Entwicklung sicherheitstechnischer Architekturen für mobile Geoinformationsdienste

NICO SCHEITHAUER[1] HERMANN STRACK THOMAS SPANGENBERG , HARDY PUNDT

Hochschule Harz,, FB Automatisierung und Informatik
D-38855 Wernigerode, nscheithauer | tspangenberg | hpundt | hstrack@hs-harz.de

Abstract. Es wird ein Überblick über die Zielstellungen des SecInfPro-Geo-Projektes gegeben. Die Konzeption von integrierbaren Sicherheitsarchitekturen und -diensten für mobile Geoinformationssysteme und Anwendungsszenarien wird vorgestellt. Für ortsabhängige Zugriffsautorisierungen und -kontrollen mit Delegation werden Erweiterungen auf SAML- und WebService-Basis vorgestellt (für Location based Services LBS).

Keywords.OGC, GIS, Security, OSCI, XML-Signature, LBA???, LBS,WSS, SOA

Einleitung

Das Kompetenzzentrumsprojekt „*Security ,Infrastructures and Process Integration*" (SecInfPro) stellt für sicherheitssensitive elektronische (interaktive) Verfahrens-, Workflow- und Dienste- Szenarien die Integration geeigneter Sicherheitsdienste auf Basis von Standards bereit. Zusammen mit dem Kompetenzzentrumsprojekt *KliK-KOGITON* werden im Kooperationsvorhaben "*SecInfPro-Geo*" Sicherheitsintegrationen für Geoinformationssysteme (GIS) entwickelt. Zweck und Motivation ist die gesicherte, authentisierte sowie autorisierte Erfassung, Verwaltung, Nutzung, Analyse und Modellierung raumbezogener Daten und deren Beziehungen zu einander in mobilen Szenarien. Nachfolgend werden Sicherheitsintegrationen und – Architekturen für GIS in mobilen Szenarien vorgestellt. Das Kompetenzzentrum (KAT) für Informations- und Kommunikationstechnologien wird seit Jahren an der Hochschule Harz vom Land Sachsen-Anhalt gefördert.

[1]Corresponding Author.

1. Mobile Geodienste-Szenarien und Sicherheitsanforderungen

1.1. Szenarien und Motivation

Ziel ist es, in Zusammenarbeit mit dem Projekt *KliK-KOGITON* (Anwendungsszenarien z.B.: Mobile Tourenplanung) die gesicherte Integration (mobiler) Geoinformations-Dienste in SecInfPro-Geo zu untersuchen und diese beispielhaft zu realisieren. Dazu werden hier zur Illustration verschiedene Sicherheitsanforderungen für mobile Geo-Dienste für folgende Anwendungsszenarien betrachtet:

- „Autorisiertes POI-Touren-Marketing“ (AUTOM):
  Das Szenario sieht für gezieltes, regionales touristisches Standortmarketing vor, dass nur die autorisierte Pflege von POI-Kartendaten ermöglicht wird und dieses auf Basis von gesicherten Quellennachweisen nachvollzogen wird. Nur präregistrierte Nutzer, die authentisiert und autorisiert sind, dürfen die POI auf Kartenausschnitten ergänzen, ggf. mit zusätzlichen standortbezogenen Autorisierungen.
- „Verbindliche Touristische Rufbus-Planung“ (TOURBUS):
  Das Szenario beschreibt eine Möglichkeit für verschiedene Nutzer, die sich mittels des neuen Personalausweises (nPA) präregistriert haben, verbindliche Tourziele an verschiedenen Standorten für Rufbus-Touren mobil und nachweisbar zu buchen. Hierfür werden die Zieleinträge für die Tour anhand prä-registrierter gesicherter Nutzerdaten authentisiert. Dieses Verfahren ist auch auf Anwendungen in der Logistik übertragbar. Tourenpunkte können so auf verbindlicher Vertragsbasis für vorher authentisierte Nutzer angefahren werden.
- „Mobiles Immobilien-Makeln“(MobImM):
  Ein Immobilien/Grundstücks-Makler möchte seine Dienste (mobil) elektronisieren und mit elektronischen Dienste-Mehrwerten versehen zur Verbreiterung seines potentiellen Kundenkreises, dabei jedoch seine Immobilien-Informationen für Besichtigungen nur an komplett vorauthentisierte und registrierte Kunden herausgeben, um den Missbrauch seiner Immobiliendaten zu verhindern (entgangene Courtage). Zur Erleichterung der Vorregistrierung der Kunden soll diese auch remote erfolgen können. Für weitere Mehrwertdienste soll die autorisierte selektive Abrufung von Kartendaten aus geschützten Liegenschaftsregistern standortbezogen nur für wirklich interessierte Kunden ermöglicht werden (z.B. aus ALKIS) bei nachgewiesenem berechtigten Interesse, nur für Kunden, die sich vor Ort auf der Liegenschaft befinden.

