt Funktionalität bereit, um die Rechte der unterschiedlichen Ressourcen anhand von Einschränkungen spezifischer Parameter (Wertebereiche) durchzusetzen.

Dementsprechend definiert GeoDRM wie die Rechte bei der Lizenzierung von Geoinformationen auf Grund der geometrischen Ausprägung deklariert und durchgesetzt werden können. Der tatsächliche Nutzen von GeoDRM ist aber mitunter stark von der Akzeptanz der Anwender abhängig. Vergleiche mit der Handhabung von digitalen Rechten in anderen Bereichen (z.B. Musikindustrie) zeigen, dass die Einführung eines strikten DRM auch für legale Anwendungen eine teilweise grosse Einschränkung darstellen kann. Dies ergibt sich aus der Tatsache, dass die Nutzung von digitalen Daten und Diensten vom Service Anbieter nicht a priori vorausgesehen werden kann. Im Weiteren gilt es auch zu beachten dass mit der Einführung von DRM die Aspekte der Interoperabilität und Performance nicht beeinträchtigt werden dürfen.

2.4.5 WPOS / XCPF

Die Spezifikation des WPOS[74] und des XCPF[75] wurde vom Fraunhofer Institut[76] und der GDI NRW[77] entwickelt und legt die Basis für die Standardprozesse im eBusiness-Bereich einer GDI. Diese Prozesse widmen sich den Aufgaben Preiskalkulation, Onlinebestellung und Auslieferung und stellen Verfahren zur Verfügung, um auf Basis der Dienstnutzung (Accounting) die entsprechenden Leistungen in Rechnung zu stellen. Die Definition WPOS/XCPF wurde aus Gründen der Vollständigkeit an dieser Stelle erwähnt. Auf eine detaillierte Betrachtung der Verfahren zur Bestellung und Bezahlung von Web Services kann, wie bereits im Kapitel Abgrenzung (Kap. 1.6) erwähnt, im Rahmen dieser Arbeit nicht eingegangen werden.

[74] Web Pricing & Ordering Service, OGC Discussion Paper (OGC, 2002)

[75] XML Configuration & Pricing Format (OGC, 2002)

[76] Fraunhofer-Gesellschaft: www.fraunhofer.de (30.06.2007)

[77] Geodaten Infrastruktur Nordrhein-Westfalen: www.gdi-nrw.org (30.06.2007)

2.5 Aktuelle GDI-Initiativen

2.5.1 deegree

Die deegree-Initiative[78] ist aus einer Forschungsinitiative der Universität Bonn entstanden und bietet eine Open Source[79]-GDI-Lösung auf Basis von bestehenden ISO und OGC Standards. Treibenden Kräfte hinter deegree sind die Universität Bonn und die aus der Universität Bonn entstandene spin-off Firma lat/lon GmbH[80]. Sie entwickeln gemeinsam an einer Palette von GDI-Bausteinen. Serverseitig bestehen diese Bausteine aus der Umsetzung und Implementierung von OGC Web Services und den dazugehörigen Sicherheitskomponenten. Clientseitig werden die entsprechenden desktop- oder browserbasierenden Clients zur Verfügung gestellt.

Die Sicherheitskomponenten von deegree werden in der „iGeoSecurity"-Lösung zusammengefasst. Die Idee von „iGeoSecurity" besteht darin, dem zu schützenden OGC Web Service (OWS) einen Proxy vorzuschalten der als „Stellvertreter" fungiert. Dieser so genannte „owsProxy" unterstützt die gleiche Schnittstelle wie der standardisierte OWS, bietet aber zusätzliche Funktionalität durch die Bereitstellung von Sichten auf die jeweiligen OWS. Der Zugriff auf diese Sichten wird durch den „owsProxy" geschützt und kann serverseitig so eingeschränkt werden, dass nur ein speziell ausgerüsteter Client mit den entsprechenden Zugriffsrechten auf die geschützten Daten zugreifen darf. Die Interoperabilität des OWS bleibt gewährleistet, da der Zugriff auf die frei zugänglichen Daten mit einem Standard-Client weiterhin funktioniert (lat/lon, 2007).

„deegree iGeoSecurity" besteht aus folgenden Modulen (lat/lon, 2007):

- Der „deegree owsProxy" unterstützt die gleiche Schnittstelle wie der OWS und bietet zusätzliche Funktionalität durch die Bereitstellung von Sichten auf die jeweiligen OWS.
- Die Konfiguration der Sichten erfolgt in einem Policies-Repository. Das Policies-Repository umfasst XML-Dateien zur globalen Steuerung des Verhaltens des „owsProxy".

[78] deegree: http://www.deegree.org (30.06.2007) und (deegree, 2007)

[79] Freie Software geschützt durch GNU Lesser General Public License: http://www.fsf.org (30.06.2007)

[80] lat/lon Gesellschaft für raumbezogene Informationssysteme mbH: http://www.lat-lon.de (30.06.2007)

- Das Rechte, Rollen und Ressourcen Modul (U3R) bildet die Benutzerrechte an den zur Verfügung stehenden Ressourcen ab und weist diese den Nutzern oder Nutzergruppen zu. Die Verwaltung wird mit einer Web-Oberfläche durchgeführt und die Daten in einer Datenbankinstanz (PostgreSQL, Oracle, MS Access) gespeichert.
- Mit dem deegree Web Authentication Service (WAS) werden die Benutzer authentifiziert und Tickets für den Zugriff auf den gewünschten OWS ausgestellt (vgl. Kap. 2.4.1).
- Der deegree Web Security Service (WSS) leitet die Anfragen mit gültigen Tickets an die von ihm abgesicherten Dienste weiter. Der Funktionsumfang des deegree WSS basiert auf dem vorgängig vorgestellten WSS (vgl. Kap 2.4.2) und erweitert diesen um die Funktionalität des WAS. So kann der deegree WSS als Kombination von WAS/WSS betrieben werden und gleichzeitig auch die Anfragen eines WAS verarbeiten.
- Clientseitig wird der Zugriff auf die geschützten Dienste mittels Web Authentication Client (WAC) oder iGeoPortal gewährleistet.

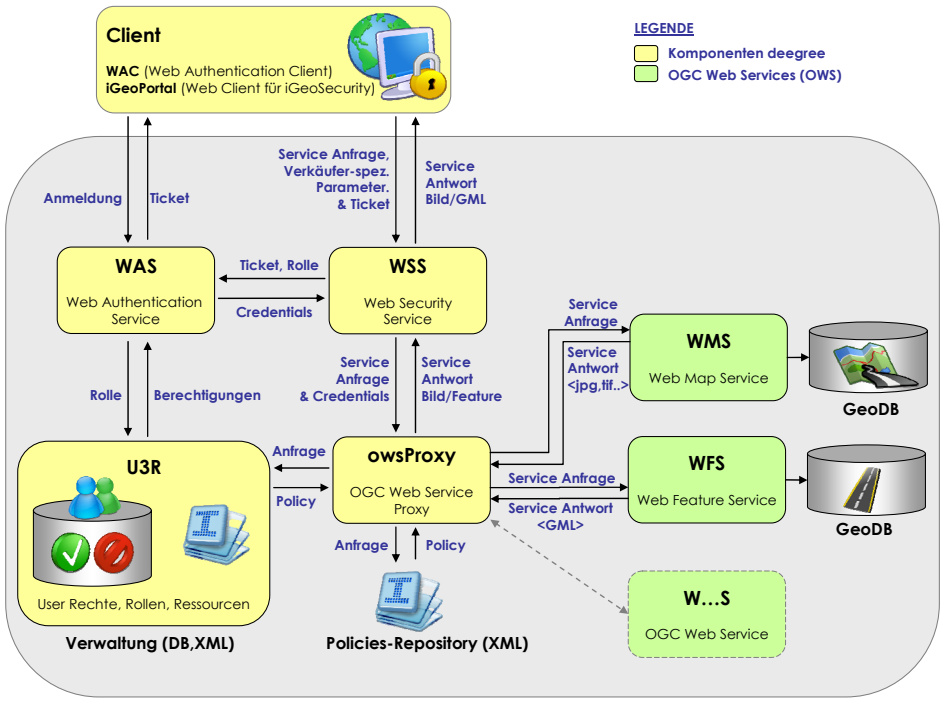

Abb. 31: Aufbau, Interaktion und Kommunikation von deegree

2.5.2 52°North

Die Initiative 52°North wurde vom Institut für Geoinformatik der Universität Münster[81] und der Firma con terra GmbH[82] gegründet und hat sich die Entwicklung innovativer, frei verfügbarer und Open Source-basierter GDI-Software zum Ziel gesetzt. Seit der Gründung im Jahre 2004 sind mit ITC[83] und ESRI[84] zwei weitere namhafte Partner hinzugekommen.

Ein wesentlicher Teilbereich von 52°North widmet sich dem Thema Websicherheit. In diesem Zusammenhang wurden der Web Authentication Service (WAS; vgl. Kap. 2.4.1) der Web Security Service (WSS; vgl. Kap. 2.4.2) und der Web Security Client (WSC) spezifiziert und entwickelt. Die Architektur der Rechteverwaltung und -auswertung von 52°North lehnt sich stark an das Modell von XACML respektive GeoXACML an. Die wichtigsten Module sind nachfolgend aufgeführt:

- Der WSC[85] erweitert einen „herkömmlichen" OGC Web Service Client um die Funktionalität mit dem WAS und WSS kommunizieren zu können.
- Die Authentifizierung mittels WAS erfolgt über SAML und kann verschiedene Authentifizierungsmethoden unterstützen - die aktuelle Version von 52°North unterstützt die User/Passwort-Methode. Die erhaltenen Credentials werden der Service-Anfrage an den WSS/PEP hinzugefügt.
- Der WSS amtet als eine Art „Proxy" eines OWS. Er erhält über das WSS-Protokoll neben den Parametern für die OWS-Anfrage auch die Credentials des Users und dient damit in der XACML-Terminologie als Policy Enforcement Point (PEP). Dieser Bestandteil wird im Rahmen des kommerziellen Teils als „securityManager PDP" bezeichnet. Der WSS/PEP (oder genauer dessen Interceptoren) extrahiert aus der Anfrage die geforderten Ressourcen, Aktionen und Subjekte und leitet diese als Entscheidungsanfrage an den PDP weiter.
- Der Policy Decision Point (PDP) wertet diese Anfrage aus, indem er wahlweise auf eine Policy-Datenbank oder ein Verzeichnis mit XACML-Dateien zugreift und die zutreffenden XACML-Policies extrahiert.

[81] Universität Münster: http://www.uni-muenster.de (30.06.2007)

[82] con terra GmbH: http://www.conterra.de (30.06.2007)

[83] Int. Institute for Geo-Information Science and Earth Observation: http://www.itc.nl (30.06.2007)

[84] Environmental Systems Research Institute Inc.: http://www.esri.com (30.06.2007)

[85] Web Security Client (52°North, 2007)

Die nachfolgende Grafik (Abb. 32) gibt einen Überblick über die Bestandteile von 52°North und zeigt deren Interaktion.

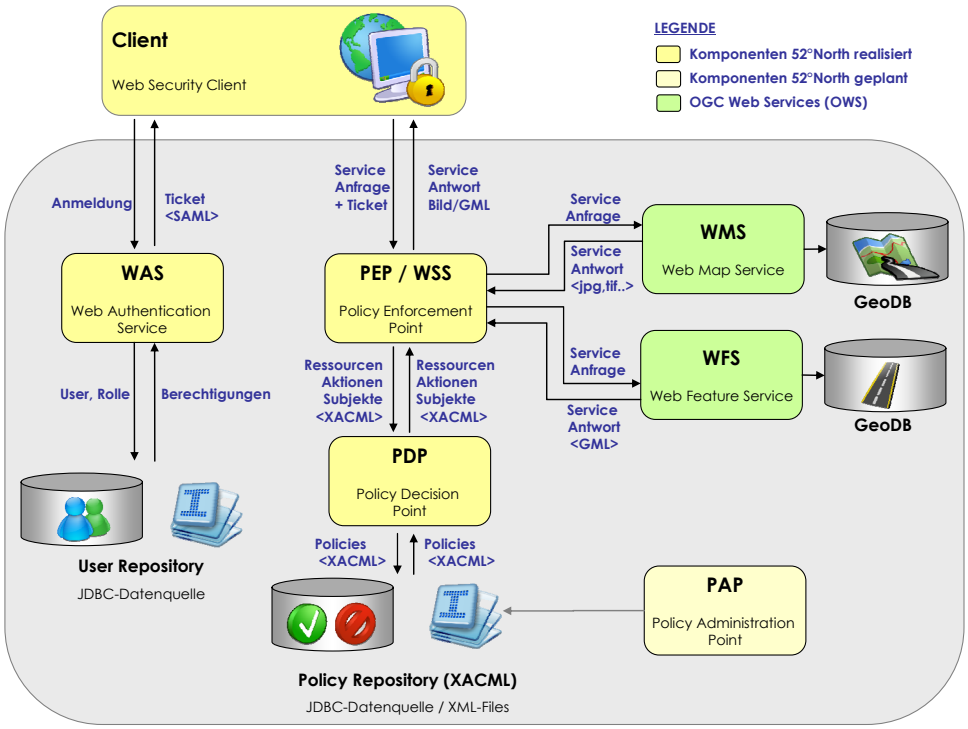

Abb. 32: Aufbau, Interaktion und Kommunikation von 52°North

Zusammenfassend lässt sich feststellen, dass die Zugriffseinschränkung von 52°North basierend auf dem Ansatz von XACML bewerkstelligt wird. Das nachfolgende Codebeispiel zeigt die thematischen Einschränkungen über die Ressourcen (engl. resources, Zeile 7-9) und Aktionen (engl. actions, Zeile 10-12), sowie die zeitlichen Einschränkungen durch Bedingungen (engl. conditions, Zeile 14-16). Die räumlichen Einschränkungen werden über Auflagen (engl. obligations) modelliert. Diese sind nicht in die XML Anfrage integriert, sondern stellen einen optionalen Befehl dar, der dem Ticket hinzugefügt und vom PEP ausgewertet wird.

```
1  <Rule RuleId="Rule1" Effect="Deny">
2    <Target>
3      <Subjects>
4        ...// Das zugreifende Subjekt.
5      </Subjects>
6      <Resources>
7        ...// Das Objekt auf das zugegriffen werden soll.
8      </Resources>
9      <Actions>
10       ...// Die Operation die auf der Ressource ausgeführt werden soll.
11     </Actions>
12   </Target>
13   <Condition>
14       ... // Eigenschaft die für die Zugriffsentscheidung ausgewertet wird.
15   </Condition>
16 </Rule>
```

Tab. 14: Pseudocode einer GeoXACML-Anfrage

3. Lösungsansatz

Im Lösungsansatz werden die Theorieansätze der ISO/OSI Sicherheitsarchitektur und der integrierten Sicherheitsarchitektur rekapituliert sowie der Stand der Sicherheitsbemühungen aus dem GDI-Umfeld (Kap. 3.1) zusammengefasst. Die daraus abgeleiteten Anforderungen für die Konzeption des GDI-Sicherheitsframeworks werden in Kap. 3.2 beschrieben.

