

Praktikumsbericht

ELCA

Dominic Ullmann

Imput.	Rapport	Version	Datum	Verfasser	Status	Visa
644-235	-	1.0	25.10.02	DUL	gültig	

I. Inhaltsverzeichnis

I.	Inhaltsverzeichnis	2
1	Organisatorisches	3
1.1	Dauer	3
2	Aufgabenstellung	4
3	Tätigkeit	5
3.1	Webservices verstehen	5
3.2	Sicherheitslösungen	5
3.3	Implementation / Verwendung der Sicherheitslösungen	5
3.3.1	Sicherheitslösung auf SOAP/XML Ebene	5
3.3.2	Sicherheitslösung mit SSH-Tunneling.....	6
3.3.3	Sicherheitslösung mit SSL.....	6
3.3.4	Skalierbarkeitstests	6
4	Eindrücke und Erfahrungen	7

1 Organisatorisches

Praktikant: Dominic Ullmann
Firma: ELCA Informatique SA
Betreuer: Philipp Oser

1.1 Dauer

Beginn: 8. Juli 2002
Ende: 18. Oktober 2002

In Wochen: 15

2 Aufgabenstellung

In letzter Zeit wurden Webservices immer mehr für nicht allzu kritische Businessfunktionen verwendet.

Damit auch kritischere Funktionen über Webservices zur Verfügung gestellt werden können, müssen Sicherheitsmechanismen verfügbar sein und verwendet werden.

Im Rahmen dieses Praktikums sollte untersucht werden, wie für Webservices Sicherheit implementiert werden kann. Folgende Sicherheitservices sollten von den Sicherheitslösungen angeboten werden

- Authentifizierung
- Integrität
- Vertraulichkeit

Ziel der Arbeit war es verschiedene Sicherheitslösungen für Webservices anzuwenden, respektive zu implementieren und diese anschliessend zu evaluieren.

Die entsprechenden Lösungen sollten in bezug auf Skalierbarkeit, Sicherheit und Konfigurationsmöglichkeiten/Installation verglichen werden.

3 Tätigkeit

3.1 Webservices verstehen

In einem ersten Schritt ging es darum, mich mit Webservices vertraut zu machen und entsprechende Frameworks für die Java-Entwicklungsplattform kennen zu lernen.

3.2 Sicherheitslösungen

Da die grosse Stärke von Webservices die Interoperabilität ist, sollten die betrachteten Sicherheitslösungen nicht allzu weit von den sich entwickelnden Standards in diesem Bereich abweichen.

Als erstes musste ich also herausfinden, was die grossen Spieler im Webservice Bereich vorschlugen, um Webservices sicher zu machen.

Im Moment werden grössere Anstrengungen unternommen um die Sicherheitsmechanismen auf der SOAP/XML Schicht zu implementieren. Ein Konsortium um Microsoft/IBM/Verisign arbeitet an entsprechenden Standards.

Als weitere Möglichkeit wird vorgeschlagen Sicherheitsmechanismen zu verwenden, die auf der Transportschicht arbeiten (SSL oder SSH – Tunneling).

3.3 Implementation / Verwendung der Sicherheitslösungen

3.3.1 Sicherheitslösung auf SOAP/XML Ebene

Als erstes machte ich mich daran eine Sicherheitslösung auf der SOAP/XML Schicht zu implementieren. Dazu realisierte ich in einem ersten Schritt in etwa die Vorschläge aus dem WS-Security Standard von Microsoft/IBM/Verisign.

Nach ersten Tests mit dieser Lösung war klar, dass sie in der jetzigen Form eine äusserst ungenügende Performance aufwies. In einem weiteren Schritt mussten nun Lösungen gefunden werden, um die Performance zu verbessern.

Das Performanceproblem stammte zum grossen Teil daher, dass meist teure asymmetrische Kryptographieverfahren verwendet wurden um die Sicherheitsmechanismen zu realisieren. Deshalb bot es sich an das Session-Konzept zu verwenden um billige symmetrische Kryptographieverfahren einsetzen zu können. Dazu werden Session Keys für Verschlüsselung/Entschlüsselung und Signieren/Verifizieren etabliert und dann verwendet.

Tatsächlich brachte die Implementierung des Session-Konzeptes eine Verbesserung der response-Time um einen Faktor fünf bis sieben.

3.3.2 Sicherheitslösung mit SSH-Tunneling

Diese Sicherheitslösung benutzt das SSH-Protokoll um TCP/IP Verbindungen durch einen sicheren Tunnel zu leiten.

Für diese Lösung brauchte es praktisch keinen Aufwand meinerseits, da die entsprechende SSH-Software die Funktionalität bereits zur Verfügung stellte.

3.3.3 Sicherheitslösung mit SSL

Diese Sicherheitslösung verwendet TLS/SSL um die Daten auf der Transportschicht zu sichern. In Java 1.4 ist die entsprechende Library bereits integriert. Die Webservice-Frameworks unterstützen die Verwendung von SSL/TLS Verbindungen auch. Deshalb musste ich hier vor allem herausfinden, wie diese Lösung verwendet wird.

Des weiteren galt es noch eine Möglichkeit zu finden, die authentifizierte Identität des Kommunikationspartners für einen Autorisierungsmechanismus zur Verfügung zu stellen.

3.3.4 Skalierbarkeitstests

Skalierbarkeitstests sollten zeigen wie gut die betrachteten Sicherheitslösungen skalieren, d.h. es galt herauszufinden, wie schnell sich die Responsetime eines Webservices mit zunehmender Anzahl Klienten verschlechtert.

Als Resultat ergab sich, dass die Sicherheitsmechanismen auf Transportebene viel besser skalieren als die Lösung auf der SOAP/XML Ebene.

4 Eindrücke und Erfahrungen

Die gestellte Aufgabe war sehr spannend und herausfordernd. Besonders interessant für mich war, dass die Aufgabe einen Bereich betraf, der sich im Moment sehr stark entwickelt. Dadurch war es mir möglich mit verschiedenen Technologien und Möglichkeiten zu experimentieren.

Für diese Aufgabe konnte ich das während dem Studium in verschiedenen Bereichen erworbene Wissen gut gebrauchen. Vor allem nützlich waren die Kenntnisse in Kryptographie / Security, in verteilten Systemen und in Softwaretechnologie.

Das Arbeitsklima war sehr angenehm. Auch an das Arbeiten in einem Grossraumbüro konnte ich mich schnell gewöhnen. Trotz der durchaus vorhandenen Ablenkungen war es mir möglich, konzentriert zu arbeiten.

Die Betreuung durch mein Team während dem Praktikum war ausgezeichnet. Auch die anderen Mitarbeiter waren sehr hilfsbereit, wenn ein Problem auftauchte, das in ihr Gebiet fiel.

Alles in allem hat mir das Praktikum sehr gut gefallen und war sehr lehrreich für mich. Ich bin froh, dass ich die Gelegenheit hatte, ein Praktikum bei ELCA zu absolvieren.