1.2. Sicherheitsanforderungen

Grundlegende Ziele für die Sicherheit von Geoinformationssystemen unter dem Gesichtspunkt von Datenschutz, Daten- und Dienste-Sicherheit können wie folgt zusammengefasst werden:

S1. Vertraulichkeit (Verhindern der Offenlegung von sensiblen Geo-Daten)
S2. Integrität (Gewährleistung nur autorisierter Änderungen und ansonsten von Unversehrtheit)
S3. Authentizität und Autorisierung (Nachweisbarkeit und Kontrolle der Identität von Zugreifenden, insbesondere für autorisierte Karten-Editoren/Gestalter, sowie von deren Autorisierungen sowie ggf. auch von mobilen Standort-Credentials und im Ergebnis von den durchgeführten Karten-Updates (Quellennachweise))

S4. Verbindlichkeit/Nichtabstreitbarkeit: Nachweisbare Zustellung von (integren) Kartendaten an autorisierte Kunden/Zugreifende.

Von besonderem Interesse sind solche Sicherheitsanforderungen zum einen hinsichtlich von lesenden "Kartenzugriffen" von "Karten-Nutzern" eines Kartendienste-Anbieters, zum anderen hinsichtlich von "Karten-Editoren" (z.B. im Auftrag des Providers). Diese Sicherheitsanforderungen sind von besonderem Interesse beim "Verschneiden" von GIS-Daten verschiedener Akteure/Quellen für ein "kombiniertes" Kartensystem, unter Berücksichtigung auch von standortbezogenen Autorisierungs-Credentials für Berechtigungen (auch für Location based Services LBS).

2. Sicherheitsarchitekturen und Integration gesicherter Dienste

Für GIS-Architekturen existieren verschiedene Ansätze mit ähnlichen Zugriffsprofilen und Services. Das ALKIS-Datenmodell sieht z.B. hier verschiedene Prozeduren für das Abrufen, Eintragen und Speichern der GIS-Daten vor. Hier hat sich ein vom OGC standardisiertes Format auf Basis von XML etabliert. Die Geographic Markup Language (GML) dient hier zum einen für den Transport sowie zur temporären Haltung von Geo-Daten. Ein GML-zentrales Element ist das Feature Element, welches es erlaubt, eigene Objekt der realen Welt zu definieren. Für einen normbasierten Datenaustausch kommt die Austauschschnittstelle NAS zur Anwendung, welche verschiedene Operationen unterstützt (Sperrung, Reservierung, Benutzung). Die Verschneidung, also das Kombinieren verschiedener Karten-Daten unterschiedlicher Autoren, ist durch den XML-basierten Aufbau von GML flexibel umsetzbar. Sicherheitsfunktionalität soll vor dem Hintergrund von Abschnitt 1 geeignet integriert werden.