3.1 Theorieansatz

3.1.1 ISO/OSI-Sicherheitsarchitektur

Die ISO/OSI identifiziert im Rahmen der OSI-Sicherheitsarchitektur 13 mögliche Sicherheitsdienste, die sich in die fünf Bereiche Authentifizierung, Zugriffskontrolle, Vertraulichkeit, Verbindlichkeit und Integrität unterteilen lassen. Die Empfehlungen der ISO/OSI, auf welcher Ebene des OSI-Referenzmodells diese Sicherheitsdienste am effektivsten anzusiedeln sind, können der nachfolgenden Grafik (Abb. 33) entnommen werden.

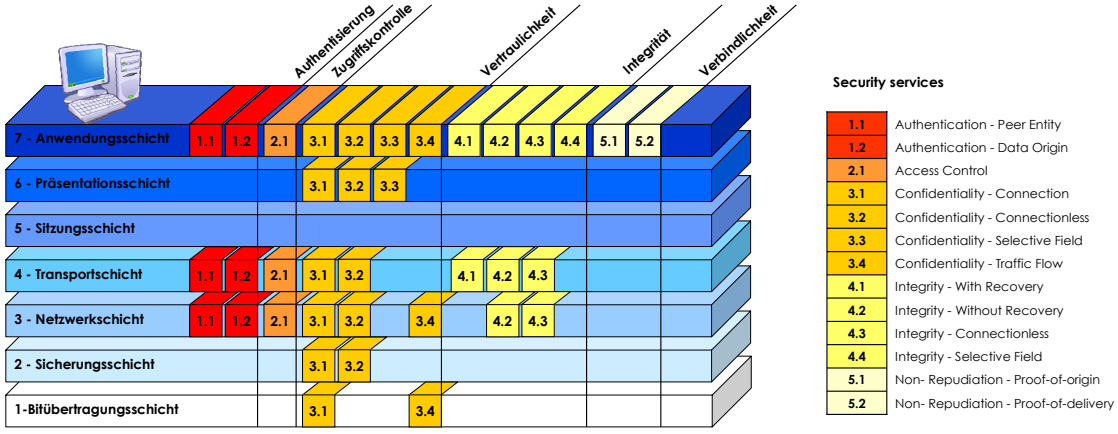

Abb. 33: Einordnung der OSI-Sicherheitsdienste in das OSI-Referenzmodell

Bei der Betrachtung der Grafik (Abb. 33) fällt auf, dass alle genannten OSI-Sicherheitsmassnahmen auf der Anwendungsschicht aufgesetzt werden können. Das bedeutet gleichzeitig, dass sich auf dieser Ebene die spezifischsten und „feingranularsten" Massnahmen definieren lassen. Dies hat zur Folge, dass auf Applikationsebene durch den Anspruch der Interoperabilität und Kompatibilität der grösste Entwicklungsaufwand zur deren Umsetzung betrieben werden muss. Auf der Netzwerk- und Transportschicht tragen die Standardverfahren der Netzwerksicherheit (Firewall, Router, generelle Verschlüsselung der Datenpakete etc.) dazu bei, die geforderten Sicherheitsansprüche bereits auf den unteren ISO/OSI-Schichten (1-4) teilweise zu erfüllen.

Bei den OSI-Sicherheitsmechanismen sind insbesondere die selektiven Verfahren (Sicherheitsmechanismen) von Interesse, da sie die grundlegenden Massnahmen zur Absicherung aufzeigen. Die nachfolgende Auflistung zeigt, mit welchen der zuvor vorgestellten Verfahren sich diese Sicherheitsmechanismen umsetzen lassen.

- Kryptografische Verfahren: **Nachrichtensicherheit**
- Digitale Signaturen: **Authentifizierung**
- Zugriffskontrollmechanismen: **Autorisierung** (Zugriffskontrolle)
- Datenintegritätsmechanismen: **Transport- und Nachrichtensicherheit**
- Mechanismen zum Austausch von Authentizitätsinformationen: **Authentifizierung**
- Anonymisierung von Verkehrsdaten: **Transport- und Nachrichtensicherheit**
- Mechanismen zu Kontrolle der Wegewahl: **Transport- und Nachrichtensicherheit**
- Notariatsmechanismen: **Authentifizierung, Accounting**

3.1.2 Integrierte Sicherheitsarchitektur

Der Ansatz der integrierten Sicherheitsarchitektur definiert eine eher konzeptuelle Betrachtungsweise von Sicherheit innerhalb einer verteilten Service-Architektur und basiert auf den drei Ebenen: Netzwerkebene (OSI-Schichten 1 bis 3), Netzwerkunterstützende Ebene (OSI-Schichten 4 bis7) und Applikationsebene (OSI-Schicht 7).

Als Basis dienen auch hier der sichere Datenaustausch, der Datenschutz, die Vertraulichkeit und die Integrität. Zum Erreichen der Verbindlichkeit werden Verschlüsselungstechniken empfohlen. Zudem werden im Rahmen der Grundprinzipien der integrierten Sicherheitsarchitektur ein einheitliches Rechte- und Zugriffsmanagement sowie ein sicheres Netzwerkmanagement gefordert.

3.1.3 Sicherheit im GDI-Umfeld

Die Sicherheitsanforderungen im GDI-Umfeld lassen sich weitestgehend mit allgemeinen Anforderungen an IT-Sicherheitssysteme vergleichen. So benennen Drewnak und Gartmann (Drewnak et al., 2005) folgende Anforderungen an ein Sicherheitskonzept für GDIs:

- Interoperabilität und Standardisierung der Verfahren
- Keine Modifikation bestehender Standards
- Dezentral verteilte Organisation der Zugriffskontrollinstanzen
- Single Sign-On Verfahren innerhalb der GDI

Diese Anforderungen wurden als Ausgangslage für die Konzeption eines Sicherheitskonzepts für beliebige OGC Web Services verwendet (Drewnak et al., 2005). Daraus entstanden die Spezifikationen eines Web Authentication Services (Drewnak et al., 2002) und eines Web Security Services (Drewnak, 2003), die im Rahmen des Testbeds der GDI NRW[86] prototypisch implementiert wurden. Die beiden Spezifikationen sind in Kap. 2.4.1 und 2.4.2 dokumentiert.

Zusätzlich zu den oben genannten Spezifikationen lässt sich die raumbezogene Zugriffs-kontrolle als weitere, geo-spezifische Anforderung deklarieren. Basierend auf der objektartigen Struktur der Geoinformationen können damit Zugriffsrechte für einzelne Informationsobjekte oder deren Raumbezug deklariert und durchgesetzt werden (Matheus, 2005). Es ergeben sich dadurch Zusatzanforderungen für die Zugriffsbeschränkung auf:

- Typen von Informationsobjekte (z.B. Punkt, Linie etc.),
- Informationsobjekte (z.B. Gebäude, Strassen etc.)
- geographische Gebiete (z.B. Gemeinde, Planungsgebiet etc.) und die Typen oder Instanzen von Informationsobjekten, die eine bestimmte raumbezogene Relation zu diesen geografischen Gebieten besitzen

Diese Anforderungen wurden im Rahmen der Spezifikation von GeoXACML umgesetzt. GeoXACML hat mittlerweile den Status eines OGC Discussion Papers erlangt und wurde im Kap. 2.4.3 detaillierter vorgestellt.

Im Juni 2006 wurde beim OGC eine Arbeitsgruppe „Sicherheit“[87]. geschaffen, deren erklärtes Ziel es ist, „[…] to establish an interoperable security framework for OpenGIS Web Services to

[86] Geodateninfrastruktur Nordrhein-Westfalen: http://www.gdi-nrw.org (30.06.2007)

[87] OGC Security Working Group (OGC, 2007b)

enable protected geospatial information processing“. Da das Thema Sicherheit bei OGC Web Services bis dato weitestgehend unbehandelt blieb, sollen mit Hilfe eines Sicherheits-Frameworks die nötigen Spezifikationen geliefert werden, so dass eine sichere Bearbeitung und Lizenzierung von Geoinformationen möglich wird. Die Sicherheitsmassnahmen sollen in einer interoperablen Art und Weise umgesetzt werden und wenn immer möglich bestehende IT-Standards nutzen. Die Security WG zeigt sich dabei für folgende Teilaspekte verantwortlich (OGC, 2007b):

- Authentifizierung als Grundvoraussetzung für eine Zugriffskontrolle und Lizenzierung von Geoinformationen
- Autorisierung zur Regulierung der Verfügbarkeit der Geoinformationen
- Einsatz von Verschlüsselung für den Datenschutz
- Zuverlässige Kommunikationsmechanismen für den Informationsaustausch zwischen Geschäftskunden
- Schutz vor unberechtigten Datenzugriffen bei einer Geodatenlizenzierung
- Lizenzierung von Geoinformationen

3.2 Beurteilung

Im Bereich der IT haben sich wie in Kap. 2.2.3 aufgeführt die vier zentralen Sicherheitsaspekte Vertraulichkeit, Authentizität, Verbindlichkeit, Integrität etabliert. Diese Aspekte werden sowohl in der OSI-Sicherheitsarchitektur als auch bei der integrierten Sicherheitsarchitektur entsprechend berücksichtigt. Zusätzlich zu den Sicherheitsansprüchen aus dem IT-Umfeld definieren beide Sicherheitsarchitekturen den Bereich der Zugriffskontrolle als weiteren Aspekt, den es bei der Konzeption einer sicheren GDI zu berücksichtigen gilt.

Die von der OSI identifizierten Sicherheitsmechanismen lassen sich mit den fünf zentralen Massnahmen der Transport und Nachrichtensicherheit sowie der Authentifizierung, der Autorisierung und des Accountings bewerkstelligen. Die Definition der OSI-Sicherheitsdienste und -mechanismen basiert auf der Grundlage des 7-Schichten-Modells. Nicht explizit erwähnt werden darin die Host- und Betriebsystem-Sicherheit die einen Teilaspekt der Verfügbarkeit abdecken. Der Ansatz der integrierten Sicherheitsarchitektur orientiert sich ebenfalls am 7-Schichten-Modell der OSI, reduziert dieses aber auf drei Ebenen. Die dadurch erzielte Generalisierung der OSI-Sicherheitsarchitektur verdeutlicht, dass sich die Komplexität der Sicherheitsanforderungen reduzieren lässt.

Für die Konzeption des Sicherheitsframeworks lassen sich aus der Theorie zusammenfassend folgende Sicherheitsaspekte ableiten.

- Authentifizierung Wer beansprucht die Dienstleistung?
- Zugriffskontrolle Welche Dienstleistung wird beansprucht?
- Vertraulichkeit Die Dienstleistung ist vor unautorisiertem Zugriff geschützt.
- Verbindlichkeit Die Dienstnutzung kann nicht abgestritten werden.
- Integrität Die unautorisierte Manipulation der Dienstleistung ist unmöglich.

Für die Umsetzung lassen sich aus den Literaturgrundlagen die folgenden zentralen Massnahmen identifizieren:

- Transportsicherheit Die Nachricht wird geschützt und verbindlich transportiert.
- Nachrichtensicherheit Die Nachricht wird signiert respektive verschlüsselt.
- Authentifizierung Die Identität der Kommunikationspartner wird festgestellt.
- Autorisierung Der Zugriff wird kontrolliert und durchgesetzt.
- Accounting Die Nutzung der Dienstleistung wird protokolliert.

Die oben beschriebenen Sicherheitsaspekte und Massnahmen bilden die Grundlage für die Konzeption des nachfolgenden GDI-Sicherheitsframeworks. Unter Berücksichtigung dieser Anforderungen lässt sich eine durchgehende Sicherheit innerhalb einer verteilten Architektur gewährleisten.

4. GDI-Sicherheitsframework

Das im Rahmen dieser Arbeit erstellte GDI-Sicherheitsframework beinhaltet eine Strukturierung und Einordnung der zuvor erläuterten Konzepte und Spezifikationen in ein Sicherheitsgesamtkonzept für Geo Web Services. Das folgende Kapitel fasst in einem ersten Teil die wesentlichen Sicherheitsaspekte und Massnahmen (4.1) zusammen. Diese dienen als Grundlage für die im zweiten Teil beschriebene Konzeption des GDI-Sicherheitskonzepts (4.2).

