Validator Next Generation

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Gerhard Hassenstein
Experte: Prof. Dr. Andreas Spichiger
Industriepartner: Glue Software Engineering AG, Bern

Die schweizerische Bundesverwaltung stellt für die Validierung von signierten PDF Dokumenten nach Schweizer Recht (ZertES) den Dienst «Validator.ch» zur Verfügung. Dokumente die nach der europäischen eIDAS Verordnung signiert sind, können mit der aktuellen Version nicht überprüft werden. In Hinsicht auf die anwachsende Digitalisierung in der politischen und wirtschaftlichen Welt wurde ein Prototyp implementiert, der sowohl PDF Dokumente nach ZertES und eIDAS validieren kann.

Ausgangslage

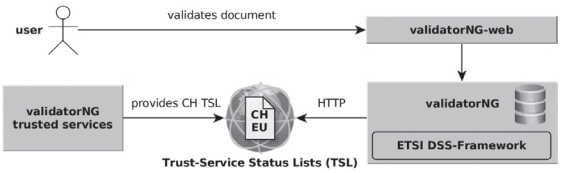
Im Rahmen eines Vorprojekts wurde bereits analysiert, wie es möglich ist, den bestehenden «Validator.ch» um den eIDAS bzw. ETSI Standard der europäischen Union zu erweitern, damit auch Signaturzertifikate von EU akkreditierten Anbieterinnen von Zertifizierungsdiensten validiert werden können. Der Ausgang der Vorarbeit zeigte, dass eine neue Implementation des «Validator.ch» basierend auf der europäischen Referenzimplementation (DSS-Framework) die besten Optionen für künftige Erweiterungen bietet.

Auftrag

Der «Validator.ch» soll von Grund auf als Prototyp neu implementiert werden. Für die kryptografische Überprüfung der Signaturen eines PDF Dokuments soll das DSS-Framework der europäischen Union verwendet werden. Für PDFs mit einer Signatur nach ZertES (Bundesgesetz über die elektronische Signatur) soll das Dokument zusätzlich einer fachlichen Prüfung unterzogen werden. Dabei wird anhand der Signaturen und Attribute überprüft, ob das zu validierende Dokument beispielsweise ein gültiger schweizerischer Strafregisterauszug, ein Dokument der Bundesverwaltung oder eine Urkunde ist.
Die Verwaltung und Bereitstellung der vertrauenswürdigen Anbieterinnen von Zertifikatsdiensten der Schweiz und den europäischen Mitgliedstaaten soll mittels ETSI definierten «Trust-Service Status Lists» umgesetzt werden.
Der Endbenutzer soll über eine Weboberfläche das zu validierende PDF Dokument per Drag and Drop hochladen und die Prüfung starten können.

Umsetzung

Der neue «Validator.ch» wurde als Webapplikation mittels Java EE 7, Payara Application Server und MySQL umgesetzt. Für automatisierte Tests wurde zusätzlich ein Command Line Interface implementiert. Die fachlichen Prüfungen für schweizerische Dokumente wurden mittels Groovy Skripts umgesetzt. Da diese zur Laufzeit kompiliert und ausgeführt werden, ermöglicht es das Anpassen und Hinzufügen einzelner Prüfungen ohne die gesamte Applikation zu ersetzen.
Die schweizerische «Trust-Service Status List» wurde gemäss ETSI-Standard im XML-Format erstellt und signiert. Diese wird dem «Validator.ch» über HTTP zur Verfügung gestellt.
Die existierenden europäischen «Trust-Service Status Lists» werden über die offizielle Quelle eingebunden.



Übersicht der Hauptkomponenten

Ergebnis und Ausblick

Bei der Implementation des Prototyps bestand eine Schwierigkeit darin, möglichst alle Synergien vom ETSI-Standard und ZertES zu nutzen und das Handling von Unterschieden optimal umzusetzen.
Es konnte erreicht werden, dass die Applikation signierte Dokumente sowohl nach schweizerischen wie auch nach europäischen Richtlinien erfolgreich erkennen und validieren kann. Dies erlaubt einem Benutzer, PDF Dokumente zu überprüfen, ohne deren Inhalte zu kennen. Durch die flexible Softwarearchitektur können Komponenten wie beispielsweise das DSS-Framework, das Web-Frontend oder die fachliche Prüfung ausgetauscht werden.
Der «Validator.ch» Prototyp bietet durch den Einsatz des DSS-Frameworks die nötige Grundlage für zukünftige Änderungen von Signaturvorschriften. So referenzieren die neuen «Technischen und administrativen Vorschriften» (TAV Ausgabe 5) des BAKOM mehrheitlich dieselben ETSI Standards.

Jan Andreas Hirsiger

Nicolas Kyd