2.1. Sicherheitsarchitekturen, -funktionen und Standards

In Vorgängerprojekten wurden bereits Sicherheitsarchitekturen im Bereich eGovernment und eBusiness entwickelt [6-8], auf Basis der Integration von Internet-Security-Standards wie „Secure WebServices" und von eGovernment-Standards, wie PKI nach Signaturgesetz, wie Telesignaturserver für rechtsverbindliche qualifizierte "Massensignaturen", wie OSCI für rechtsverbindlich nachweisbare und datenschutzkonforme Nachrichten- und Dokumenten-Zustellungen in XÖV [5] und wie des neuen Ausweises (nPA) für datenschutzkonforme Nutzer-Authentisierungen und qual. Signaturen. Vor diesem Hintergrund wird nun hier ein Transfer von Sicherheitsstrukturen für den kartenbasierten GIS-Bereich vorgeschlagen. Von besonderem Interesse ist hier zunächst die Unterscheidung nach Art von Sicherheits-Integrationsvarianten: es werden sogenannte **Shell-Architekturen** (Security-Umhüllung/Ergänzung der herkömmlichen Systemarchitektur durch Sicherheitsschalen/Funktionen/Speicher, ohne oder nur mit "minimal invasiven" Eingriffen in die bisherigen Systemschnittstellen/strukturen) von **Builtin-Architekturen** unterschieden [8] (direkte Integration von Sicherheitsfunktionalität mit Eingriff/Updates der herkömmlichen Systemschnittstellen/Architekturen, d.h. z.B. unter Verlust von bisheriger Standardkonformität).

2.2. Komponenten und Funktionen zur Sicherheitsintegration

Auf Basis der Orientierung nach Internetstandards wie SOAP, SAML, XML, Web Service Security und Web-Interfaces kann mit den folgenden Komponenten eine flexible und transparente Sicherheitsintegration nach Shell-Architekturansatz als auch (dann aufwändiger) nach Builtin-Architekturansatz für web-basierte Ausgangsarchitekturen geleistet werden, wie bereits in [8] gezeigt.

OSCI: SOAP-basiertes eGovernment-Transportprotokoll/Standard mit signierten Zustellquittungen, Signaturintegration und Ende-zu-Ende-Sicherheit durch integrierte Verschlüsselungen (von Datenschutzbeauftragten empfohlen): für Ziele S1, S2, S3, S4 - z.B. zur Sicherung der Zustellung von Kartenausschnitten

NPA: datenschutzkonforme Identifikations- und Authentifikationsdienste für Internetdienste/Web unter Nutzung des SAML-Standards: für Ziel S3 - z.B. zur authentisierten Anmeldung und für Dienste-Zugangsautorisierungen

PKI SigG: rechtsverbindliche qualifizierte Signaturen für Ziele S2, S3, S4 - zur rechtsverbindlichen Signierung von Kartendaten und Quellnachweisen, sowie für "Online-Nutzungsverträge", auch zur verbindlichen Integration/Beglaubigung von Standort-Daten.

Für die Operationen Eintragen, Auslesen und Speichern von Kartenobjekten für Kartensysteme können dabei die entsprechenden Sicherheits-Integrationserfahrungen für nachrichten- und dokumentenorientierte eGovernment-Systeme nach Shell-Ansatz übertragen werden (Ergänzung von detachted signatures, OSCI-Kapselungen und Dienste-Zugriffssicherungen auf nPA-Basis und separierte Management-Interfaces/Strukturen). Entsprechende Übertragungen auf Karten-Systemarchitekturen werden vorgestellt, sowohl auf Basis gesicherter mobiler Web-Applikationen als auch von Web Services. Zusätzlich werden mobile Standortortdaten (aus LBS) dabei als zusätzliche Authentisierungs- und Autorisierungs-Credentials integriert.