4.1 Sicherheitsaspekte und Massnahmen

Die Betrachtung der fünf zentralen Sicherheitsaspekte einer GDI lässt erkennen, dass sich die Anforderungen der unterschiedlichen Bereiche mit gemeinsamen Massnahmen sicher stellen lassen. Die Transport- und Nachrichtensicherheit dienen als Voraussetzung für alle Sicherheitsaspekte und bilden die Basis für die weiteren Massnahmen. Die Autorisierung erfüllt die Aspekte der Vertraulichkeit, Integrität und Zugriffskontrolle. Die Verbindlichkeit respektive Nicht-Abstreitbarkeit wird zusätzlich zur Transport- und Nachrichtensicherheit mittels Authentifizierung und Accounting gewährleistet. Die nachfolgende Übersicht (Tab. 15) soll die Zuordnung der Sicherheitsaspekte zu den zu treffenden Massnahmen verdeutlichen.

Sicherheitsaspekt	Massnahme zur Sicherstellung
Vertraulichkeit	▪ Nachrichtensicherheit (Kryptografie) ▪ Transportsicherheit ▪ Autorisierung
Authentizität	▪ Nachrichtensicherheit (Kryptografie) ▪ Transportsicherheit ▪ Authentifizierung

Verbindlichkeit, Nicht-Abstreitbarkeit	▪ Nachrichtensicherheit (Kryptografie) ▪ Transportsicherheit ▪ Authentifizierung ▪ Accounting
Integrität	▪ Nachrichtensicherheit (Kryptografie) ▪ Transportsicherheit ▪ Autorisierung
Zugriffskontrolle	▪ Nachrichtensicherheit (Kryptografie) ▪ Transportsicherheit ▪ Autorisierung

Tab. 15: Sicherheitsaspekte im IT-Bereich und die zugehörigen Verfahren

Es lässt sich konstatieren, dass sich durch den Einsatz der oben erwähnten Massnahmen und Verfahren die wesentlichen Sicherheitsfragen einer verteilten Systemarchitektur beantworten lassen. Im Rahmen des Kontexts können damit offene Web Services und GDIs in genügendem Masse abgesichert werden. Alle übrigen Aspekte definieren Spezialverfahren die spezifischen Anforderungen genügen und sich deshalb ausserhalb des gesetzten Rahmens befinden.

4.2 GDI Konzept

Das GDI-Sicherheitsframework identifiziert die fünf wesentlichen Ebenen einer sicheren Geodateninfrastruktur. Diese lassen sich in zwei Gruppen unterteilen:

- Verbindungssicherheit — Transportsicherheit und Nachrichtensicherheit
- Applikationssicherheit — Authentifizierung, Autorisierung und Accounting

Die Gruppe der Verbindungssicherheit stellt eine durchgängige und für alle beteiligten Instanzen vertrauenswürdige Kommunikationsgrundlage dar, die während dem Informationsaustausch bestehen bleibt. Durch die darin enthaltenen Ebenen der Transport- und Nachrichtensicherheit wird sowohl die Nachricht selbst als auch deren Übertragung abgesichert.

Die Gruppe der Applikationssicherheit garantiert eine sichere Identifizierung der am Austausch beteiligten Instanzen (Authentifizierung), überprüft und überwacht den Zugriff auf die angebotenen Dienstleistungen (Autorisierung) und bietet eine verbindliche Protokollierung der effektiven Nutzung der Dienste und Daten (Accounting).

In der nachfolgenden Übersicht (Abb. 34) sind die wesentlichen Ebenen der Sicherheitsmechanismen einer GDI grafisch dargestellt. In den nachfolgenden Kapiteln werden die Anforderungen an diese Ebenen einzeln beschrieben.

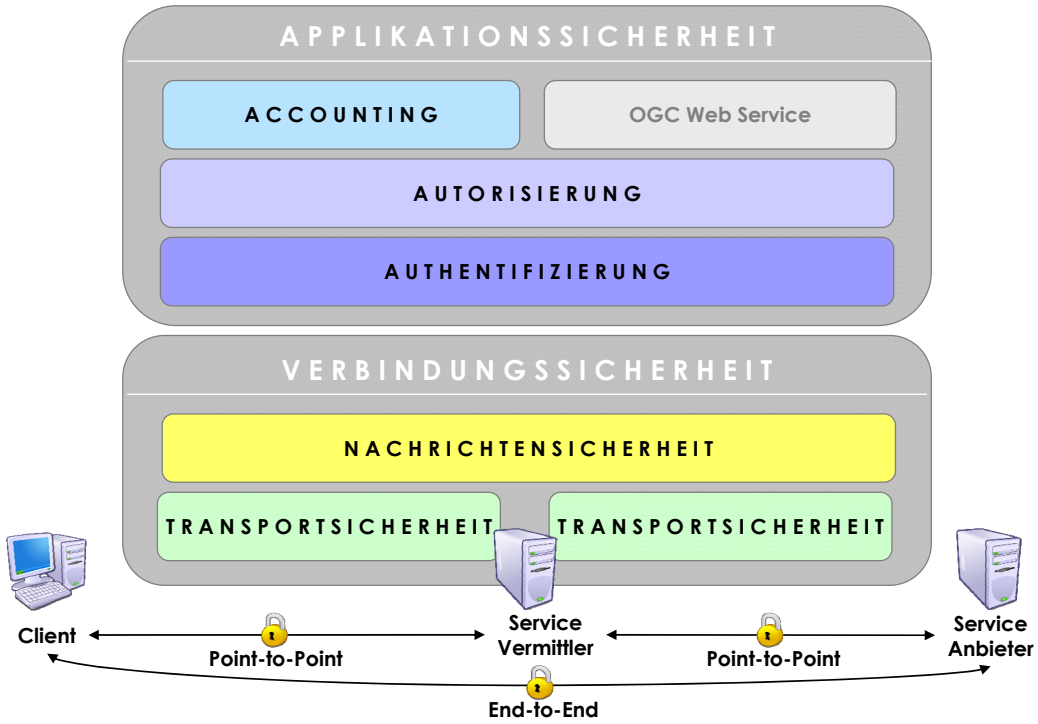

Abb. 34: GDI-Sicherheitsframework

4.2.1 Verbindungssicherheit

Die Verbindungssicherheit bietet eine durchgängige Basisfunktionalität, die während der Kommunikation gewährleistet sein muss.

4.2.1.1. Transportsicherheit

Die Transportsicherheit garantiert eine sichere Verbindungsleitung zwischen Client, Service Vermittler und Service Anbieter und bildet damit die Voraussetzung für eine sichere Datenübertragung von Start- zum Zielmedium (End-to-End). Dies bedeutet, dass die Daten zwischen den Kommunikationspartnern während der gesamten Verbindungsdauer vertraulich und vor unbefugten Zugriffen oder Modifikationen geschützt transferiert werden müssen. Die sichere End-to-End-Verbindung muss für alle an einer GDI beteiligten Services gewährleistet werden können. Dies ist bei einer verteilten GDI vor allem dann von Bedeutung, wenn die

Benutzer- und Rechteverwaltung von der eigentlichen Geodatenverwaltung getrennt ist und die Transportsicherheit auch zwischen den Services gesichert sein muss.

4.2.1.2. Nachrichtensicherheit

Die Nachrichtensicherheit beinhaltet die Absicherung einer Nachricht während der gesamten Verbindungsdauer und verhindert damit das unautorisierte Abhören oder Manipulieren des Nachrichteninhalts. Nachrichtensicherheit lässt sich grundsätzlich mit Hilfe von Verschlüsselungsverfahren (Kryptografie) erfüllen, wobei eine Nachricht oder Teile einer Nachricht verschlüsselt werden können. Ein wichtiger Aspekt bei der Verschlüsselung stellt der Austausch der Schlüssel dar, der in den meisten Fällen über ein asymmetrisches Verfahren (Public-Key) bewerkstelligt wird. Hierzu ist es wichtig, dass sich die beiden Kommunikationspartner auf eine korrekte gegenseitige Authentifizierung verlassen können. In diesem Bereich haben sich PKI-Verfahren etabliert, die mit Hilfe von elektronischen/digitalen Signaturen die Kommunikationspartner gegenseitig authentifizieren.

Die Verschlüsselung der gesamten Nachricht ist aus Gründen der Sicherheit und Performance meist nicht sinnvoll. Die Nutzung von SOAP als Standardprotokoll für Web Services bietet hier den Vorteil, dass SOAP als XML-basiertes Format eine physische und logische Struktur beinhaltet. Somit ermöglicht SOAP einzelne Teilbereiche einer Nachricht (z.B. Elemente oder Attribute) getrennt zu verschlüsseln. Damit lassen sich beispielsweise die Zahlungs- und Nutzinformationen innerhalb einer Nachricht mittels zweier unterschiedlicher Verfahren verschlüsseln, wodurch verschiedene Kommunikationspartner ihren Teilbereich der Nachricht jeweils getrennt signieren können.

Bei der Anfrage mittels parametrisierter URL-Anfrage (REST-Methode), wie sie für OOG Web Services derzeit meist vorkommt, kann durch die Verwendung eines sicheren Transportverfahrens (z.B. SSL/TLS) ein ausreichender Schutz geboten werden.

4.2.2 Anwendungssicherheit

Die Anwendungssicherheit dient dazu, Web Services mit Hilfe der Authentifizierungs-, Autorisierungs- und Accounting-Verfahren (Triple-A) abzusichern. Zur Durchsetzung dieser Triple-A-Verfahren bedarf es zusätzlich einer zentralen Instanz zur Prüfung und Durchsetzung der Zugriffsentscheidungen (Rechteprüfung oder Policy Enforcement). Hier wird entschieden, wer auf welche Ressource in welchem Umfang zugreifen darf und wie oft er dies tut. Die

Rechteprüfungs-Instanz stellt somit im übertragenen Sinn die Stelle dar, an der der Vertrag zwischen dem Anfrager und Anbieter entsteht.

4.2.2.1. Authentifizierung

Die Authentifizierung beschreibt das Vorgehen der qualifizierten Überprüfung einer Identität. Die Überprüfung der Identität geschieht durch die Bekanntgabe von Credentials, mit denen das Subjekt bei einer Authentifizierungs-Instanz Zeugnis über seine Identität ablegt. Die Bekanntgabe der Credentials muss über eine sichere Verbindung erfolgen. Im Bereich der Web Services haben sich Authentifizierungsverfahren mittels Benutzernamen und Passwort etabliert, da sie sich am einfachsten und flexibelsten implementieren lassen. Bei sicherheitskritischen Anwendungen werden auch elektronische Signaturen oder Smartcards verwendet. Der Aufwand zu deren Realisierung lohnt sich dann, wenn auch von Seiten der Transportsicherheit entsprechend dedizierte Verfahren zum Einsatz kommen.

Bei erfolgreicher Authentifizierung wird von der Authentifizierungs-Instanz zum einen ein serverseitiges Session-Objekt (oder auch Assertion-Objekt) erzeugt, welches während der Interaktion mit der GDI bestehen bleibt. Zum anderen wird dem Subjekt ein entsprechendes Ticket ausgestellt, mit dem es beim Zugriff auf die GDI seine Authentizität nachweisen kann. Die Informationen des Tickets müssen vor möglichem Missbrauch geschützt werden (z.B. Man-in-the-Middle-Attacken[88]) und dürfen deshalb nicht unverschlüsselt oder über eine unsichere Transportverbindung ausgetauscht werden. Eine zusätzliche Sicherheit bietet in diesem Zusammenhang die Verwendung von Authentifizierungsverfahren die nur eine Referenz auf das erzeugte Session-Objekt weitergeben und nicht das Objekt selbst. Dies schützt vor Wiedereinspielungs-Angriffen[89].

Die Authentifizierung setzt die Funktionalität eines Single-Sign-On-Verfahrens voraus. Dies bietet zum einen den Gewinn an Benutzerkomfort, da der Nutzer während der Gültigkeitsdauer seines Tickets sich nur einmal authentifizieren muss. Zum anderen kann ein SSO auch zu einer erhöhten Sicherheit beitragen, da die Häufigkeit der Übermittlung der sicherheitskritischen Credentials vermindert wird. Die SSO-Funktionalität lässt sich mittels eines „Circle-of-Trust“ realisieren. Der Nutzer kann sich somit bei einem Authentifizierungs-Service anmelden und

[88] Bei einer Man-in-the-Middle-Attacke versucht ein Angreifer den Datenkanal mittels Manipulation unter seine Kontrolle zu bringen.

[89] Bei Replay-Attacken versucht ein Angreifer mit einem alten oder gefälschten Authentifizierungsnachweis auf die Dienstleistung zuzugreifen.

erhält ein Ticket für den Zugriff auf die weiteren GDI-Services innerhalb des „Service-Vertrauensverbundes“. Diese dezentralisierte Identitätsverwaltung erlaubt den Austausch von Identitäten über die Sicherheitsdomänen hinweg.

4.2.2.2. Autorisierung

Unter Autorisierung versteht man die Einhaltung von Benutzerberechtigungen, so dass jeder Rolle nur die Dienstleistungen (Services oder Daten) zur Verfügung stehen, für die sie entsprechend autorisiert ist. Innerhalb von GDIs kann der Zugriff auf die Ressourcen thematisch, zeitlich und räumlich eingeschränkt sein. Die thematische Einschränkung sollte sowohl die Autorisierung nach einzelnen Themengebieten (z.B. Datenlayer) als auch nach einzelnen Funktionen (z.B. getCapabilities) gewährleisten.

