

Motivation

Die Validierung einer elektronischen Signatur kann recht komplex sein (beispielsweise wenn die in einem anderen Bakk-Projekt bearbeiteten Langzeitverfahren eingesetzt werden, wo unter Umständen mehrere Generationen von Zeitstempeln verwendet werden müssen, um schwächer gewordene Hashverfahren oder zu kurze Schlüssellängen auszugleichen).

Die Nachvollziehbarkeit einer derartigen Validierung ist demnach oft ebenso schwierig. Letztlich wird aber der Benutzer diese Entscheidung der Software akzeptieren müssen - oder ignorieren wollen. Um ihm dies einfacher zu machen, benötigen wir eine brauchbare, adaptive Benutzerschnittstelle, mit der das Validierungsprotokoll analysiert werden kann.

Dieses Projekt soll eine derartige Benutzerschnittstelle exemplarisch in Form einer "browsbare Validierungsumgebung" implementieren. Diese Software soll es ermöglichen, Parameter der Validierung einzustellen und damit dann eine elektronische Signatur zu prüfen. Das Ergebnis soll dann in einer Browserumgebung den Bedürfnissen eines Benutzers entsprechend mehr oder weniger detailliert dargestellt werden. Vorstellbar ist beispielsweise, dass zuerst nur "Signaturprüfung fehlgeschlagen" mit einer Begründung des Fehlschlags angezeigt wird. Erst nach klicken auf einzelne Elemente erhält der Benutzer weitere Informationen, wie bei der Prüfung verwendeten Elemente, bis hinunter zu den Bits und Bytes.

Goals and Tasks

- ▶ Einarbeiten in die Grundlagen der Signaturvalidierung und HTML5
- ▶ Ausarbeitung eines Konzeptes
- ▶ Implementierung eines Frameworks für die Anzeige von Validierungsergebnissen
- ▶ Zusammenarbeit mit der Gruppe für "Validierung alter Signaturen"

Deliverables

- ▶ Konzept der Implementierung
- ▶ Implementierung
- ▶ Dokumentation
- ▶ Präsentation

Studies

INF SW TEL TM

Prerequisites

- ▶ Java-Programmierenkenntnisse
- ▶ Grundkenntnisse elektronischer Signaturen (Einführung IT Sicherheit)

Advisor / Contact

peter.lipp@iaik.tugraz.at