

## WS-Security Policy in Financial Solutions

Autor: Boris Düdder

Microsoft Corporation und IBM Corporation haben in Zusammenarbeit mit Bea, Verisign und RSA-Security am 19. Dezember 2002 eine neue Spezifikation für den Web-Services-Sicherheitsstandard WS-Security entwickelt. Dieser Standard erlaubt es verteilten Applikationen, welche das SOAP-Protokoll verwenden, Nachrichten in sicherer Form über ein ungesichertes Medium, wie es das Internet ist, zu versenden. Diese Protokollergänzung erlaubt eine sichere, standardisierte Kommunikation zwischen dem Web-Services der IMMO-DATA AG / IMMO-CHECK GmbH und den Client-Applikationen bei unseren Kunden.

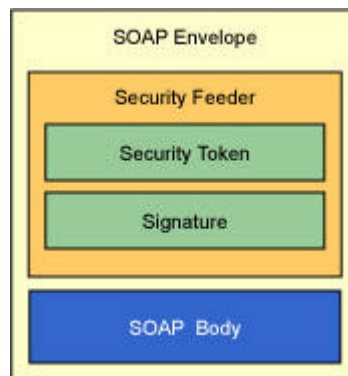


Abbildung 1: SOAP Envelope (Quelle: IBM Corp.)

Eine Client-Applikation kommuniziert mit einem Web-Service mittels eines SOAP-Dokuments. Mangels eines Sicherheitsstandards erfolgte bis dato an dieser Stelle die Sicherung durch eine SSL-Verbindung. Die ressourcenintensive Verschlüsselung der gesamten Informationen sowohl auf Hin- als auch auf dem Rückweg ist ein schwerwiegendes Manko. Der neue Standard erlaubt nun eine Ressourcenschonende, selektive Sicherung sensibler Informationen bei dieser Kommunikation. Die Protokollerweiterung, die SOAP-Envelopes verwendet, bietet:

- Digitale Signatur durch X.509 Zertifikate
- Verschlüsselung durch X.509 Zertifikate sowie Verschlüsselungsalgorithmen wie AES (Rijndael) / 3DES
- Anhänge (Attachments)
- Integrität
- Sicherheit
- Proof-of-Possession

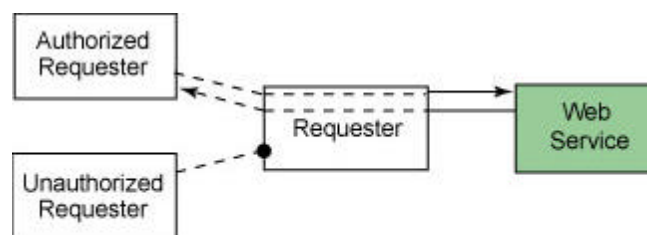


Abbildung 2: Issued Security Token (Quelle: IBM Corp.)



Der SOAP-Router bereitet das SOAP-Dokument für den Web-Services-Host auf:

5. Entschlüsselung des User-Tokens
6. Verifikation der Digitalen Signatur bei einer vertrauenswürdigen Zertifizierungsstelle, z.B. DTAG, VeriSign, usw.
7. Entschlüsselung der Methode und deren Parameter, gemäß der gewählten Verschlüsselungsmethode
8. Weiterleitung des aufbereiteten SOAP-Dokuments an den durch die Verantwortlichkeit zugeordneten Web-Services-Host.

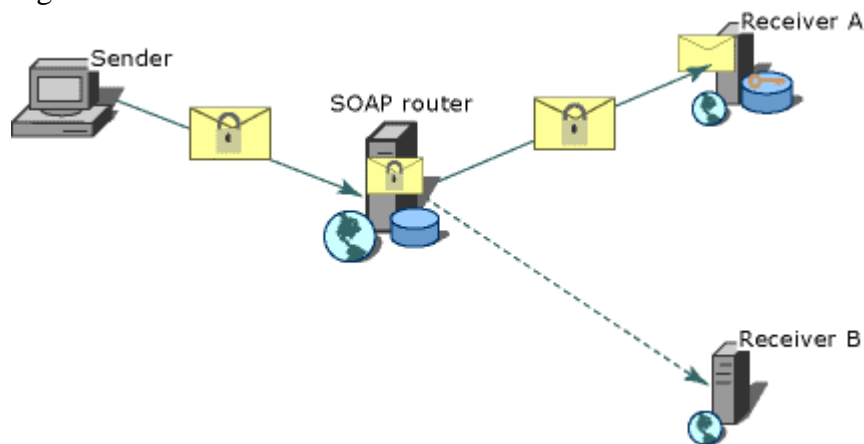


Abbildung 4: SOAP-Router (Quelle: Microsoft Corp.)

Der Web-Services-Host führt als letzter in dieser Kette die gewünschte Anfrage durch:

9. Verifizierung des User-Tokens und Abbildung auf einen User
10. Billing (e.g. Pay-per-click) und Ausführung der Anfrage
11. Zusammenstellung eines Resultats als SOAP-Dokument
12. Versendung dieses Dokuments an den SOAP-Router

Das Prozedere bei der Sendung des Resultats ist bis auf die Nutzung eines User-Tokens ähnlich.