Ein dadurch mögliche Zugriffsregel für ein Subjekt (z.B. Bob in der Rolle eines Studenten) könnte wie folgt definiert sein:

- Thematisch — Auf welche Thematik und Funktion soll in der Servicenutzung zugegriffen werden? (z.B. GetFeature auf der Informationsebene Strassen eines OGC WFS-Services)
- Zeitlich (temporal): — In welchem Zeitintervall ist die Servicenutzung erlaubt? (z.B. Werktags zwischen 06:00 und 20:00 Uhr)
- Räumlich (spatial) — In welchem geografischen Bereich ist die Servicenutzung zulässig? (z.B. Im Bereich des Projektgebiets Schweiz)

Die Zugriffsregeln müssen möglichst bedarfsgerecht erstellt werden, wobei darauf zu achten ist, dass die Verwendbarkeit auch über verschiedene Anwendungsbereiche und Projekte hinweg gewährleistet bleibt. Eine zu strikte Zugriffsbegrenzung würde eine interdisziplinäre Nutzung der Daten und Services unnötig einschränken. Die dazu erforderliche Verwaltung und Administration der Zugriffsregeln (engl. policies) muss in einer zentralen Verwaltungs-komponente erfolgen.

Eine einkommende Service-Anfrage enthält zusätzlich zu der Anfrage über die Nutzung der Funktion eines Web Services (OWS-Request) auch die vom Authentifizierungsservice für das anfragende Subjekt ausgestellte Ticketinformation. Nach der Entschlüsselung der Nachricht erfolgt die Prüfung der Validität der mitgelieferten Authentifizierungsinformation. Damit kann sicher gestellt werden, dass die Service-Anfrage auch wirklich vom zugreifenden Subjekt stammt. Die erfolgreiche Kontrolle der Ticketinformation bestätigt die Authentizität des Subjekts. Dies ist Voraussetzung für die Analyse der beabsichtigte Web Service Nutzung.

Diese Analyse besteht aus zwei Teilen. In einem ersten Schritt werden die Parameter und Wertebereiche im Hinblick auf mögliche DoS-[90] oder XML-Poisoning-Attacken[91] überprüft. Wird kein möglicher Angriff festgestellt, wird in einem zweiten Schritt die beabsichtigte Web Service Nutzung mit den erfassten Zugriffsregeln verglichen. Aufgrund einer Übereinstimmung der Anfrage mit den definierten Zugriffsregeln wird die Anfrage an den entsprechenden Geo Web Service weitergeleitet. Nach getaner „Arbeit", liefert der Geo Web Service die Ergebnisse der Anfrage zurück an den Autorisierungsservice. Hier wird nun zum einen die Information über die tatsächlich bezogene Dienstleistung an den Accounting Service weitergeleitet. Zum anderen werden die Informationen signiert und über die sichere Transportleitung an den Client zurückgesendet.

4.2.2.3. Accounting

Im Rahmen des Accountings wird die Nutzung der Services einer GDI protokolliert. Das Accounting dient dazu, um die effektive Nutzung der Dienstleistung und die damit verbundene Verbindlichkeit respektive Nicht-Abstreitbarkeit der erhaltenen Information zu gewährleisten. Mit Hilfe des Accounting lässt sich beweisen, dass ein Subjekt die Dienstleistung zum gewünschten Zeitpunkt und im gewünschten Bereich in Anspruch genommen hat.

Die Information über die tatsächlich beanspruchte Servicenutzung gelangt vom Autorisierungsservice über eine gesicherte Verbindung und in verschlüsselter Form an den Accountingservice. Dieser extrahiert die erforderlichen Parameter und verwaltet diese für eine nachträgliche verbindliche Auskunft in einer geeigneten Ablagestruktur (Filesystem oder DB). Ein Accounting-Eintrag des Beispiels aus Kap. 4.2.2.2 sollte dabei mindestens folgende Informationen enthalten:

- Rollen-ID — Welche Rolle hat den Service beansprucht? (z.B. Student)
- Datum, Zeit — Zu welchem Zeitpunkt wurde der Service genutzt? (z.B. Montag, 30.06.2007, 15:40)
- Art der Ressource — Welcher Service wurde genutzt? (z.B. WFS-ID 123, Navigation)
- Art der Nutzung — Welche Informationen, Funktionen oder Themen wurden genutzt? (z.B. GetFeature der der Informationsebene Strassen)

[90] Denial-of-Service-Attacken sind sinnlose Anfragen, die zu einer Überlastung des Systems führen.

[91] XML-Poisoning-Attacken versuchen mit einem tief-verschachtelten XML-Angriffsdokument ein DoS zu erwirken.

Das Accounting kann neben der Gewährleistung des Verbindlichkeitsaspekts auch aus kommerzieller Sicht interessant sein. Zum einen um eine interessengerechte Publikation von Betriebs- oder Angebotshinweisen zu erreichen oder eine automatisierte Rechnungsstellung zu ermöglichen. Zum anderen kann es helfen, eine missbräuchliche Nutzung der GDI zu erkennen und zu unterbinden, sowie um das Serviceangebot analysieren und verbessern zu können.

4.3 Empfehlung

Basierend auf der Konzeption des GDI-Sicherheitsframeworks wird nachfolgend versucht eine konkrete Empfehlung für die Architektur einer sicheren GDI aufzuzeigen. Dazu werden die wesentlichsten Standards und Verfahren den fünf identifizierten Sicherheitsebenen zugeordnet und in das GDI-Sicherheitsframework integriert (Abb. 37). Die Empfehlung wurde auf Grund der im Literaturüberblick erarbeiteten Grundlagen und auf Grund subjektiver Eindrücke erstellt.

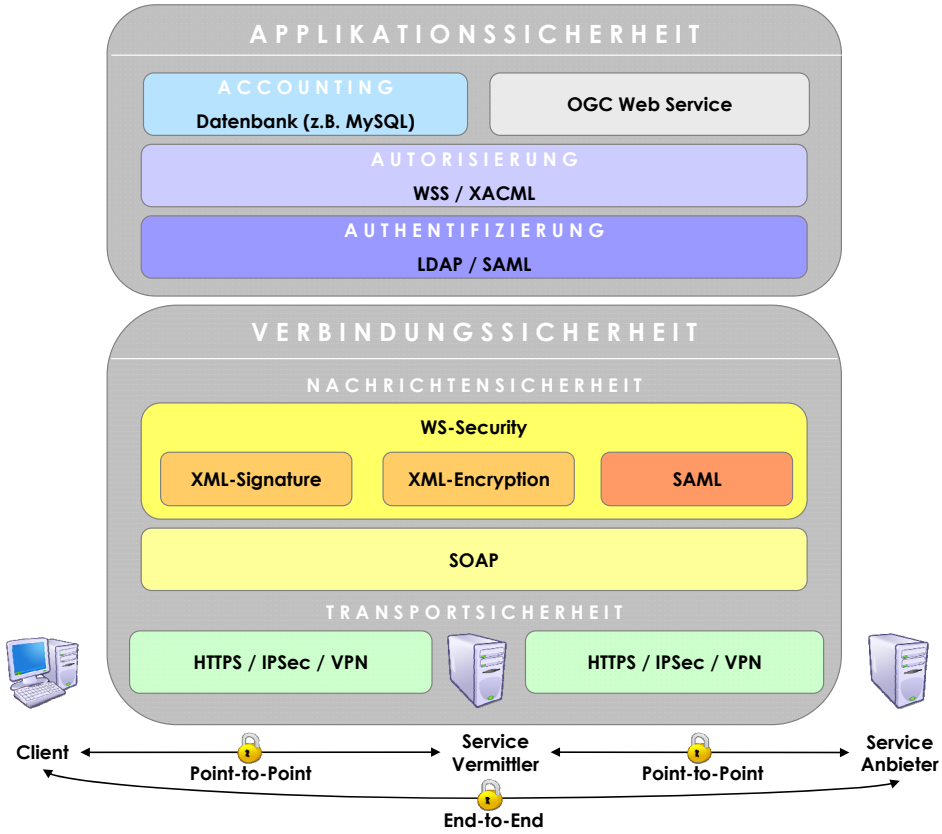

Abb. 35: GDI-Sicherheitsframework: Einordnung der Standards und Spezifikationen

4.3.1 Verfahren und Standards

4.3.1.1. Transportsicherheit

Die Wahl des jeweils besten Verfahrens für die Transportsicherheit ist massgeblich von der gewünschten Art der Anbindung abhängig. Wenn es sich um eine dauerhafte Verbindung handelt, kann der erhöhte Aufwand für das Etablieren einer VPN-Lösung (Konfiguration VPN-Gateway, Authentifizierung durch Merkmal) durchaus angebracht sein. Für eine temporäre Anbindung ist SSL/TLS (über HTTPS) ausreichend sicher, da auf Grund der zeitlich begrenzten Gültigkeitsdauer des Tickets der Aufwand zur Aufschlüsselung der gesicherten Nachricht länger dauert als die Validität des Tickets.

Die vorgestellten Verfahren stellen den sicheren Transport bis zur jeweils vorgegebenen Schicht des OSI-Schichtenmodells sicher. Bei SSL/TLS ist dies die Transportschicht (Schicht 4) und bei IPSec die Netzwerkschicht (Schicht 3). Die Verantwortung für den sicheren Transport auf den höheren Schichten obliegt der jeweiligen Start- respektive Zieldomäne. Diesen Aspekt müssen die Kommunikationspartner für ihren Bereich mittels einer adäquaten Netzwerk- und Betriebssystemsicherheit (Updates, Patches, etc.) selber sicher stellen. Diese Absicherung gilt als Voraussetzung für eine durchgehende Verbindungssicherheit. Die nachfolgende Übersicht (Abb. 36) soll die Aufteilung der Verantwortlichkeiten zwischen der Transportsicherheit (SSL/TLS und IPSec) und der Sicherheit der Start- und Zieldomäne (Netzwerk- und Betriebssystemsicherheit) verdeutlichen.

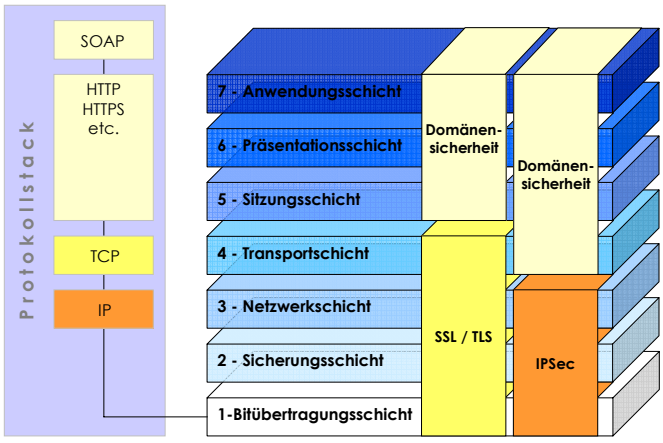

Abb. 36: Transportsicherheit in Bezug auf das ISO/OSI-Referenzmodell

4.3.1.2. Nachrichtensicherheit

Bei der Umsetzung der Nachrichtensicherheit gilt es unter anderem die Anbindung an eine Public Key Infrastruktur (PKI) sicher zu stellen. In der Schweiz gibt es bis dato drei namhafte Zertifizierungsdienstanbieter für PKIs die die benötigten Dienste bereitstellen (Swisscom Solutions AG, QuoVadis Trustlink AG, Die Schweizerische Post - SwissSign AG).

Für die Verschlüsselung einer SOAP-Nachricht (oder Teilen davon) bieten sich die Standards von XML-Signature und XML-Encryption an. XML-Signature definiert den Aufbau der benötigten digitalen XML-Signaturen und zeigt auf, welche Verschlüsselungsverfahren zu deren Signierung eingesetzt werden können. XML-Encryption stellt die Mechanismen zur Verschlüsselung von Nachrichten - oder im Fall von SOAP - von spezifischen Nachrichtenteilen zur Verfügung. Die erwähnten Standards werden im WS-Security Standard vereint. WS-Security bietet eine erweiterbarere SOAP-Grundlage um verschiedene Sicherheitssysteme sicher miteinander kommunizieren zu lassen. Ziel von WS-Security ist es, SOAP dahingehend zu erweitern, um bestehende Techniken wie XML-Signature, XML-Encryption, PKIs oder SAML in standardisierter Form miteinander interagieren zu lassen (Melzer et al., 2007). WS-Security ist gleichzeitig auch die Basis für alle weiteren Sicherheitsstandards die von Web Services genutzt werden können.

Die oben erwähnten XML-basierten Verfahren setzen die Verwendung von SOAP voraus, was aber für einen grossen Teil der OGC Web Service-Anfragen derzeit noch nicht der Fall ist. Der Absicherung einer parametrisierten URL-Anfrage, wie sie derzeit für OWS üblich ist (REST-Methode), kann auch mittels HTTP Binding für die GET- und POST-Methode erfolgen. Dabei werden die Sicherheitsparameter als sogenannte „Vendor-specific Parameters“ (VSP) der OWS-Serviceanfrage hinzugefügt und müssen durch die Autorisierungskomponente entsprechend ausgewertet werden. Ein solches Beispiel könnte wie folgt aussehen:

```
1  http://mapviewer/wms?REQUEST=GetMap &SERVICE=WMS
2                                      &VERSION=1.3.0
3                                      &AUTHINFO=SAMLArt
```

Tab. 16: Pseudo-Beispielabfrage OWS + Authentifizierungsinformation

Durch die Absicherung der Verbindung über HTTPS, IPSec oder VPN und die Verwendung einer Assertion-Referenz (vgl. SAMLArt) sind diese Anfragen ausreichend abgesichert.

4.3.1.3. Authentifizierung

Die Authentifizierung im Bereich der Geo Web Services wird idealerweise mittels eines Single-Sign-On-Verfahrens über das SAML-Protokoll realisiert. Die SSO-Funktionalität lässt sich

mittels eines „Circle-of-Trust“[92] realisieren, wie es das Liberty Alliance Project vorsieht. Der Vorteil des Liberty Alliance-Ansatzes liegt dabei darin, dass der Benutzer selber entscheiden kann welchen Web Services er seine persönlichen Daten bekannt geben möchte und an welche Dienste innerhalb der Föderation diese Informationen im Hinblick auf die Verknüpfung von Web Services (Service-Chaining) weitergegeben werden dürfen. Es handelt sich also um ein SSO-Verfahren in einem vom Benutzer definierten Teilnehmerkreis von Web Services.

