Technik

Florian Morrenth

Sichere Kommunikation verteilter Applikationen über XML Web Services mit WS-Security

Diplomarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783832476229

Florian Morrenth

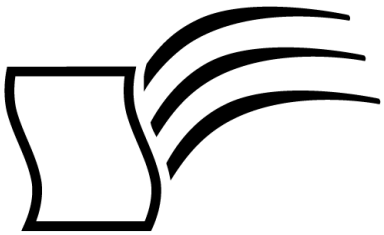
Sichere Kommunikation verteilter Applikationen über XML Web Services mit WS-Security

Diplom.de

Florian Morrenth

Sichere Kommunikation verteilter Applikationen über XML Web Services mit WS-Security

Diplomarbeit
Fachhochschule Technikum Wien
Abgabe Mai 2003



Diplomica GmbH
Hermannstal 119k
22119 Hamburg

Fon: 040 / 655 99 20
Fax: 040 / 655 99 222

agentur@diplom.de
www.diplom.de

ID 7622

ID 7622
Morrenth, Florian: Sichere Kommunikation verteilter Applikationen über XML Web Services mit WS-Security
Hamburg: Diplomica GmbH, 2004
Zugl.: Fachhochschule Technikum Wien, Diplomarbeit, 2003

Diplomica GmbH
http://www.diplom.de, Hamburg 2004
Printed in Germany

Inhalt

1. EINLEITUNG

Web Services gewinnen durch ihre Vorteile gegenüber anderen Technologien für verteilte Systeme zunehmend an Bedeutung. Neben einer hohen Interoperabilität versprechen Web Services kürzere Entwicklungszeiten und reduzierte Investitionskosten durch Wiederverwendung. Web Services eröffnen völlig neue Perspektiven bei der firmenübergreifenden Integration von Geschäftprozessen oder der firmeninternen Integration heterogener Systeme. Standardisierte Technologien wie XML, SOAP, WSDL und UDDI bieten dazu leistungsfähige Bausteine.

Diese Arbeit soll die Grundlagen von Sicherheit in Bezug auf die Kommunikation mit Web Services erläutern und mögliche Umsetzungen dieser Sicherheitsmechanismen aufzeigen. Es soll anhand eines Beispiels gezeigt werden, wie diese Mechanismen umgesetzt werden können, um den Einsatz von Web Services auf Transport- und Applikationsebene durch Identifikation und Vertraulichkeit sicherer zu gestalten.

Im theoretischen Teil dieser Arbeit werden Web Services im Allgemeinen behandelt und deren Einsatzmöglichkeiten sowie bisher standardisierte Technologien erläutert. In weiterer Folge werden verschiedene Aspekte von Sicherheit bei elektronischer Nachrichtenübermittlung erarbeitet und einige Arten von Bedrohungen eines Web Services dargestellt. Kapitel 2.3 Sicherheitsmechanismen behandelt anschließend die Themen Authentifizierung und Sicherung der Transportschicht am Beispiel von Secure Socket Layer, die eine sichere Kommunikation mit Web Services unabhängig von der Implementierung des Web Services ermöglichen. Die Themen XML Signature und XML Encryption werden daraufhin als Beispiele für die Sicherung der Botschaft selbst erklärt und im Rahmen der WS-Security Spezifikation in Bezug zu Web Services gestellt. Als Voraussetzung für den reibungslosen Einsatz von X509 Zertifikaten für die Signatur und Verschlüsselung wird danach das Prinzip einer Publik Key Infrastructure erklärt, das auch in der praktischen Umsetzung Anwendung findet. In Kapitel 3 wird nach einer systematischen Analyse des Umfeldes und der Anforderungen des Projektes, die praktische Anwendung der zuvor erläuterten Sicherheitsmechanismen mit einer detaillierten Funktions- und Umsetzungsbeschreibung erklärt. Abschließend wird eine wirtschaftliche Betrachtung von Web Services und eine Diskussion der Schlussfolgerungen vorgenommen.

2. THEORETISCHE GRUNDLAGEN

In diesem Kapitel werden die theoretischen Grundlagen für den Einsatz von sicherheitsrelevanten Technologien im Umfeld von Web Services erläutert. Nach einer allgemeinen Erklärung der Idee hinter Web Services wird auf deren Funktionsweise und verschiedene Anwendungsmöglichkeiten sowie die Standards, auf denen Web Services aufbauen, eingegangen. Danach werden Fragen der Sicherheit im Bezug auf Web Services, mögliche Angriffsarten sowie Techniken zur Sicherung der Kommunikation näher beschrieben. Ein Exkurs in die Kryptographie beschreibt dabei die Grundlagen von Signatur und Verschlüsselung. Abschließend wird auf eine Spezifikation eingegangen, welche die zuvor beschriebenen Techniken im Umfeld von Web Services umsetzt und auch in der praktischen Ausführung Anwendung findet.