Das Verfahren ist unabhängig von einzelnen Hosts sowie deren Herstellern. Die Microsoft Corp. bietet mit WSE 1.0 eine Erweiterung für das .NET-Framework. IBM bietet ein Pendant für das IBM Web Services Toolkit an. Beide Unternehmen werden diese Diensterweiterung im nächsten Update ihrer Produkte integrieren. Auf den Webseiten der beiden Unternehmen befinden sich weitergehende Informationen zu diesem Thema.

#### Weitere Quellen:

SOAP 1.2: World Wide Web Consortium

<http://www.w3.org/TR/soap12-part1>

Verschlüsselung: World Wide Web Consortium

<http://www.w3.org/TR/xmlenc-core/>

Digitale Signatur: World Wide Web Consortium

<http://www.w3.org/TR/xmldsig-core/>

WS-Security: Microsoft Corp.

<http://msdn.microsoft.com/library/en-us/dnglobspec/html/wssecurspecindex.asp>

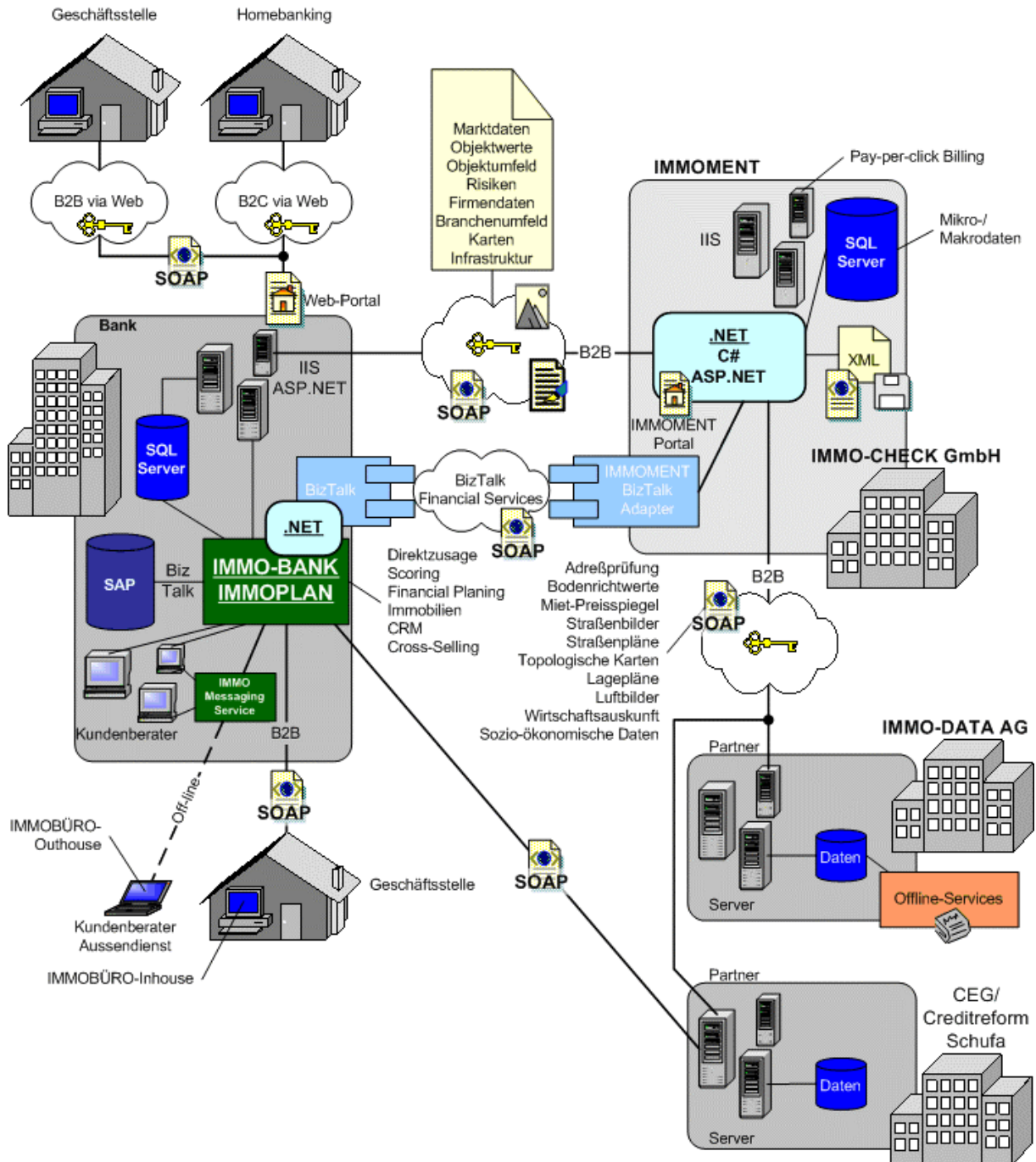


Abbildung 5: IMMOMENT