Der Vorteil von SAML besteht in der Art und Weise, wie die Credentials ausgetauscht werden. Es empfiehlt sich die Verwendung des Artefact-Profils da dadurch die Credentials nicht direkt bei der Anfrage übermittelt werden. Es wird lediglich eine Referenz auf das beim Authentifizierungsservice erstellte Assertion-Objekt übergeben und der Anbieter kann sich selber von dessen Validität überzeugen. Im allgemeinen IT-Umfeld hat sich LDAP[93] als De-facto-Standard für Authentifizierungsdienste etabliert (Howes et al., 2005). LDAP ist ein Verzeichnisdienst der die verschiedensten Authentifizierungsverfahren unterstützt und die Verwaltung der SAML-Assertions übernehmen kann.

4.3.1.4. Autorisierung

Zur Beschreibung von Autorisierungsregeln innerhalb einer GDI bietet sich GeoXACML an. Die einkommenden Service-Anfragen werden zusammen mit der Anfrage an den Policy Enforcement Point (PEP) geschickt. Der PEP extrahiert die für die Autorisierung relevanten Informationen (Ticket) von den allgemeinen Parametern einer OWS-Anfrage und leitet diese an die Autorisierungs-Entscheidungsinstanz, den Policy Decision Point weiter (deegree: owsProxy, 52°North: Policy Decision Point). Der PDP vergleicht die angefragte Dienstnutzung mit den definierten Zugriffsregeln und gibt die Autorisierungsentscheidung zurück an den PEP. Der PEP veranlasst auf Grund Entscheidung die die gewünschte Dienstleistung beim entsprechenden OGC Web Service.

4.3.1.5. Accounting

Das Accounting selbst, also die Erstellung von Log-Einträgen der Nutzung der Ressourcen durch die jeweilige Anwender-Rolle, erfolgt in einer geeigneten Ablagestruktur (Filesystem oder DB). Die dazu erforderliche Funktionalität kann entweder direkt in eine bestehenden

[92] „Circle-of-Trust“ ist eine vertrauenswürdige Dienste-Föderation bei der nach erfolgreicher Authentifikation bei einem Service die Nutzung der weiteren Dienste ohne weitere Authentifizierung ermöglicht wird.

[93] Siehe auch Anhang 1: LDAP

Rechteprüfungsinstanz integriert werden (deegree: owsProxy, 52°North: PEP/WSS) oder als eigenständiger Web Service betrieben werden. Die Konzeption eines eigenständigen Accounting-Dienstes bietet dabei den Vorteil der Unabhängigkeit von der Entwicklung der Rechteprüfungsinstanz.

4.3.2 Aufbau und Interaktion

Die oben aufgeführte Architektur setzt sich aus folgenden Komponenten zusammen:

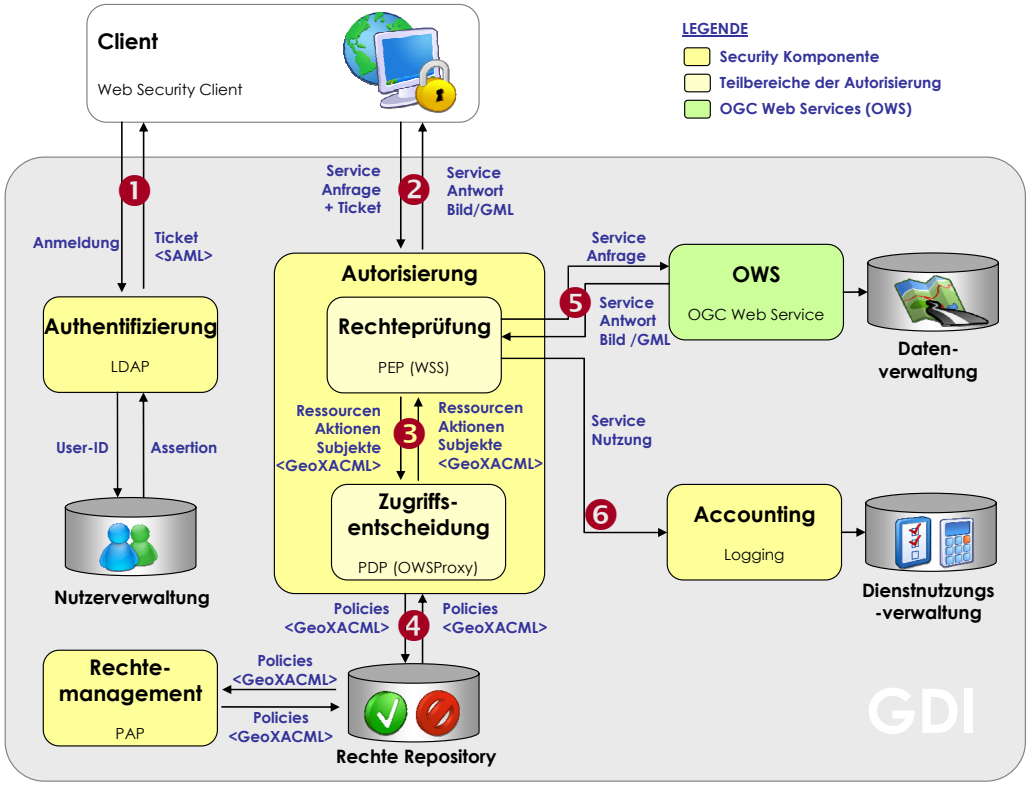

Abb. 37: Empfehlung für die Architektur einer sicheren GDI

4.3.2.1. Authentifizierung

Nach der Überprüfung der qualifizierten Anmeldung kann die Authentifizierungskomponente die Credentials mit den Einträgen im User Repository vergleichen und bei einer Übereinstimmung ein entsprechendes Ticket ausstellen. Für den Austausch dieser Informationen empfiehlt es sich, das SAML Artefact-Protokoll zu verwenden. Für die Rechteverwaltung kann LDAP verwendet werden.

- Input ❶: Credentials (Wissen, Besitz oder Merkmal)
- Output ❶: Ticket (SAML Artefact)

4.3.2.2. Autorisierung

Die Autorisierung lässt sich mittels GeoXACML bewerkstelligen. Das Accounting wurde zum einfacheren Verständnis in die Bereiche Rechteprüfung und Zugriffsentscheidung unterteilt.

Rechteprüfung: Der Policy Enforcement Point (PEP) überprüft als erstes die Validität des Tickets und die Gültigkeit der Wertebereiche. Sind diese Prüfungen erfolgreich, wird die Anfrage in die Form von GeoXACML-Policies übersetzt und mit den zur Autorisierung erforderlichen Parametern wie Ressourcen, Aktionen und Subjekte an den Policy Decision Point (PDP) weitergegeben. Basierend auf der Zugriffsentscheidung des PDP formuliert er die entsprechende Anfrage an den OGC Web Service (OWS). Die vom OWS erhaltenen Resultate sendet er in verschlüsselter Form an den Client zurück und übermittelt die Informationen über die Art und Umfang der Nutzung an die Accounting-Instanz.

- Input ❷: Service Anfrage + Ticket
- Output ❸: GeoXACML Policy Anfrage
- Input ❸: GeoXACML Policy Antwort
- Output ❺: Service Anfrage
- Input ❺: Service Antwort (Geodaten als GML, Bild)
- Output ❷: Service Antwort (Geodaten als GML, Bild)
- Output ❻: Servicenutzungsinformationen

Zugriffsentscheidung: Der Policy Decision Point vergleicht die gewünschte Nutzung mit den vorgegebenen Policies (❹) und „entscheidet“ ob der gewünschte Zugriff gewährt werden darf. Der Zugriffsentscheid (permit, deny, not applicable oder indeterminate) wird an den PEP gesendet.

- Input ❸: GeoXACML Policy Anfrage
- Output ❸: GeoXACML Policy Antwort

4.3.2.3. Accounting

Die Accounting-Komponente erhält die Angaben über die Dienstnutzung (Rollen-ID, Datum und Zeit, Art der Ressource und Nutzung) vom Policy Enforcement Point und loggt diese in der Dienstnutzungsverwaltung. Dies kann in einer SQL-Datenbank (z.B. MySQL)erfolgen.

- Input ❻: Servicenutzungsinformationen

5. Ergebnisse und Beurteilung

In diesem Kapitel werden die wichtigsten Ergebnisse dieser Arbeit dargestellt (Kap. 5.1) und kritisch beurteilt (Kap. 5.2). Die inhaltliche Beurteilung (Kap. 5.2.1) wird auf Grund der eingangs aufgestellten Thesen vorgenommen. Die Beurteilung der gewählten Methodik (Kap. 5.2.2) schliesst dieses Kapitel ab.

5.1 Ergebnisse

Die Massnahmen zur Sicherstellung der Verbindungssicherheit sind Basistechnologien aus der IT, die sich im Bereich von Web Services und verteilten Infrastrukturen bereits bewährt haben. Sie definieren die Teilbereiche der sicheren und verbindlichen Transport- und Nachrichtensicherheit. Die Schwierigkeit besteht darin, diese Teilbereiche so aufeinander abzustimmen, dass hinsichtlich des Aspekts einer durchgehenden, homogenen Sicherheit, keine Lücken entstehen. In diesen Bereichen bedarf es keiner zusätzlichen geo-spezifischen Erweiterungen. Die Verbindungssicherheit sollte auf folgenden Rahmenbedingungen basieren:

- Die Kommunikationspartner stellen durch eine stetig aktualisierte Domänensicherheit das Funktionieren der erforderlichen Netzwerk- und Betriebssystemsicherheit ihres Teilbereiches sicher.
- Es ist im Aufgabenbereich des Anbieters die Anforderungen hinsichtlich Verbindungssicherheit vorzugeben. Sein Interesse muss es dabei sein, die Sicherheit seiner Dienstnutzung mittels eines zweckmässigen Verfahrens zu gewährleisten. Neben dem Aspekt der Sicherheit sollte dabei stets auch der Benutzerfreundlichkeit und Interoperabilität der Lösung bedacht werden.
- Der Anbieter einer GDI muss mittels geeigneter Verfahren nicht nur eine sichere Verbindung zwischen dem Client und dem Service-Vermittler (Point-to-Point) sicher

stellen, sondern muss die Sicherheit innerhalb der verteilten Infrastruktur gewährleisten können. Nur so kann eine verbindliche und damit von keiner Partei abstreitbare Servicenutzung garantiert werden.

- Der Austausch der Nachrichten zwischen Web Services basiert neben dem Verfahren via REST-Methode vor allem auf dem SOAP-Protokoll (Maschine-Maschine-Kommunikation). Demzufolge besteht in diesem Bereich ein potenzielles Sicherheitsrisiko, da bei einem XML-Angriff (vgl. Kap. 2.2.2.2) die SOAP-Nachricht die bestehenden Firewalls in verschlüsselter Form passiert und nach deren Entschlüsselung direkt die entsprechende Web Service Anfrage starten kann. Durch geeignete Prüfungsverfahren (z.B. XML-Firewall) lassen sich die Anfragen an einen Service vor deren Ausführung validieren und auf eine potenzielle Gefährdung überprüfen.

Auf der Ebene der Applikationssicherheit decken die Authentifizierung und Autorisierung sowie das Accounting die Sicherheitsanforderungen ab. Sie bieten die gewünschten spezifischen Funktionalitäten um bedarfsgerechte Zugriffsentscheidungen fällen zu können und enthalten die dazu erforderlichen geo-spezifischen Erweiterungen. Für die Gewährleistung der Applikationssicherheit sollten folgende Bedingungen erfüllt werden:

- Es bedarf einer zentralen Benutzerverwaltung, die vom Betreiber der jeweiligen GDI individuell bewirtschaftet und kontrolliert werden kann. Damit ist es im Ermessen des Anbieters, welchen Rollen er welche Rechte zuweist und wie er deren Zugriff eingeschränkt.
- Der Austausch von Authentifizierungsinformationen der Benutzer und die Zuweisung zu deren Rolle basiert auf standardisierten Verfahren (z.B. SAML, SAML-Artefact). Dadurch ist es im Hinblick auf die angestrebte Sicherheitsinteroperabilität (vgl. Kap. 2.1.2) keine zwingende Voraussetzung, dass die authentifizierende Instanz selber auch Teil der GDI ist. Dies setzt voraus, dass sich die Authentifizierungs- und Autorisierungsinstanz kennen und gegenseitig vertrauen oder dass sie die Benutzerinformationen über einen gemeinsamen Vertrauenspartner austauschen können (z.B. Liberty Alliance).
- Die Authentifizierungsinformationen der Benutzer werden in einer standardisierten Struktur verwaltet, die über geeignete Mechanismen verfügt um bei einer verteilten Datenhaltung eine einfache und sichere Verteilung oder Replikation der Benutzerinformationen zu gewährleisten (z.B. LDAP).
- Der Autorisierung sollte eine flexible und standardisierte Rechteverwaltung zu Grunde liegen. Zudem sollten die Zugriffe so eingeschränkt werden, dass sie eine individuelle

Sicherheitstiefe zulassen. Das bedeutet, dass es innerhalb der Rechtedefinition entsprechende Mechanismen braucht um situativ themen-, attribut- und funktionsbezogene Einschränkungen modellieren und durchsetzten zu können. Neben den thematischen Einschränkungen müssen auch die zeitlichen und räumlichen Aspekte abgebildet werden können (z.B. GeoXACML).

