

# Charon Security Token Server - WS Trust 1.3 Implementation

Informatik  
Informatique

Web Service Security / Prof. Dr. Eric Dubuis  
Experte: Dr. Andreas Spichiger, PostFinance

Man stelle sich eine Applikation vor, die zwei Web Services benutzt. Um Unbefugten den Zugriff zu verweigern, sind beide geschützt. Bei dem ersten erfolgt die Authentifizierung über Benutzername/Password, beim anderen über ein Kerberos Ticket. Die Applikation muss sich nun bei beiden Web Services authentifizieren. Dies bereitet der EntwicklerIn der Applikation einen zusätzlichen Aufwand, da sie für beide Authentifizierungsarten separate Zugangsdaten bereitstellen muss. Diese müssen dann vom User abgefragt werden. Dies führt dazu, dass sich der Endbenutzer beim Benutzen des Programms mehrmals authentifizieren muss, weil dieses intern verschieden Web Services benutzt.

## WS-Trust

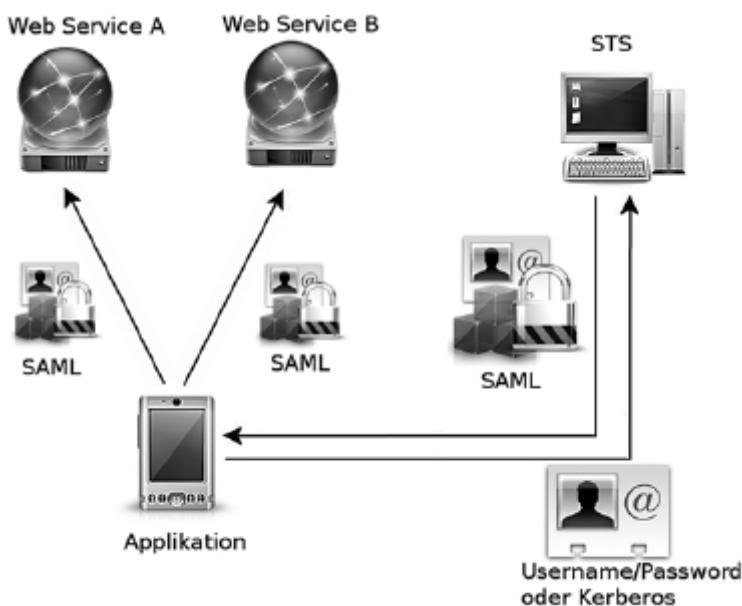
Um dieses Problem zu lösen, wurde der WS-Trust Standard definiert. WS-Trust spezifiziert eine Lösung mit zentraler Authentifizierungsstelle (Single sign-on). WS-Trust funktioniert ähnlich wie Kerberos, aber für Web Services. WS-Trust ist ein offener Standard, welcher von einem Konsortium verschiedener Unternehmungen der IT Branche definiert wurde. Der zentrale Authentifizierungsserver (STS Security Token Server) unterstützt verschiedene Authentifizierungsarten und stellt nach erfolgreicher Authentifizierung ein SAML-Token aus. SAML-Token sind beglaubigt, indem der STS diese mit seinem privaten Schlüssel digital signiert. Web Services, welche ihre Authentifizierung an den STS auslagern, bilden mit diesem ein Vertrauensverhältnis. Wenn diese ein vom STS unterschriebenes SAML-Token erhalten, vertrauen diese darauf, dass alle darin enthaltenen Informationen korrekt sind. Mit zusätzlichen Attributen können in SAML-Token Autorisierungsdaten gespeichert werden.



Lösung ohne STS

## Lösung mit STS

Im Rahmen unserer Diplomarbeit entwickelten wir den Charon STS, eine Teilimplementation des WS-Trust Standards. Die EntwicklerIn der Applikation implementiert eine vom STS unterstützte Authentifizierungsart. Jedes Mal, wenn die Applikation einen Web Service benötigt, wird vorher beim STS ein SAML Token verlangt, welches für den gewünschten Web Service ausgestellt wird. Das Token wird zu der Applikation zurückgeschickt und kann für die Anfrage an den gewünschten Web Service als Authentifizierung benutzt werden. Ein weiterer Vorteil dieser Lösung ist, dass der Web Service selber keine eigene Authentifizierungsfunktionalität mehr benötigt.



Lösung mit STS

## Charon STS

Der Charon STS ist eine Teilimplementation des WS-Trust Standards. Die Architektur der Software lässt es zu, den Charon STS über Plugins zu ergänzen. Auf diese Weise können z.B. weitere Authentifizierungsarten hinzugefügt werden. Die Betreiber von einem Charon STS können diesen mit eigenen Skripten ergänzen, welche die SAML-Attribute mit Autorisierungsdaten versehen. Die Konfiguration von Plugins, Skripten und weiteren Systemeinstellungen erfolgt über ein Webinterface.

Um Applikationsentwicklern die Kommunikation mit dem Charon STS zu erleichtern, wird diesen eine Bibliothek zur Verfügung gestellt.



Matthias Ruedlinger

1981

md@rueedlinger.ch



Philipp Uhlmann

1980

phipu@phipu.ch