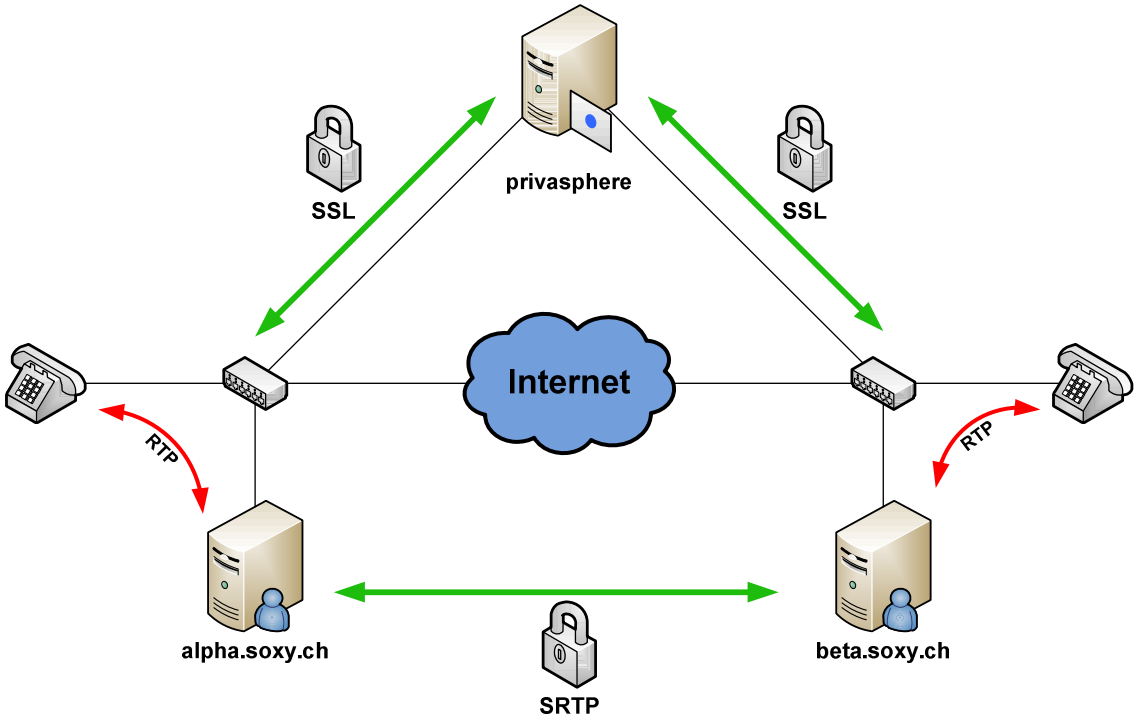
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Studienarbeit

Abteilung	I
Name der Studierenden	Michael Koch, Raoul Harlacher
Studienjahr	Herbstsemester 07/08
Titel der Studienarbeit	VoIP Integration into the PrivaSphere Secure Messaging Service
Examinatorin / Examinator	Dr. Prof. Andreas Steffen

Kurzfassung der Studienarbeit

Heutzutage wird immer öfters „Voice over IP“ genutzt, obwohl die Kommunikation nicht verschlüsselt ist. Der Benutzer kann durch spezielle Software den Anruf verschlüsseln, jedoch nicht sicherstellen, dass keine Man-in-the-Middle-Attacke vorliegt.
Diese Arbeit beschreibt wie ein VoIP Aufbau gemacht werden kann, um verschlüsselt und sicher zu kommunizieren. Um dies zu ermöglichen, mussten wir eine bestehende Secure SIP Proxy Software (Soxy – http://www.soxy.ch) mit einem Zertifikatsüberprüfungsteil ergänzen und konnten somit eine funktionierende Schnittstelle zu einer Zertifikats-Autorisierungsstelle herstellen. Diese Autorisierungsstelle war die Partnerfirma Privasphere (http://www.privasphere.com), welche diesen Dienst anbietet.



Um ein Telefongespräch zu verschlüsseln, wird eine Public Key Infrastruktur benötigt. Das Zertifikat wird beim Beginn des Anrufes ausgetauscht. Sobald dieses erfolgreich übertragen wurde, wird eine Anfrage an den Privasphere Server gemacht, ob das Zertifikat gültig ist und eine Vertrauensbeziehung zwischen den Beteiligten besteht. Eine Vertrauensbeziehung wird über einen sekundären Weg (Tel, SMS, Fax, Brief,…) getätigt. Falls das Zertifikat ungültig ist oder keine Vertrauensbeziehung besteht, wird automatisch ein Mail an die Beteiligten gesendet. Mit dieser Lösung kann eine Benutzer-Authentisierung auf Zertifikatebene durchgeführt werden, welche somit eine verschlüsselte, sichere Beziehung ermöglicht.