- Die Nutzung der Infrastruktur muss sowohl für authentifizierte als auch für herkömmliche Anfragen an Geo Web Services funktionieren. Dazu muss sichergestellt werden, dass die Authentifizierungsinformationen auch als „Vendor-specific Parameters“ (VSP) den regulären Dienstanfragen (REST-Methode) hinzugefügt werden können.

5.2 Beurteilung

5.2.1 Inhaltliche Beurteilung

Mit dem erarbeiteten Sicherheitsframework lassen sich die wesentlichen Sicherheitsfragen einer verteilten Systemarchitektur beantworten. Im Rückblick auf die eingangs definierten Ziele lässt sich festhalten, dass durch die Strukturierung der Sicherheitsaspekte und mit Hilfe der propagierten Massnahmen offene Web Services und GDIs in genügendem Masse abgesichert werden können. Aspekte die über diesen Kontext hinaus gehen, definieren Spezialverfahren die auf Grund von spezifischen Anforderungen weitere Sicherheitsmassnahmen erforderlich machen. Diese Aspekte befinden sich ausserhalb des gesetzten Rahmens dieser Master Thesis. Die Beurteilung der erarbeiteten Ergebnisse erfolgt auf Grund der anfangs definierten Thesen (vgl. Kap. 1.3).

1. **Zur ganzheitlichen Betrachtung der relevanten Sicherheitsaspekte ist ein übergeordnetes GDI-Sicherheitskonzepts erforderlich.**

Das Wissen über mögliche Angriffs- und Bedrohungsarten gepaart mit der Kenntnis der wichtigen Sicherheitsaspekte bilden die Ausgangslage für die Planung und Umsetzung von Sicherheitsmassnahmen. Erst wenn man Gewissheit hat, welche Aspekte es abzusichern gilt, lassen sich konkrete Massnahmen planen und geeignete Verfahren und Standards auswählen. Mit dem vorliegenden Sicherheitsframework werden die Anforderungen an eine sichere GDI benannt und konkrete Massnahmen zu deren Umsetzung vorgeschlagen. Dies ermöglicht es einer Entscheidungsinstanz auch mit begrenzten finanziellen und technischen Mitteln im

Bereich der IT-Sicherheit den Schutz vor Missbrauch zu gewährleisten. Den möglichen technischen und finanziellen Rahmenbedingungen wurde durch eine konsequente Nutzung offener und frei verfügbarer Standards und Spezifikationen Rechnung getragen. Durch die Betrachtung der existierenden Sicherheitsinitiativen deegree und 52°North wurde versucht den Nutzen der bereits bestehenden Open Source-basierten GDI-Komponenten hervorzuheben und deren Widerverwendung anzuregen.

2. **Die zur Verfügung stehenden Standards und Spezifikationen aus dem allgemeinen IT-Sicherheitsumfeld decken die Grundbedürfnisse für die Absicherung einer GDI weitestgehend ab. Die geo-räumlichen Zusatzanforderungen werden nur wo zwingend erforderlich durch ergänzende Spezifikationen vervollständigt.**

Die Standards und Spezifikationen aus dem allgemeinen IT-Umfeld erfüllen einen grossen Teil der Anforderungen an eine sichere GDI. Die Teilbereiche der Transport- und Nachrichtensicherheit basieren vollständig auf bereits etablierten Standards aus dem Bereich der IT-Sicherheit. Auch im Bereich der Authentifizierung lassen sich bestehende IT-Standards verwenden (SAML, LDAP etc.). Die geo-räumlichen Zusatzanforderungen lassen sich vor allem im Bereich der Autorisierung und der Zugriffsverwaltung identifizieren. Die Spezifikation von GeoXACML definiert zusätzlich zu den thematischen und zeitlichen auch die benötigten räumlichen Zugriffseinschränkungen. Im Rahmen des Accountings muss sicher gestellt sein, dass für die Nutzung des Dienstes auch die räumliche Ausprägung registriert und für die Preiskalkulation oder Onlinebestellung weiterverwendet wird.

3. **Im GDI-Umfeld sind feingranulare, rollenbasierte Kontrollmechanismen erforderlich damit eine thematische, zeitliche und räumliche Zugriffsbeschränkung garantiert werden kann.**

Die Zuweisung und Durchsetzung der Zugriffsrechte ist ein wichtiger Bereich des Sicherheitsframeworks, der im Rahmen der Autorisierung stattfindet. Die Autorisierung stellt sicher, dass eine Rolle die ihr zugewiesenen Information einsehen und beziehen kann. Die „Granularität“ der Abfrage ist dabei von grosser Bedeutung, da dadurch die Nutzungsrechte bedarfsgerecht vergeben werden können. Dies hat neben dem Aspekt der Sicherheit auch Einfluss auf die kommerzielle Nutzung der Infrastruktur. Jeder Benutzer, der in seiner zugewiesenen Rolle agiert, kann von der GDI genau die Informationen beziehen, für die er eine gültige thematische, zeitliche oder räumliche Berechtigung besitzt. Mit Hilfe von XACML und dessen Erweiterung für räumliche Kontrollmechanismen GeoXACML lassen sich diese Anforderungen erfüllen.

4. **Auch bei frei verfügbaren Geodatenbeständen die im Rahmen von GDIs veröffentlicht werden, sind Sicherheitsmassnahmen sinnvoll und generieren einen Mehrnutzen.**

Institutionen mit frei verfügbaren Geodatenbeständen könnten geneigt sein, das Thema Sicherheit nur am Rande zu betrachten, da die abzusichernden Geodaten nicht an eine kommerzielle Nutzung gebunden sind. Dabei wird aber vernachlässigt, dass der sichere Bezug von Geodaten auch den Aspekt der Verbindlichkeit beinhaltet. Dabei muss der Servicenutzer die Gewähr über die Ursprünglichkeit der Daten erhalten, was heisst, dass er sich darauf verlassen können muss, dass die Daten vom Datenanbieter stammen und von keinem anderen während oder nach dem Transport verändert wurden (Man-in-the-Middle-Angriff). Somit sollten auch für die Veröffentlichung von frei verfügbaren Geodatenbeständen die Massnahmen des GDI-Sicherheitsframeworks in Betracht gezogen werden. Die Verbindungssicherheit bildet auch hier die Basis für die weiteren Sicherheitsbemühungen. Auf der Ebene der Applikationssicherheit kann die Autorisierung gegebenenfalls vernachlässigt werden. Durch eindeutige Authentifizierung und ein entsprechendes Accounting lässt sich die Ausnutzung der GDI verfolgen. Dies dient zum einen der interessengerechten Publikation von Betriebs- oder Angebotshinweisen und hilft zum anderen bei der Überwachung und Optimierung der Servicenutzung.

5.2.2 Beurteilung der Methodik

Das Vorgehen im Rahmen dieser Master Thesis beinhaltete eine intensive Einarbeitung in die Sicherheitsthematik, was sich im Umfang des Literaturteils (Kap. 2) entsprechend widerspiegelt. Das Weglassen von Teilbereichen dieses Kapitels hätte Lücken in der Systematik des gewählten Vorgehens zur Folge gehabt, weshalb es in dieser ausführlichen Form belassen wurde. Eine weitere Herausforderung bestand darin, den gewählten Top-Down-Ansatz konsequent umzusetzen, da es auf Grund der Vielzahl von Spezifikationen schwierig war, sich deren Relevanz sicher zu sein. Es ist demnach trotz umfassender Analyse nicht auszuschliessen einfachere oder bessere Verfahren ausser Acht gelassen zu haben. Hilfreich war dabei die Fokussierung auf die beiden Initiativen deegree und 52°North die einen guten Einblick in bewährte GDI Open Source-Lösungen vermittelten. Gleichzeitig gilt es aber zu erwähnen, dass sich auch weitere Initiativen dieser Thematik angenommen haben und entsprechende Lösungen vorschlagen (z.B. DACS[94]).

[94] Distributed Access Control System: http://nfis.org (30.06.2007)

6. Zusammenfassung und Ausblick

Dieses Kapitel fasst die Inhalte der vorliegenden Master Thesis noch einmal zusammen (Kap. 6.1) und zeigt im Rahmen eines Ausblicks (Kap. 6.2) mögliche weitere Aspekte auf, die nicht oder nicht abschliessend betrachtet werden konnten oder bei einer Fortsetzung dieser Arbeit hilfreich sein können.

6.1 Zusammenfassung

Sicherheit ist ein wesentlicher Bestandteil einer jeden Geodateninfrastruktur, den es im Hinblick auf eine langfristige und nachhaltige kommerzielle Nutzung im Rahmen von Businessprozessen zu gewährleisten gilt. Der Grad an Sicherheit kann dabei sehr unterschiedlich sein und ist mitunter auch davon abhängig, wie gross die Risikotoleranz des Dienstanbieters ist und wie viel Aufwand er in die Absicherung der Dienste investieren kann und will. Im IT-Bereich sind die grundlegenden Aspekte von Sicherheit bekannt und es haben sich für einzelne Teilbereiche bereits Standards etabliert. Um die Sicherheit auch in verteilten Servicearchitekturen wie einer GDI gewährleisten zu können ist es wichtig, dass eine durchgehende Sicherheit garantiert wird. Denn auch hier gilt die Regel, dass eine sichere GDI nur so sicher ist, wie deren schwächste Komponente.

Im Rahmen des konzipierten Sicherheitsframeworks wurden die sicherheitsrelevanten Bereiche einer GDI aufgezeigt und in einem übergeordneten Gesamtkontext zusammengeführt. Dies ist deshalb von zentraler Bedeutung, weil sich dadurch für alle an einer GDI beteiligten Komponenten eine homogene und durchgehende Sicherheit gewährleisten lässt. Ausgehend von der Systemsicherheit der beteiligten Kommunikationspartner kann mit Hilfe der Verbindungssicherheit eine sichere Übertragung der Nachricht vom Sender zum Empfänger gewährleistet werden. Basierend auf der durchgehenden Verbindungssicherheit, lassen sich weitere

spezifische Sicherheitsmassnahmen für die Authentifizierung, die Autorisierung und das Accounting auf Applikationsstufe (Triple-A Services) etablieren.

Die Authentifizierung kann innerhalb der eigentlichen GDI oder ausserhalb stattfinden. Dazu muss jedoch gewährleistet sein, dass sich die Authentifizierungs- und Autorisierungsinstanzen kennen und vertrauen. Zudem muss es der GDI-Autorisierungsinstanz möglich sein, die Richtigkeit eines von der Authentifizierungsinstanz ausgestellten Tickets zu validieren. Dazu bedarf es einer zentralen interoperablen Sicherheitsinstanz die sowohl die Ressourcen und Rollen als auch die ihnen zugeordneten Regeln an einem zentralen Ort vorhält. Alle an einer GDI beteiligten Services können dadurch Autorisierungsentscheidungen an die entsprechende Komponente delegieren und sich auf die ihnen zugedachte Aufgabe konzentrieren. Dies bringt den Vorteil, dass die bestehenden OGC-Spezifikationen (WMS, WFS, etc.) nicht um sicherheitstechnische Zusätze angepasst oder erweitert werden müssen.

Triple-A Services können auch bei frei zugänglichen Ressourcen (Services und Geodaten) durchaus einen Mehrnutzen bringen. Zum einen kann durch das Monitoring eine missbräuchliche Servicenutzung festgestellt und verhindert werden. Zum anderen lassen sich durch das Wissen über die Servicenutzung auch entsprechende Analysen durchführen (Geo-Marketing, Data Mining) und allfällige Angebots- oder Prozessverbesserungen vornehmen.

6.2 Ausblick

Die Bestrebungen der OGC verdeutlichen die Relevanz einer standardisierten, interoperablen Sicherheitsvorgabe im Bereich von GDIs. Mit der Abstract Specification der Geospatial Digital Rights Management (GeoDRM) Working Group wurde ein erster Schritt für die Gewährleistung von Rechten für digitale Geodaten und Services gemacht. Durch die Entstehung der Security Working Group im Jahre 2006 ist in naher Zukunft auch in den Bereichen Authentifizierung, Zugriffskontrolle und Verschlüsselung mit konkreten Empfehlungen zu rechnen. Diese Entwicklung gilt es im Hinblick auf eine zeitgerechte Standardisierung der derzeit fehlenden GDI-Sicherheitskomponenten weiter zu beachten.

Im Bereich der Authentifizierung bietet sich die Nutzung von LDAP an. Die Eigenschaften von LDAP (verbreiteter IT-Standard, hohe Performance, Interoperabilität, Replizier- und Austauschbarkeit der Informationen) bringen es mit sich, dass der Einsatz dieses Verzeichnisdienstes auch für weitere Bereiche genutzt werden könnte. Auch die Autorisierung und das Accounting liessen sich mit LDAP bewerkstelligen. Als Austauschverfahren zwischen

den LDAP-Servern könnte dabei SAML für die Authentifizierung und GeoXACML für die Beschreibung der Zugriffsrechte verwendet werden. Ein kurzer Ausblick in die Funktionsweise von LDAP soll mit Anhang 1 (Anhang 1: LDAP) vermittelt werden.

Die prozessorientierte Sicht wurde im Rahmen dieser Arbeit bewusst ausgeklammert. Es wurde aber erwähnt, dass sich die Wirtschaftlichkeit von interaktiven und interoperablen Dienstleitungen erst dann in Wert setzen lässt, wenn sich die Sicherheitskomponenten auch in bestehende Geschäftsprozesse nahtlos integrieren lassen. In diesem Bereich würde sich die Adaption der Erkenntnisse dieser Arbeit auf die Information Technology Infrastructure Library (ITIL[95]) anbieten. ITIL ist der weltweite De-facto-Standard zur Beschreibung von Prozessen, die IT-Dienstleister implementieren müssen, um IT Services erfolgreich zu betreiben (Brunnstein, 2006).