3. Sicherheits-Anwendungsarchitektur für „mobiles Makeln“

3.1. Sicherheitsintegration für das AAA-Modell

Für die in den Abschnitten 1 und 2 diskutierten Sicherheitsanforderungen und Szenarien ergeben sich verschiedene Umsetzungsansätze. Das Konzeptuelle Anwendungsschema AFIS-ALKIS-ATKIS [9], welches durch die Arbeitsgemeinschaft der Vermessungsverwaltung der Länder der BRD initiiert und neu konzipiert wurde, gibt hier einen ersten technologischen Ansatz wieder. Das Referenzmodell strebt das Ziel an, eine bundesweit einheitliche Beschreibung von Geoinformationen zu schaffen. Dadurch erhalten die Geobasisdaten eine einheitliche Struktur, die auf internationalen Standards basiert. Für Sicherheitszwecke, namentlich der Authentisierung und Autorisierung, lassen sich für verschiedene Service-Schnittstellen entsprechende Internet-Standards wie SAML – Security Assertion Markup Language – nutzen (insbesondere für Web Service Security). Auf dieser Grundlage wird im Folgenden ein erweitertes Autorisierungs- und Zugriffskontroll-Schema (ZK) für das „MobImM“-Szenario auf SAML-Basis vorgeschlagen.

3.2. Sicherheitsintegration für mobile Autorisierungen mittels SAML-Token

SAML-Token enthalten „Bescheinigungen“ eines „Issuer“ (Herausgebers), welche einen Satz von Zusicherungen (Assertions) wiedergeben. Diese postulieren mittels sogenannter Attribute bestimmte Eigenschaften, die einer Entität oder einem Subjekt vom Issuer zugeschrieben bzw. bescheinigt werden, dabei zur externen Nachweisbarkeit/Authentisierung ggf. mit Signatur versehen. Vorteile in der Verwendung von domänen-übergreifenden SAML-Token sind z.B., dass vorregistrierte Nutzer einer Identiy-Federation sich über einen Account-Linking-Mechanismus nicht erneut authentifizieren müssen und für verschiedene Anwendungsdomänen der gleiche (vertrauenswürdige) eID-Service genutzt werden kann. Entsprechend können so Autorisierungen festgelegt werden, so dass diese benutzerbezogene Rechte genau für bestimmte Ressourcen darstellen. Ein ähnlicher Mechanismus, allerdings dort nur für Identifizierung und Authentifizierung, ist bei der eID-Infrastruktur für den neuen Personalausweis (nPA) zu finden [10], jedoch ohne die hier notwendige Autorisierungsfunktionalität. Im folgenden wird am Beispiel des MobImM-Szenariums die Integration entsprechender (mobiler) Autorisierungen erläutert.

Ziel ist es, für mobile Szenarien verfeinerte und entsprechend gesicherte Autorisierungsmechanismen für mobile Kundenzugriffe auf Makler- bzw. GIS-Amt-Kartensysteme (z.B. ATKIS) bereit zu stellen. Als Voraussetzung für die im folgenden vorgeschlagenen Abläufe, Infrastrukturen und Funktionen sei hier die Bereitstellung einer eID-Funktionalität auf SAML-Basis angenommen (z.B. per nPA-eID-Infrastruktur).

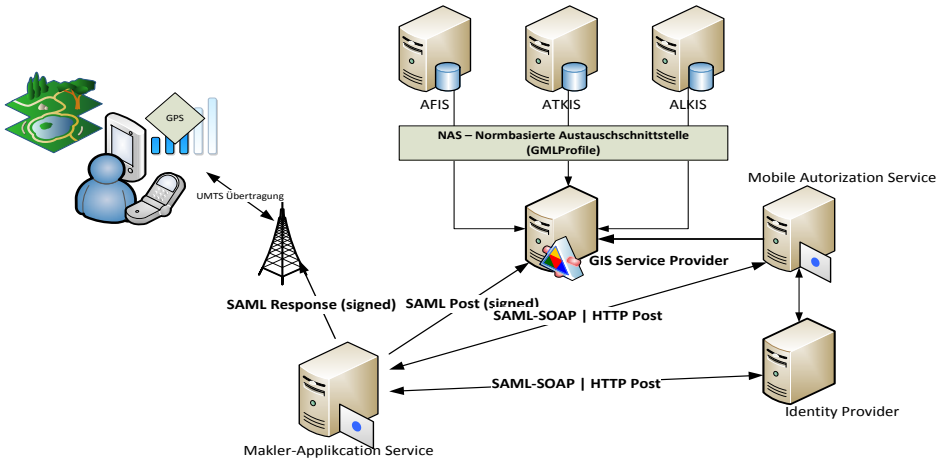

Abbildung 1: Architektur für "mobiles Immobilien-Makeln"

