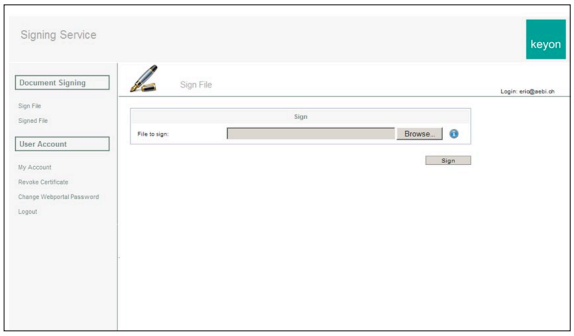
Eric
Aebi

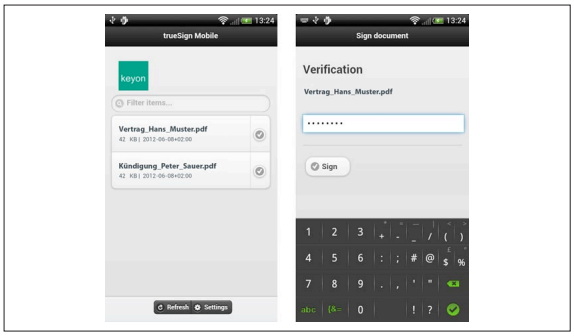
Diplomand	Eric Aebi
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit
Projektpartner	keyon AG, Jona SG

Zentraler Signaturdienst

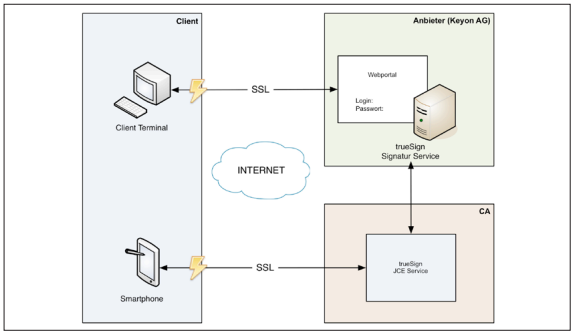
Rechtsgültiges Signieren von Dateien ohne Smartcard



Webseite des zentralen Signaturdienstes



Android-Client-Applikation



Schematischer Aufbau der gesamten Applikation

Ausgangslage: Mit der Suisse ID ist es bereits möglich, Dokumente rechtsgültig digital zu signieren. Hierfür wird jedoch eine Smartcard benötigt. Viele User sind aber mit der Installation und Anwendung einer Smartcard überfordert. Die Firma Keyon AG in Jona hat einen Signaturserver entwickelt, welcher nun entsprechend erweitert werden soll, um die gesetzlichen Vorgaben für qualifizierte Signaturen, wie unter anderem die Zwei-Faktor-Authentisierung, zu erfüllen.

Vorgehen/Technologien: In einer ersten Phase wurden Sicherheitsszenarien auf Grundlage des Schweizer Signaturgesetzes analysiert. Dabei galt es in erster Linie zu verhindern, dass ein Angreifer eine Signatur mit einem Zertifikat einer Drittperson ausführen kann. Dies konnte durch eine durchgehende SSL-Verschlüsselung sowie eine Zwei-Faktor-Authentisierung mittels einer Smartphone-App bewerkstelligt werden. Da bei dieser Arbeit eine bereits bestehende Applikation erweitert wurde, war die Technologie weitgehend vorgegeben. Der Serverteil wurde in Java entwickelt. Beim Web-Frontend handelt es sich um eine ASP.Net-(C#)-Applikation. Bei der Mobile-App handelt es sich um eine neue Entwicklung. Diese wurde, um den Entwicklungsaufwand für alle mobilen Plattformen möglichst gering zu halten, mit dem Phonegap-Framework erstellt. Phonegap basiert auf HMTL5 und JavaScript und ermöglicht so, die Applikation für alle Plattformen nur einmal zu entwickeln.

Ergebnis: Die entwickelte Applikation ermöglicht das Signieren von Dokumenten via Webportal. Der User kann das zu signierende Dokument im Webportal hochladen, dieses wird ihm anschliessend zur Bestätigung an sein Smartphone geschickt, wo der User die Datei kontrollieren und die Signatur bestätigen kann. Nach erhaltener Bestätigung durch das Smartphone signiert der Server das Dokument und stellt es im Webportal zum Download bereit. Dank der Bestätigung via Smartphone wird die für qualifizierte Signaturen vom Schweizer Signaturgesetz vorgeschriebene Zwei-Faktor-Authentisierung eingehalten. Das Login zum Webportal wurde zusätzlich durch eine TAN gesichert, welche ebenfalls in der Mobile-App angezeigt wird.