Zum Schluss bleibt der Wunsch, mit den Ergebnissen dieser Arbeit das Bewusstsein bei Entscheidungsträgern im Bereich von GDIs geschärft zu haben, dass eine ganzheitliche Sicherheitsbetrachtung eine essentielle Voraussetzung für die nachhaltige und zuverlässige Nutzung von Geodaten in verteilten Architekturen darstellt. Diesen Anforderungen gilt es bereits bei der Konzeption der Infrastruktur mit geeigneten Massnahmen Rechnung zu tragen. Damit steigt die Transparenz und Beherrschbarkeit der Sicherheit innerhalb einer GDI und gleichzeitig minimiert sich das Risiko eine Bedrohung zu übersehen.

> „Es ist ein allgemeiner Fehler der Menschen, nicht in den Zeiten der Meeresstille mit dem Sturm zu rechnen."
>
> *Niccolò Machiavelli (1469 - 1527)*

[95] IT Infrastructure Library des Office of Governance Commerce, Norwich: http://www.itil.org (30.06.2007)

7. Literaturverzeichnis

Abbie, 2003	ABBIE, B., (2003): Web Services Security: An Enabler of Semantic Web Services http://www.cs.unb.ca/baseweb/baseweb03/papers/abbie-barbir-BaseWeb2003-paper1.pdf (30.06.2007)
AM Consult, 2005	AM CONSULT: GeoXACML Documentation (2005). http://www.geoxacml.org/documentation (30.06.2007)
Bakom, 2003	BAKOM, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation; Bundesamt für Kommunikation: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (2003) http://www.admin.ch/ch/d/ff/2003/8221.pdf (30.06.2007)
Bakom, 2004a	BAKOM, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation; Bundesamt für Kommunikation: Inkrafttreten des Bundesgesetzes über die elektronische Signatur (2004) http://www.bakom.ch/dokumentation/medieninformationen/00471/index.html?lang=de&msg-id=2002 (30.06.2007)
Bakom, 2004b	BAKOM, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation; Bundesamt für Kommunikation: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (2004) http://www.admin.ch/ch/d/sr/9/943.032.de.pdf (30.06.2007)
Bakom, 2006	BAKOM, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation; Bundesamt für Kommunikation: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (2006) http://www.bakom.admin.ch/themen/internet/00467 (30.06.2007)
Bernhard et al., 2002	BERNHARD, L., STREIT, U., (2002): Geodateninfrastrukturen und Geoinformationsdienste: Aktueller Stand und Forschungsprobleme. Publikationen der Deutschen Gesellschaft für Photogrammetrie und

	Fernerkundung (Band 11): S. 11-20
Brunnstein, 2006	BRUNNSTEIN, J., (2006): ITIL-Security-Management realisieren: IT-Service Security-Management nach ITIL - so gehen Sie vor, Vieweg Verlag, 168 S.
degree, 2007	DEEGREE, Free Software for Spatial Data Infrastructures (2007): http://www.deegree.org (30.06.2007)
Dostal et al., 2004	DOSTAL, W., JECKLE, M., (2004): Semantik, Odem einer Service-orientierten Architektur, Java Spektrum (1/2004), Seiten 53-56
Drew, 2004	DREW, M., (2004): Eine Einführung in die Sitepersonalisierung durch Microsoft Passport (Microsoft Corporation) http://www.microsoft.com/germany/msdn/library/net/aspnet/EineEinfuehrungInDieSitepersonalisierungDurchMicrosoftPassport.mspx (30.06.2007)
Drewnak et al., 2002	DREWNAK, J., GARTMANN, R., JUNGERMANN, F., (2003): Testbed II - Web Authentication Service www.gdi-nrw.org (30.06.2007)
Drewnak, 2003	DREWNAK, J., (2003): Authentifizierung und Autorisierung in Geodateninfrastrukturen am Beispiel der GDI NRW, Diplomarbeit am Institut für Geoinformatik Universität Münster, 92 S. http://ifgi.uni-muenster.de/downloads/diplomarbeiten_intern/Drewnak/sjfioewtr6t446etr46tr64trerw.pdf (30.06.2007)
Drewnak et al., 2005	DREWNAK, J., GARTMANN, R., (2005): Zugriffsschutz in Geodateninfrastrukturen, S.140-144 in WAGNER, R., BERNHARD, L., FRITZKE, J., (2005): Geodateninfrastruktur. Grundlagen und Anwendungen, Wichmann Verlag, Heidelberg, 311 S.
Eckert, 2006	ECKERT, C., (2006): IT-Sicherheit, Oldenbourg Verlag München, 4. Auflage, 918 S.
FIPS, 1999	FIPS, National Institute of Standards and Technology U.S. Department of Commerce: Federal Information Processing Standards Publication (FIPS): Data Encryption Standard (DES); FIPS Pub 46-3 (1999) http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (30.06.2007)
Flückiger et al., 2004	FLÜCKIGER, U., ANGST, D., BÜHLER, W., EUGSTER, R., LIECHTI, M., SÄGESSER, E., KELLER, S., BURGHARDT, D., (2004): Sicherheitsaspekte bei Web-GIS Lösungen. Bericht der Fachgruppe GIS-Technologie SOGI, 44 S. http://www.sogi.ch/sogi/Technologie2.pdf (30.06.2007)
Friedmann, 2006	FRIEDMANN, T., (2006): Die Welt ist flach - Eine kurze Geschichte des 21. Jahrhunderts, Suhrkamp Verlag, 1. Auflage, 710 S.

Groot et al., 2000 — GROOT, R., MCLAUGHLIN, J., (2000): Geospatial data infrastructure - Concepts, cases, and good practice, Oxford University Press, 320 S.

Hauser et al., 2004 — HAUSER, T., LÖWER U.M. (2004) Web Services - Die Standards, Galileo Press, 1. Auflage, 234 S.

Hey, 2005 — HEY, R., (2005): Entwicklung einer XML-basierten Authentifizierungsmethode für mobile Netze der vierten Generation; Diplomarbeit am Institut für Informatik der Universität München, 108 S. http://www.pms.ifi.lmu.de/publikationen/diplomarbeiten/Thomas_Robert.Hey/DA_Thomas_Robert.Hey.pdf (30.06.2007)

Howes et al., 2005 — HOWES, T., SMITH M., GOOD G., (2005): Understanding and Deploying LDAP Directory Services, Addison-Wesley, 2nd Edition, 936 S.

IBM, 2002 — IBM, Microsoft, VeriSign (2002): WS-Security Profile for XML-based Tokens http://www-128.ibm.com/developerworks/library/specification/ws-sectoken (30.06.2007)

IBM et al., 2005a — IBM, BEA Systems, Microsoft, Layer 7 Technologies, Oblix, VeriSign, Actional, Computer Associates, OpenNetwork Technologies, Ping Identity, Reactivity, RSA Security (2005): Web Services Trust Language http://www-128.ibm.com/developerworks/library/specification/ws-trust (30.06.2007)

IBM et al., 2005b — IBM, Microsoft, RSA Security, VeriSign (2005): Web Services Security Policy Language http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secpol (30.06.2007)

IBM et al., 2005c — IBM, BEA Systems, Microsoft, Computer Associates, Actional, VeriSign, Layer 7 Technologies, Oblix, OpenNetwork Technologies, Ping Identity, Reactivity, RSA Security (2005): Web Services Secure Conversation Language http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secon (30.06.2007)

IBM et al., 2006 — IBM, BEA Systems, Microsoft, SAP AG, Sonic Software, VeriSign (2006): Web Services Policy Framework http://www-128.ibm.com/developerworks/webservices/library/specification/ws-polfram (30.06.2007)

IBM et al., 2007 — BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, VeriSign (2007): Web Services Federation Language

http://www-128.ibm.com/developerworks/library/specification/ws-fed (23.04.2007)

IDEA, 2005 — MEDIACRYPT AG.: International Data Encryption Algorithm (IDEA): Technical Description (2005) http://www.mediacrypt.com/_pdf/IDEA_Technical_Description_0105.pdf (30.06.2007)

IETF, 1996a — IETF, Internet Engineering Task Force, Transport Layer Security Working Group: The SSL Protocol, Version 3.0 (1996) http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00 (30.06.2007)

IETF, 1996b — IETF, Internet Engineering Task Force, Transport Layer Security Working Group: Multipurpose Internet Mail Extensions (MIME) Part One (1996) http://www.ietf.org/rfc/rfc2045.txt (30.06.2007)

IETF, 1998 — IETF, Internet Engineering Task Force, Network Working Group: Security Architecture for the Internet Protocol (1998) http://www.ietf.org/rfc/rfc2401.txt (30.06.2007)

IETF, 1999a — IETF, Internet Engineering Task Force, Network Working Group: The TLS Protocol (1999) http://www.ietf.org/rfc/rfc2246.txt (30.06.2007)

IETF, 1999b — IETF, Internet Engineering Task Force, Network Working Group: Diffie-Hellman Key Agreement Method (1999) http://www.ietf.org/rfc/rfc2631.txt (30.06.2007)

IETF, 2002 — IETF, Internet Engineering Task Force, Network Working Group: XML-Signature Syntax and Processing (2002) http://www.ietf.org/rfc/rfc3275.txt (30.06.2007)

ISO, 1989 — ISO, International Organization for Standardization: Information processing systems - Open Systems Interconnection - Basic Reference Model -- Part 2: Security Architecture (1989) http://www.iso.org (30.06.2007)

ITU-T, 2005 — ITU-T, International Telecommunication Union; Telecommunication Standardization Sector: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks - X.509 (2005) http://www.itu.int/rec/T-REC-X.509/en (30.06.2007)

KOGIS, 2007 — KOGIS, Koordinationsorgan für Geoinformation und geografische Informationssysteme des Bundes (2007). http://www.e-geo.ch/NGDI_d.htm (30.06.2007)

lat/lon, 2007 — LAT/LON, GmbH für raumbezogene Informationssysteme (2007) http://www.lat-lon.de (30.06.2007)

Liberty, 2006	LIBERTY ALLIANCE, ID-WSF 2.0 Specifications (2006) http://www.projectliberty.org/resource_center/specifications (30.06.2007)
Mahmoud, 2005	MAHMOUD, Q., (2005): Securing Web Services and the Java WSDP 1.5 XWS-Security Framework http://java.sun.com/developer/technicalArticles/WebServices/security/index.html (30.06.2007)
Matheus, 2005	MATHEUS, A.,: Declaration and Enforcement of Access Restrictions for Distributed Geospatial Information Objects (2005), Dissertation an der Fakultät für Informatik der TU München, 238 S. http://tumb1.biblio.tu-muenchen.de/publ/diss/in/2005/matheus.pdf (30.06.2007)
Melzer et al., 2007	MELZER, I.,: Service-orientierte Architekturen mit Web Services: Konzepte - Standards - Praxis (2007) Spektrum Akademischer Verlag, 2. Auflage, 359 S.
Muster, 2006	MUSTER, D., (2006): Digitale Unterschriften und PKI - Eine Einführung in die modernen Sicherheitsverfahren und deren Problemfelder; Hochschule für Technik Zürich, 3. Auflage, 549 S.
Nebert et.al. 2006	NEBERT, D., REED, C., WAGNER, R., (2006) Proposal for a Compatible SDI Standards Suite, “SDI 1.0”; Research and Theory in Advancing Spatial Data Infrastructure Concepts (preprint); 15 S. http://gsdidocs.org/gsdiconf/GSDI-9/papers/TS19.1paper.pdf (30.06.2007)
OASIS, 2005a	OASIS, Organization for the Advancement of Structured Information Standards: eXtensible Access Control Markup Language TC v2.0 (2005) http://www.oasis-open.org/specs/index.php#xacmlv2.0 (30.06.2007)
OASIS, 2005b	OASIS, Organization for the Advancement of Structured Information Standards: Security Assertion Markup Language (SAML) v2.0 (2005) http://www.oasis-open.org/specs/index.php#samlv2.0 (30.06.2007)
OASIS, 2005c	OASIS, Organization for the Advancement of Structured Information Standards: Assertions and Protocols for the OASIS Security Assertion Markup Language (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (30.06.2007)
OASIS, 2005d	OASIS, Organization for the Advancement of Structured Information Standards: Bindings for the OASIS Security Assertion Markup Language (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf (30.06.2007)
OASIS, 2005e	OASIS, Organization for the Advancement of Structured Information Standards: Profiles for the OASIS Security Assertion Markup Language

(2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
(30.06.2007)

OASIS, 2005f — OASIS, Organization for the Advancement of Structured Information Standards: Glossary for the Security Assertion Markup Language (SAML) V2.0 (2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf
(30.06.2007)

OASIS, 2005g — OASIS, Organization for the Advancement of Structured Information Standards: Authentication Context for the Security Assertion Markup Language (SAML) V2.0 (2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf (30.06.2007)

OASIS, 2005h — OASIS, Organization for the Advancement of Structured Information Standards: Security and Privacy Considerations for the OASIS Security Assertion Markup Language (2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf
(30.06.2007)

OASIS, 2005i — OASIS, Organization for the Advancement of Structured Information Standards: Conformance Requirements for the OASIS Security Assertion Markup Language (2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf
(30.06.2007)

OASIS, 2005k — OASIS, Organization for the Advancement of Structured Information Standards: Metadata for the OASIS Security Assertion Markup Language (2005)
http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
(30.06.2007)

OASIS, 2006a — OASIS, Organization for the Advancement of Structured Information Standards: Security Assertion Markup Language (SAML) V2.0 Technical Overview; Working Draft 10; (2006)
http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf (30.06.2007)

OASIS, 2006b — OASIS, Organization for the Advancement of Structured Information Standards: Web Services Security: SOAP Message Security 1.1 (2006)
http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf (30.06.2007)

OASIS, 2006c — OASIS, Organization for the Advancement of Structured Information Standards: Username Token Profile 1.1 (2006)
http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-

spec-os-UsernameTokenProfile.pdf (30.06.2007)