2.1 WEB SERVICES

Aktuelle Webapplikationen gehen davon aus, dass ihre Clients Webbrowser sind, die direkt von Menschen benutzt werden, um Information zu sammeln oder sich auszutauschen. Angenommen diese Applikationen generieren HTML und erzeugen eine graphische Benutzeroberfläche, so funktioniert diese Art der Kommunikation einwandfrei, was die breite Nutzung solcher Applikationen im Internet bestätigt. Das ist aber nicht die einzige Möglichkeit Information über das Internet auszutauschen. Ebenso wie Browser können Desktopprogramme als Clients einer Webapplikation agieren, um beispielsweise online Flugtickets zu reservieren. Dies ist herkömmlichen Programmen durch Parsen und Extrahieren der benötigten Information einer Webseite möglich, was einen erheblichen Entwicklungsaufwand mit sich bringt. Eine einfachere Möglichkeit ist es, die Funktionalitäten einer Webseite, wie etwa die Suche nach Flügen und die Reservierung der Tickets, entfernt aufrufen zu können. Genau diese Möglichkeit bieten Web Services. Sie stellen Webapplikationen dar, deren veröffentlichte Methoden mit entsprechenden Parametern aufgerufen werden und ein Ergebnis zurückliefern. [W1]

Die einschlägige Presse [I4] diskutiert zurzeit die Vor- und Nachteile die Web Services mit sich bringen, sowie die Technologie und die Standards, die Web Services so populär machen. Wie bei anderen Technologien gelten das große Interesse und die

Erwartungshaltung der endgültigen Fertigstellung der Spezifikationen und immer wieder tauchen Fragen nach dem wirklichen Nutzen von Web Services auf. [W2] Julian Bond schreibt in einem Artikel über die Missverständnisse bezüglich Web Services: "*Web Services are systems that enable application to application communication across the internet, in the same way that the early internet protocols focussed on application to user communication across the internet.*" [W3] Er reduziert damit die Beschreibung von Web Services auf die Essenz von entfernten Methodenaufrufen, die schon seit Jahren in verschiedensten Formen bekannt sind. David Chapell schreibt in seinem Artikel "Lifting the fog on Web services":

> *"The truth (about Web Services, Anm. d. Verf) is that the core idea of Web services -- invoking methods in remote systems -- has been around for decades. As most commonly used today, SOAP is just another way to do RPC. Riding on HTTP is a useful idea, but not much of an innovation. The difference between SOAP and its many antecedents, including Microsoft DCOM, Java RMI and CORBA IIOP, is that every vendor has bought into it."* [W4]

Der Kern der Revolution von Web Services besteht demnach nicht so sehr in einer neuartigen Technologie oder in den verwendeten Transportmechanismen und –Protokollen, sondern in der Art und Weise in der sich marktführende Softwarehersteller und Standarisierungsorganisationen auf einen Weg geeinigt haben. Dieses Einverständnis bedeutender Organisationen wie IBM, BEA, SUN und Microsoft stellt eine Grundlage für die breite Akzeptanz von Web Services dar und soll helfen proprietäre Mechanismen zu ersetzen.

Das Ziel von Web Services ist es, auf einfache Weise eine einheitliche Kommunikation zwischen verteilten Applikationen zu ermöglichen, um dadurch herkömmliche Grenzen wie Betriebssysteme, Programmiersprachen und Softwarearchitektur zu überwinden. Eine mögliche Definition von Web Services beinhaltet die Kernaussagen verschiedener Definitionen und umfasst folgende Punkte.

- Web Services stellen Webusern oder Applikationen nützliche Funktionalitäten für entfernte Methodenaufrufe über Standard Webprotokolle zur Verfügung.
- Web Services bieten die Möglichkeit, ihr Interface und ihre Funktionalität hinreichend genau zu beschreiben, um einem Client eine Kommunikation mit ihm zu ermöglichen. Diese Beschreibung ist in einem XML Dokument in der „Web Service Description Language“ (WSDL) zusammengefasst. [W5]

Nachdem die Grundzüge und das Wesen von Web Services behandelt sind, werden im Folgenden Kapitel einige exemplarische Einsatzmöglichkeiten von Web Services umrissen und anhand eines konkreten Beispiels erläutert.

2.1.1 Anwendungsgebiete von Web Services

Web Services können in vielen Bereichen und auf verschiedene Weise firmenintern oder über das Internet genutzt werden. Im Folgenden wird ein denkbarer Einsatz der Web Service Technologie anhand der Dienste einer Fluggesellschaft vorgestellt. Sicherheitsrelevante Aspekte werden hier im Sinne einer Symbolisierung außer Acht gelassen und erst in Kapitel 2.2 Sicherheit detailliert betrachtet.
Web Services werden in den allermeisten fällen in eine Multitier Architektur eingebunden, in der unterschiedliche Maschinen über ein Netzwerk miteinander kommunizieren. In einer solchen Architektur können ein oder mehrere Web Services in unterschiedlichen logischen Programmschichten involviert sein. In speziellen Fällen kann ein Benutzer direkt über einen Browser die Dienste eines Web Services über HTTP GET oder HTTP POST in Anspruch nehmen, wobei auf die meisten Sicherheitsmechanismen, ausgenommen gewisser Authentifizierungsmaßnahmen über den Browser und leitungsnahen Verschlüsselungsmechanismen wie SSL, verzichtet werden muss.
Zwei Möglichkeiten für direkte Zugriffsarten, bei denen ein Client, der in der Regel eine Applikation und kein Mensch ist, auf die Funktionalitäten eines Web Services über LAN oder das Internet zugreift und diese in seine eigene Logik einbindet, sind in Abbildung 1 symbolisiert. Eine Client involviert das Web Service einer Fluggesellschaft, um verfügbare Flüge anzeigen zu können, um gewünschte Flüge zu reservieren und der Fluglinie entsprechende Zahlungsinformationen zukommen zu lassen. Das Web Service kann, um