HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	**Informatik**
Name der Studierenden	**Franziska Altorfer, Rolf Latzer**
Studienjahr	**HS 2008/09**
Titel der Studienarbeit	**WCF Security Token Service based on WS-Trust and WS-Security**
Examinatorin / Examinator	**Betreuer: Alain Schneble** **Verantwortlicher: Hansjörg Huser**

Kurzfassung der Studienarbeit

Die Studienarbeit implementiert das Konzept eines Single Sign On auf Basis des Security Token Service (STS). Single Sign On bedeutet, dass ein Benutzer nach einmaliger Authentifizierung alle Dienste nutzen kann ohne sich ein weiteres Mal einloggen zu müssen. Beispielsweise kann dadurch ein Flug nach New York gebucht und ohne ein weiteres Login auch das Hotel in New York reserviert werden.

Die Arbeit ist in zwei Teile gegliedert. Der theoretische Teil umfasst dabei eine Studie, wie aufgrund der vorhandenen Technologien und Standards ein STS realisiert werden kann. Der praktische Teil setzt das theoretische Konzept mittels eines Prototyps um.

Theoretischer Teil

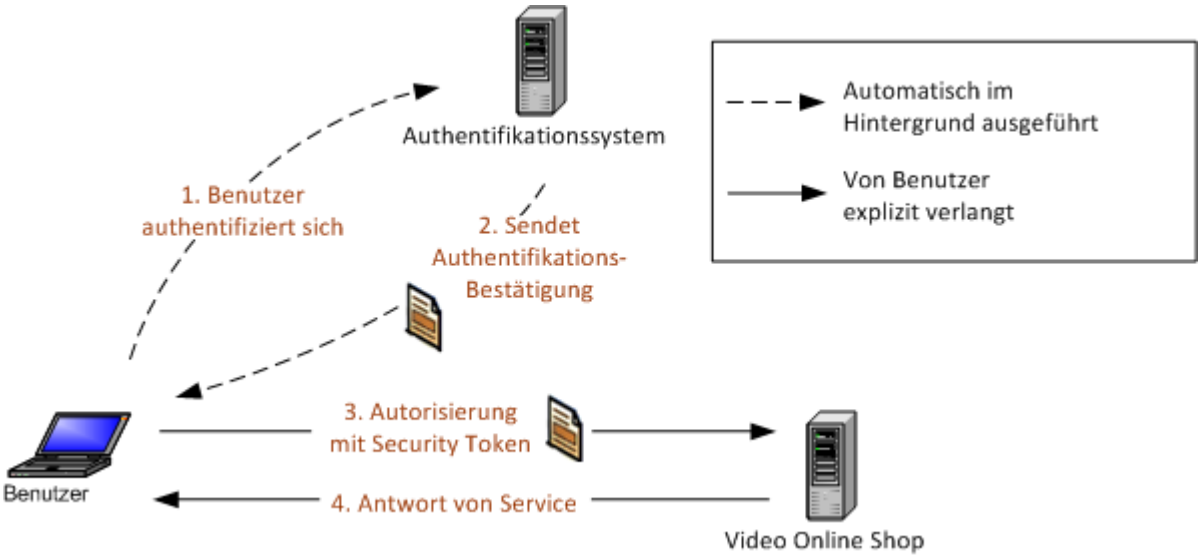
WS-Trust definiert das Konzept eines Security Token Service (STS). Ein STS übernimmt dabei die Aufgabe eines Brokers welcher Security Tokens ausstellt und für die weitere Verwendung zur Verfügung stellt. WS-Security unterstützt dabei verschiedene Security Tokens (Token Profiles) wie z.B. Username, X.509, Kerberos oder SAML Tokens. Diese Tokens werden vom neuen Windows Communication Foundation (WCF) Framework von .Net bereits unterstützt. Der praktische Teil baut auf diesem Framework auf.

Als Token wird SAML verwendet, da es mit den Claims die grösstmögliche Flexibilität bietet. Claims sind Anrechte, die eine Person besitzt. Jede Person besitzt beispielsweise das Anrecht *Alter* (ClaimType) mit dem entsprechenden Alter der Person (Resource bzw. Value des Claims).

Praktischer Teil

Der praktische Teil umfasst eine Implementierung eines STS, eines Beispielservices sowie eines Clients. Der Kern bildet dabei die Implementierung des STS. Als Authentifikation wird Benutzername/Passwort (UsernameToken) und als Autorisierung gegenüber dem Service ein SAML-

Security Token verwendet. Der Service muss sich nicht um die Authentisierung und Verwaltung der Benutzerrechte sorgen, da dies vollständig vom STS übernommen wird. Als Beispielszenario dient die Implementierung eines VideoOnlineShops. Dieser erlaubt eine Videoliste anzuzeigen und Videos herunterzuladen.



Die Implementierung des lauffähigen Prototyps benutzt die Programmiersprache .Net. Die Resultate dieser Studienarbeit können als Basis für zukünftige Implementierungen eines Security Token Services verwendet werden.