OASIS, 2006d — OASIS, Organization for the Advancement of Structured Information Standards: X.509 Token Profile 1.1 (2006) http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf (30.06.2007)

OASIS, 2006e — OASIS, Organization for the Advancement of Structured Information Standards: SAML Token profile 1.1 (2006) http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf (30.06.2007)

OASIS, 2006f — OASIS, Organization for the Advancement of Structured Information Standards: Kerberos Token Profile 1.1 (2006) http://www.oasis-open.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf (30.06.2007)

OGC, 2002 — OGC, Open Geospatial Consortium Inc. (2002): Web Pricing & Ordering Service (WPOS) XML Configuration & Pricing Format (XCPF), Version: 0.2 http://portal.opengeospatial.org/files/?artifact_id=11500 (30.06.2007)

OGC, 2005a — OGC, Open Geospatial Consortium Inc. (2005): Web Feature Service Implementation Specification, Version: 1.1.0 http://www.opengeospatial.org/standards/wfs (30.06.2007)

OGC, 2005b — OGC, Open Geospatial Consortium Inc. (2005): OpenGIS® Filter Encoding Implementation Specification, Version: 1.1.0 http://www.opengeospatial.org/standards/filter (30.06.2007)

OGC, 2005c — OGC, Open Geospatial Consortium Inc. (2005): OGC™ Catalogue Services Specification, Version: 2.0.2 http://www.opengeospatial.org/standards/cat (30.06.2007)

OGC, 2005d — OGC, Open Geospatial Consortium Inc. (2005): OpenGIS® Web Processing Service, Discussion Paper, Version: 0.4.0 http://portal.opengeospatial.org/files/?artifact_id=13149&version=1&format=pdf (30.06.2007)

OGC, 2005e — OGC, Open Geospatial Consortium Inc. (2005): GeoXACML, a spatial extension to XACML, OGC Discussion Paper, Doc-ID 05-036 http://portal.opengeospatial.org/files/index.php?artifact_id=10471 (30.06.2007)

OGC, 2006a — OGC, Open Geospatial Consortium Inc. (2006): OpenGIS® Web Map Server Implementation Specification, Version: 1.3.0 http://www.opengeospatial.org/standards/wms (30.06.2007)

OGC, 2006b — OGC, Open Geospatial Consortium Inc. (2006): Geospatial Digital Rights

	Management Reference Model (GeoDRM RM, 06-004r3), Abstract Specification, Version: 1.0.0 http://www.opengeospatial.org/standards/as/geodrmrm (30.06.2007)
OGC, 2006c	OGC, Open Geospatial Consortium Inc. (2006): Web Coverage Service (WCS) Implementation Specification, Version: 1.1.0 http://www.opengeospatial.org/standards/wcs (30.06.2007)
OGC, 2007a	OGC, Open Geospatial Consortium, Inc. (2007): FAQ - OGC and "Openness" http://www.opengeospatial.org/ogc/faq/openness (30.06.2007)
OGC, 2007b	OGC, Open Geospatial Consortium, Inc. (2007): Security WG http://www.opengeospatial.org/projects/groups/securitywg (30.06.2007)
Rajabifard et al., 2002	RAJABIFARD, A., FEENEY, M.E. and WILLIAMSON I.P. (2002): Directions for the Future of SDI Development http://eprints.infodiv.unimelb.edu.au/archive/00001254/02/ITC_Journal_2002.pdf (30.06.2007)
RSA, 2002	RSA Security Inc.: Public-Key Cryptography Standards (PKCS #1): RSA Cryptography Standard (2002) ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf (30.06.2007)
Rummeyer et al., 2006	RUMMEYER, O., DÜSTERHAUS, J., (2006): SSO frei Haus - Einfache Lösungen zur Implementierung von Single Sign-on http://entwickler.de/zonen/portale/psecom,id,101,online,910,p,0.html (30.06.2007)
Saraha et al., 2006	SARAHA, H., FARISS, N., (2006): Sicherheit in Webservices; Technische Universität Darmstadt, 29 S. http://www.st.informatik.tu-darmstadt.de/database/seminars/data/Sicherheit%20in%20Webservices.pdf?id=218 (30.06.2007)
Schmidt, 2006	SCHMIDT, K. (2006): Der IT Security Manager. Hanser Fachbuchverlag München; 1. Auflage, 308 S.
Shah, 2007	SHAH, S. (2007): Hacking Web Services, Charles River Media, 1st Edition, 352 S.
Shirey, 2000	SHIREY, R., (2000): Internet Security Glossary http://www.faqs.org/rfcs/rfc2828.html (30.06.2007)
SOGIS, 2003	SOGIS, Schweizerische Organisation für Geo-Information, Bericht der Fachgruppe GIS-Technologie: Worin liegt der praktische Nutzen von Interoperabilität und Normung für den GIS-Anwender in der Schweiz? (2003), http://www.sogi.ch/sogi/Technologie1.pdf (30.06.2007)

Stark et al. 2006	STARK H.-J., SCHÜTZ S, ANNEN A. WIEDMER H. U., (2006): Anwendungsprofil Geodienste, Version 1.0, 100 S. http://www.ech.ch/index.php?option=com_docman&task=doc_download&gid=789&lang=de (30.06.2007)
W3C, 2002a	World Wide Web Consortium (W3C); XML-Signature Syntax and Processing; W3C Recommendation (2002) http://www.w3.org/TR/xmldsig-core (30.06.2007)
W3C, 2002b	World Wide Web Consortium (W3C); XML-Encryption Syntax and Processing; W3C Recommendation (2002) http://www.w3.org/TR/xmlenc-core (30.06.2007)
W3Schools, 2007	W3SCHOOLS, Refsnes Data (2007) http://www.w3schools.com/wsdl/default.asp (30.06.2007)
Wikipedia, 2007	WIKIPEDIA - The Free Encyclopedia http://www.wikipedia.org (30.06.2007)
52°North, 2007	52°NORTH - Geospatial Open Source Software GmbH (2007) http://52north.org (30.06.2007)

Anhang 1: LDAP

Das Lightweight Directory Access Protocol (LDAP[96]) ist ein standardisiertes, erweiterbares Internet Protokoll für den Zugriff auf Verzeichnisdienste (engl. Directory Services). LDAP beschreibt einen objektorientierten Ansatz wie die Informationen von und über Organisationen (Personen- und Infrastrukturdaten) in kontrollierter Form über Datenkommunikationsnetze verfügbar gemacht werden können. Dabei ist nicht der Verzeichnisdienst selbst standardisiert, sondern die Zugriffsmethoden über die Datenkommunikationsnetze. LDAP setzt auf dem TCP/IP Protokoll und besteht aus den folgenden vier Modellen (Howes et al. 2005):

- Das Informationsmodell (engl. information model) beschreibt welche Informationen in ein LDAP-Verzeichnis eingefügt werden können. Es definiert die Entitäten, Attribute und Werte der einzelnen LDAP-Objekte.
- Das Namensmodell (engl. naming model) beschreibt wie Verzeichnisdaten von LDAP organisiert sind und wie darauf zugegriffen werden kann. LDAP basiert auf einer invertierten Verzeichnisbaum bei dem ausgehend von einem root-Objekt alle weiteren Objekte hierarchischen angeordnet sind (vgl. Abb. 38).

[96] Lightweight Directory Access Protocol: http://www.ietf.org/rfc/rfc4511.txt (30.06.2007)

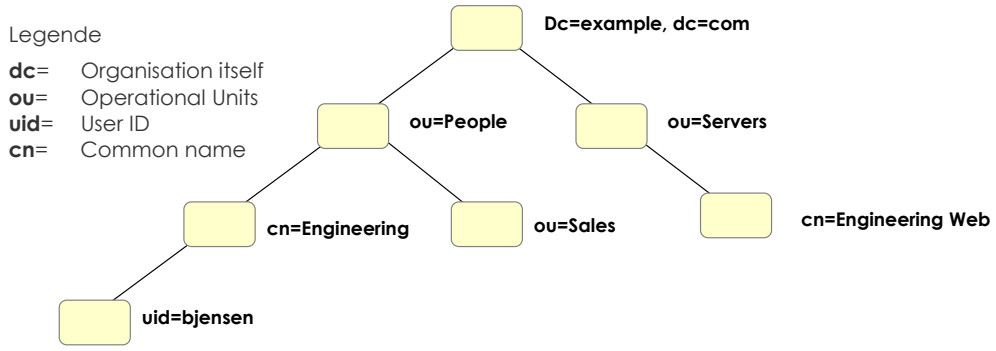

Abb. 38: Beispiel eines LDAP Verzeichnisbaums (nach Howes et al., 2005)

- Das Funktionsmodell (engl. functional model) deklariert was mit LDAP-Verzeichnisdaten getan werden kann und darf.
- Das Sicherheitsmodell (engl. security model) beschreibt wie LDAP-Verzeichnisdaten vor unberechtigtem Zugriff geschützt werden können.

Um die Struktur von LDAP zu verstehen, ist es wichtig die Funktionsweise eines Verzeichnisdienstes zu kennen. Ein Verzeichnisdienst funktioniert in seinen Grundzügen ähnlich wie eine Datenbank, unterscheidet sich aber in seinem Aufbau und seinen Eigenschaften ganz grundlegend von dieser. Ein Verzeichnis kann vereinfacht als eine hierarchische Struktur (Baumstruktur) von Tabellen verstanden werden, die für den schnellen Lesezugriff ausgelegt ist. Eine Tabelle beschreibt jeweils eine Objekteinheit (engl. entry) und enthält Attribute. Verzeichnisdienste können über einen standardisierten Zugriff (Protokoll) effizient und schnell nach Entries und Attributen durchsucht (respektive traversiert) werden und sind daher geeignet für eindimensionale Abfragen aller Art. Durch ihre hierarchische Struktur lassen sich Verzeichnisdienste auch einfach auf mehre Server und Netzwerke verteilen (redundante Speicherung an mehreren Standorten) und replizieren (Datenabgleich zwischen den Standorten).

LDAP ist ein nachrichtenorientiertes Verfahren, bei dem ein LDAP-Client eine Suchanfrage and den Directory Server (LDAP-Server) sendet. Der LDAP Server sucht das Verzeichnis nach möglichen Objekten ab, die den gewünschten Suchkriterien entsprechen und sendet diese an den Client. Das Verfahren einer typischen LDAP-Anfrage (vgl. Abb. 39) funktioniert wie folgt:

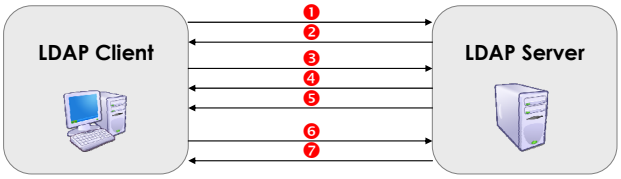

Abb. 39: Verfahren einer typischen LDAP-Anfrage (nach Howes et al., 2005)

1. Der Client öffnet eine TCP-Verbindung zum Server und übermittelt mittels einer `bind`-Operation seine Credentials (Zertifikat, Passwort) zusammen mit der URL des LDAP Servers (Port 389) auf den er sich authentifizieren möchte.
2. Der LDAP Server verifiziert die Credentials (Zertifikat, Passwort) und gibt eine Rückmeldung, dass die Authentifizierung erfolgreich war.
3. Der Client setzt die gewünschte Suchanfrage ab (`search`-Operation).
4. Der Server prozessiert die Suchanfrage und sendet jeweils eine Nachricht für jeden gefundenen Eintrag (Objekt) an den Client zurück.
5. Der Server sendet neben den gefundenen Objekten auch eine Resultatmeldung der Such-Operation an den Client zurück.
6. Der LDAP-Client teilt dem Server mittels einer `unbind`-Operation mit, dass er die geöffnete TCP-Verbindung beenden möchte.
7. Der Server beendet die Verbindung und bestätigt dies dem Client.

LDAP wird auf Grund seiner Einfachheit von den meisten Verzeichnisdiensten (u.a. Microsoft, Apple, Sun, Novell, Oracle, uvm.) unterstützt und wird vor allem für die Benutzer- und Ressourcenverwaltung eingesetzt. LDAP eignet sich sowohl für die Verwaltung von lokalen Domänenressourcen als auch für die Zugriffsverwaltung von verteilten Web Services. Die Vor- und Nachteile von LDAP sind in der nachfolgenden Tabelle gegenübergestellt (Wikipedia, 2007).

Vorteile	Nachteile
▪ LDAP-Verzeichnisse sind für den schnellen Lesezugriff optimiert. ▪ LDAP ist auf Authentifizierungs- und Autorisierungsabfragen optimiert. ▪ LDAP ermöglicht eine verteilte Datenhaltung und Replikation und bietet damit eine hohe Verfügbarkeit ohne komplexe Konfiguration. ▪ LDAP basiert auf einem flexiblen, objektorientierten Datenmodell, das sich einfach und schnell erweitern lässt.	▪ LDAP kennt keine Normalform wie eine herkömmliche Datenbank. Daher können Attribute auch mehrere, unterschiedliche Werte enthalten. ▪ Relationale Operationen werden - mit Ausnahme der Projektion (Spaltenauswahl) - nicht unterstützt.

Tab. 17: Vor- und Nachteile von LDAP

Ein weiterer wesentlicher Vorteil von LDAP ist, dass es neben der Authentifizierung und Autorisierung auch für das Accounting verwendet werden kann. Mit der LDAP-Erweiterung SASL (Simple Authentication and Security Layer) steht zudem ein erweiterbares Format für die Unterstützung von verschiedensten Authentifikationsmethoden zur Verfügung. Für weitere Angaben zu LDAP sei an dieser Stelle auf (Howes et al., 2005) verwiesen.

[eof]