Für das Szenarium „mobiles Makeln“ werden zwei Autorisierungs-Subszenarien unterschieden. Zum einen, ein 1-stufiges Vergabesystem für die Rechte-Vergabe des Maklers auf Makler-Systeme. Zum anderen ein mehrstufiges Rechte-Vergabesystem auf amtliche Karten, erteilt zunächst vom zuständigen Amt für den Makler für (nachgewiesene) Verkaufsimmobilien von dessen Verkaufskunden (z.B. per Kundenvollmacht), dann vom Makler via temporärer Sub-Delegationen mit Einschränkungen (und unter Datenschutzauflagen) an nachgewiesene Kauf-Kunden des Maklers weiterreichbar. Für beide Systeme werden sogenannte SAML-Autorisierungstoken ausgestellt. In dem Fall des mehrstufigen Autorisierungstoken muss jedoch der Makler eine Amts-Zulassung erhalten. Diese Berechtigung für die (lesende) Verwendung der Kartenausschnitte, dort nur für Objekte aus berechtigtem Interesse (für Verkaufskunden), wird vom Kartenvergabeamt (z.B. ATKIS) signiert, um Integrität und Authentizität zu gewährleisten.

Für das Amts-Subszenario bekommt der Kauf-Kunde des Maklers ein temporäres SAML-Delegations-Token, dass zum einen den Verweis auf das amts-signierte Makler-Token beinhaltet und zum anderen die vom Makler signierte Sub-Delegation, unter Einschluss der Identität des Kauf-Kunden, des Objektes mit Koordinaten sowie des Zugriffszeitraum und von Datenschutzauflagen. Für die entsprechende Zugriffskontrolle in mobile Szenarien (LBS) bedeutet die, dass nur Kartenausschnitte vom Maklerkunden eingesehen werden können, welche zum einen vom Amt für den Makler frei gegeben wurden und zum anderen vom Makler temporär für den Kunden, der sich vor Ort bei der Immoblie aufhält, wobei dieser Kunde das jeweilige SAML-Token zusammen mit den korrekten Live-GPS-Koordinaten des Immobilienortes via entsprechender LBS-Services mit sendet. Für das ganze Szenario können wie folgt 3 Autorisierungsknoten (SAML-Token) unterschieden werden:

- Temporäres Delegationsticket für den Kauf-Kunden des Maklers
- Makler-Token vom Kartenvergabeamt (z.B. ATKIS).

Für die Auswertung der SAML-Token sind zusätzliche Inhalte wie die eID, Ablaufdatum und eine Referenz auf den jeweiligen abgefragten Kartenausschnitt über GPS notwendig.

4. Resümee

Es wurden erweiterte Architekturen auf Basis internationaler und nationaler Standards aufgezeigt, um Authentisierungen und Autorisierungen und entsprechende Zugriffskontrollen für GIS-Services für Kartenzugriffe in mobilen Szenarien durch Integration entsprechender Sicherheitsfunktionen (u.a. auf SAML-Basis) umzusetzen. Die Kopplung der Architekturen zu vorhandenen Systemen ist dabei nach zwei Integrations-Varianten möglich: Shell- oder Builtin-Ansatz.

