

Selectio Helvetica – Prozesse und Implementation

Betreuer: Prof. Dr. Eric Dubuis
Prof. Dr. Andreas Steffen

Baloti ist ein Webportal für Immigranten in der Schweiz. Mit Hilfe von Baloti sollen sie das politische System der Schweiz besser kennen lernen. Konkret werden nationale Abstimmungen und Wahlen simuliert. Baloti erfüllt, analog zu einer offiziellen Abstimmung, viele Sicherheitsanforderungen wie z.B. den Schutz der Privatsphäre. In dieser Arbeit wurde aus dem kryptographischen Protokoll «Selectio Helvetica» die notwendigen Prozesse entwickelt und implementiert.



Severin Hauser

Selectio Helvetica

Selectio Helvetica ist ein speziell auf die Bedürfnisse von Baloti angepasste Konkretisierung eines Protokolls für elektronische Abstimmungssysteme. Um die gewünschten Eigenschaften zu erreichen, wurden verschiedene kryptographische Funktionen miteinander kombiniert und/oder verkettet. Dadurch ergaben sich folgende Rollen, welche für dieses Protokoll benötigt werden:

Administration - Die Administration möchte eine Abstimmung durchführen. Sie bestimmt alle Daten rund um die Abstimmung. Dazu zählt auch, dass sie eine Liste der stimmberechtigten Voter bestimmt und entscheidet, welche Trustees für diese Abstimmung vertrauenswürdig sind. Die Administration ist auch verantwortlich für die Bereitstellung aller öffentlichen Daten.

Trustee - Der Trustee vertritt die Interessen einer Gruppe von Votern. Im Zuge dieser Aufgabe stellt er sicher, dass bei einer Abstimmung alles korrekt abläuft. Dies geschieht, indem der Trustee bei den kryptographischen Funktionen mitarbeitet.

Pro Abstimmung gibt es immer mehrere Trustees, welche je verschiedene Interessengruppen vertreten.

Voter - Der Voter möchte seine Stimme für eine bestimmte Abstimmung abgeben. Dabei ist für ihn wichtig, dass er sicher sein kann, dass seine Stimme gezählt wird und niemand weiss, wie er gestimmt hat.

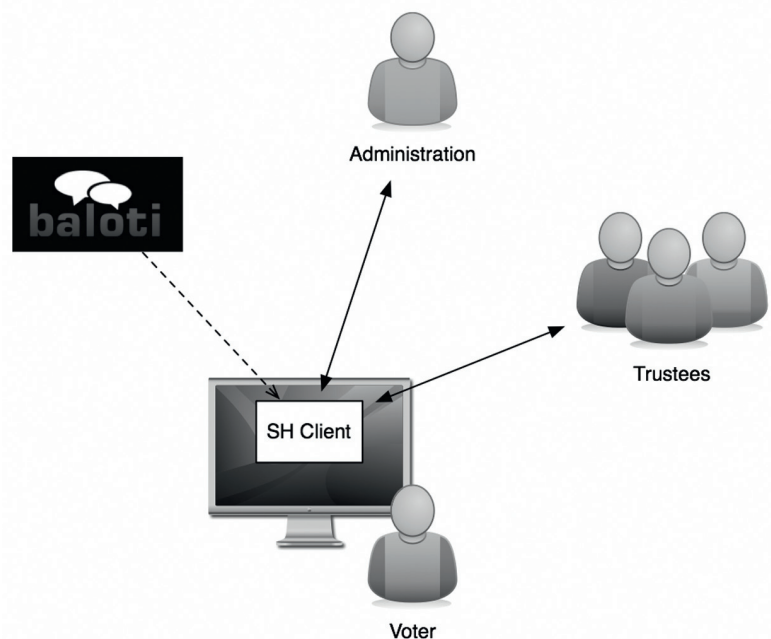
Prozesse

Die vielen verwendeten kryptographischen Funktionen haben jeweils ihre eigenen Prozesse. Auf Grund der vielfachen Kombinationen ist sehr schwierig, den korrekten Ablauf sichern zu stellen. Darum wurde im Rahmen dieser Arbeit die kompletten Prozesse von Selectio Helvetica erarbeitet. Aus diesen Prozessen lassen

sich die notwendigen Schnittstellen der einzelnen Teilnehmer bestimmen, was die Implementation überhaupt erst möglich macht.

Implementation

Wie in der Abbildung zu sehen ist, wird dem Besucher des Webportals ein JavaScript-Programm geschickt. Dieses baut die Kommunikation mit der Administration und den Trustees auf. Über diese Kanäle wird das Protokoll abgewickelt. Die Kommunikation erfolgt mittels JSON-Objekte. Die Administration und die Trustees sind auf verschiedenen JavaEE-Servern installiert. Untereinander kommunizieren diese über Webservices.



Übersicht Kommunikation