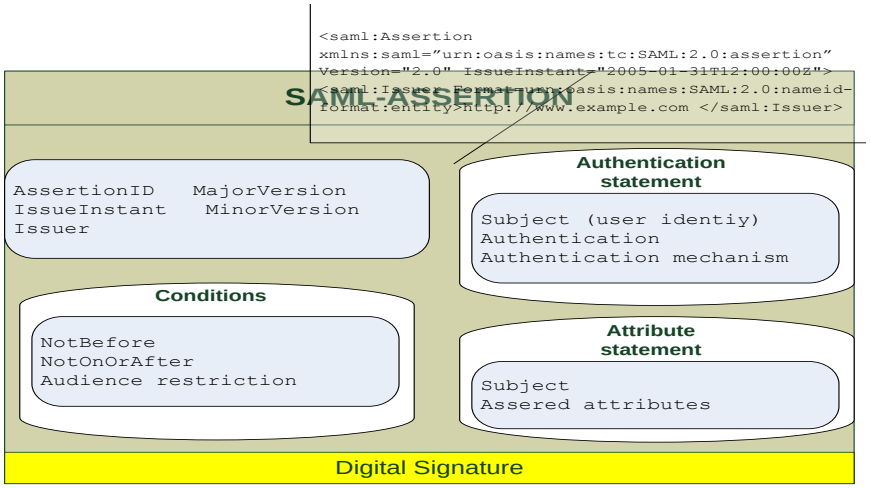

Abbildung 2: SAML-Token Aufbau

Literaturangaben

[1] Pundt, H., Spangenberg, T., Weinkauf, R. (2011): Individualisierung webbasierter und mobiler GI-Dienstezur nutzergerechten und nachhaltigen Tourenplanung. GIS.Science, 24. Jg., 1-3/2011, S. 45 -50.

[2] Pundt, H., Spangenberg, T.: Individualized Travel Planning through theIntegration of different Information Sources, including a POI Ontology

[3] Jörg Blankenbach, *Handbuch der mobile Geoinformation*, Herbert Wichmann Verlag, Heidelberg, 2007.

[4] Ingo Melzer, Service-orientierte Architekturen mit Web Services, Spektrum Verlag, Heidelberg, 2010

[5] KoSIT (Ed.): XÖV-Standard-XML in der öffentlichen Verwaltung, www.xoev.de

[6] Strack, H., Karich, Ch.: „BeGovSAH – Begleitforschung zur Umsetzung des eGovernment-Aktionsplans in Sachsen-Anhalt“; in: Jana Dittmann (Ed.): Tagungsband „Sicherheit 2006, Sicherheit – Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v.(GI), 02/2006 Magdeburg; LNI, Band 77, Springer-Verlag, 2006

[7] Strack, H., Karich Ch.: „A Distributed Architecture for the Management of Transcripts of Records and Student Mobility Data within the Bologna Process Framework“;in: Proceedings of EUNIS 2007 Conference, Universities of Grenoble andUniversity P.M. Curie of Paris, France, 2007

[8] Henning, M., Kußmann, P., Strack, H.: eCampus-Services & -Infrastrukturen – eGovernment-Komponenten- und Service-orientierte elektronische Campusverwaltung mit verbesserter Sicherheit; Tagungsband 12. Nachwuchswissenschaftlerkonferenz Mitteldeutschland 2011, Hochschule Harz, Wernigerode, 2011

[9] Arbeitsgemeinschaft der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV).: Dokument zur Modellierung der Geoinformationen des amtlichen Vermessungswesen (GeoInfoDok); April 2008

[10] BMI (ed.), Jens Fromm, Marian Margraf: Neuer Personalausweis – eID-Server und eID-Service, Berlin, www.ccepa.de , 2011

[11] OASIS, Metadata fort the OASIS Security Assertion Markup Language (SAML), OASIS Standard, 15.März 2005, http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[12] OASIS, Web Service Reliable Messaging TC WS-Reliability 1.1, OASIS Standard, 15. November 2004, http://docs.oasis-open.org/wsrm/ws-reliability/v1.1/wsrm-ws_reliability-1.1-spec-os.pdf

[13] OASIS, Web Service Security SOAP Message Security 1.0 (WS-Security 200401), März 2004 http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf