TrustVote
Schlussbericht

BFH Projekt 8121PT_TI TrustVote
Eric Dubuis

1 Einleitung, Projektkontext, wichtigste Ergebnisse

Das Projekt TrustVote hatte zum Ziel, einen Prozess der Verbesserung der E-Voting-Situation in der Schweiz zu lancieren. Mit Hilfe von Vertrauens- und Bedrohungsmodellen sollten die aktuellen Systeme Genf, Neuenburg und Zürich analysiert werden, und, falls nötig, Verbesserungsvorschläge ausgearbeitet werden. Eher begleitend war vorgesehen, eine partielle Implementation eines E-Voting-Systems[1] zu realisieren.

Auf Grund des Mangels an frei erhältlichen Publikationen, aber auch auf Grund der Ansicht, dass E-Voting-Systeme auf der Basis von Transparenz, und nicht auf der Basis von blindem Vertrauen, gebaut sein sollten, wurde die Tätigkeit des Modellierens durch das Studium moderner E-Voting-Protokolle ersetzt, und es wurde ein eigenes E-Voting-Protokoll *Napkin*, da später in *TrustVote*-Protokoll unbenannt wurde, ersetzt.

Projektbeginn:	01.01.2008
Projektende:	30.06.2009
Aufwände:	1786 Personenstunden
Kosten BFH:	CHF 140'904
Projektmitarbeiter:	Bernhard Anrig, Emmanuel Benoist, Eric Dubuis, Rolf Haenni, David-Olivier Jaquet-Chiffelle, Reto Koenig, Severin Hauser (Assistent)

Die wichtigsten, handfesten Ergebnisse könne wie folgt zusammengefasst werden:

- Organisation und Durchführung des Swiss E-Voting Workshops vom 5.06.09
- Das TrustVote-Protokoll,ein E-Voting-Protokoll, das Transparenz in E-Voting-Systemen verspricht, siehe Forschungsbericht BFH-TI Nr. 6 vom 1.08.09
- Die TrustVote-Implementation

Im Kapitel 2 listen wir die wichtigsten Tätigkeiten bzw. Meetings, Ereignisse und Ergebnisse auf. Im Kapitel 3 beschreiben wir die erreichte Valorisierung. Kapitel 4 bilden den Schluss und den Ausblick.

2 Tätigkeiten/Meetings, Ereignisse und Ergebnisse

In diesem Kapitel listen wir die wichtigsten Tätigkeiten/Meetings, Ereignisse und Ergebnisse in chronologischer Reihenfolge auf.

Nr.	Datum	Kategorie	Was
1	17.01.08	Meeting	Kick-off-Meeting Endre Bangerter verlässt aus Zeitgründen das Projekt. Er wird durch Emmanuel Benoist ersetzt (ab 1.09.08).
2	ab	Ereignis	Einarbeitung in das Thema elektronische Wahlen, Suche nach Literatur

1 Wir beschäftigen uns ausschliesslich mit elektronischen Abstimmungs- und Wahlsystemen übers Internet. Diese sollten richtigerweise I-Voting-System heissen; aus Konsistenzgründen bleiben wir aber beim Begriff E-Voting-System.

	17.01.08		über die Schweizerischen Systeme. Es zeigte sich bald einmal, dass es über die Schweizerischen Systeme keine (Neuenburg), nur zwei widersprüchliche (Zürich), oder mehrere, zum Teil auch widersprüchliche (Genf), öffentliche zugängliche Beschreibungen gibt.
3	22.02.08	Meeting	Erste Ergebnisse der Suche nach Literatur über die Schweizerischen System werden vorgestellt. Reto Koenig stösst zum Projekt. Die Anstellung des Forschungsassistenten wird solange hinausgeschoben, bis die Anforderungen an eine Implementation eines transparenten elektronischen Wahlsystems festgelegt sind.
4	17.03.08	Meeting	Teilergebnisse der Analysen der Schweizerischen Systeme werden diskutiert. Es entsteht die Erkenntnis, dass die Systeme Genf und Zürich nicht transparent sind, und dass nur auf Grund der spärlichen Dokumente und ohne weitere Zusatzinformationen, die nur vertraulicher Art sein können, gar keine gründliche Analyse (zum Beispiel in Form von sogenannten *attack trees*) gemacht werden können. Vom System von Neuenburg gibt es keine direkten Informationen; wir haben über Umwege herausgefunden, dass Neuenburg ein System der kommerziellen Firma Scytl, Barcelona, Spanien, einsetzt.
5	07.04.08	Meeting	Weitere Analyse-Berichte über Genf, Zürich und das System von Estland. (Estland hat ein E-Voting-System eingesetzt, das auf einer PKI für die Stimmbürger beruht.) David-Olivier Jaquet-Chiffelle hätte Zugang zu vertraulichen Dokumenten des Kantons Neuenburg; das Projekt entscheidet, zwecks allfälliger Publikation von Resultat *nicht* auf vertraulich eingestufte Dokumente zurückgreifen zu müssen; als Konsequent verzichten wir im Projekt auf vertrauliche Dokumente.
6	21.04.08	Ereignis	Für E-Voting im Kanton Bern ist die Berner Staatskanzlei, Herr Tilman Braun, zuständig.
6	21.05.08	Meeting	Rolf Haenni stellt eine Übersicht über die in der Wissenschaft bekannten E-Voting-Protokolle zusammen. Keines der Schweizerischen Systeme (mit Ausnahme vielleicht von Neuenburg) baut auf einem bekannten, publizierten E-Voting-Protokoll auf.
8	12.06.08	Meeting	Stephan Fischli präsentiert den OASIS Standard EML (*Election Markup Language*)
9	13.06.08	Ergebnis	Verein eCH: Themenantrag „Vote électronique“ eingereicht. Eric Dubuis hat beim Fachverein eCH obigen Themenantrag eingereicht (Mitantragssteller ist Prof. U. Ultes-Nitsche, Universität Fribourg). Das Projekt war der Meinung, dass die Aspekte der Modellierung und Analyse der Sicherheit der Schweizerischen System auf Ebene des Fachvereins Sinn macht.
10	16.07.08	Meeting	Sitzung bei der Bundeskanzlei (BK). Anwesende seitens BK: Hans-Urs Wili, Sektionschef Politische Rechte, Ardita Driza Maurer, Leiterin der Arbeitsgruppe „Vote électronique“, Daniel Muster. Anwesende seitens Akademie: Ulrich Ultes-Nitsche, Universität Fribourg, Eric Dubuis und Rolf Haenni, BFH. Themen: Vorstellung des Projektes, Plan eines Workshops.
11	07.08.08 – 09.08.09	Ereignis	Besuch der Konferenz EVOTE08 in Bregenz durch Eric Dubuis, Rolf Haenni und Reto Koenig.
12	01.09.08	Ergebnis	Die Website *Swiss Competence Center for E-Voting Technologies* (www.e-voting-cc.ch) geht online.
13	12.09.08	Ereignis	Wir erhalten den negativen Entscheid von eCH, das Thema „Vote électronique“ im Rahmen eCH zu diskutieren. Auszug aus dem E-Mail des eCH-Geschäftsführers, Nicolai Lütschg: Der Expertenausschuss hat Ihren Themenantrag abgelehnt. Die Begründung:

			• Standards zu diesem Thema existieren bereits, bzw. sind in Arbeit • das Thema ist vorwiegend politisch besetzt • die Themenhoheit ist bei der Bundeskanzlei angesetzt, nicht bei eCH
14	17.09.08	Meeting	Forschungsassistent Severin Hauser wird per 1.10.08 angestellt. Die Implementation eines E-Voting-Systems (Funktionsmusters), basierend auf blinden Signaturen und *secret key sharing* wird gestartet. Leitung: Stephan Fischli.
15	01.10.08	Ergebnis	Förderungsantrag an den SNF *SecVote: Secure E-Voting* zur Finanzierung zweier Doktoranden.
16	02.10.08	Ergebnis	Vorstellung unseres Projektes und unserer Ziele anlässlich der Sitzung des interkantonalen Arbeitsgruppe „vote électronique“.
17	24.10.08	Ergebnis	Publikation des Forschungsberichts BFH-TI Nr. 5 vom 24.10.08, *Research on E-Voting Technologies*. Autoren sind: Rolf Haenni, Eric Dubuis und Ulrich Ultes-Nitsche.
18	05.11.08	Ergebnis	Präsentation „E-Voting – Wie weit sind wir?“ durch Eric Dubuis im Rahmen des FAEL-Anlasses Internet Security - Wo lauern die Gefahren?
19	11.03.09	Ereignis	Der SNF empfiehlt uns, den SNF-Förderantrag zurückzuziehen. Entscheid: die moderaten Mängel zu beheben, und den daraus resultierenden Antrag an die Hasler Stiftung einzureichen.
20	23.03.09	Ergebnis	Der Forschungsbericht „*A Hybrid E-Voting System for Large-Scale Elections*“, von Rolf Haenni, Reto Koenig, Stephan Fischli und Eric Dubuis wurde an der Tagung VoteID 2009 eingereicht.
21	27.03.09	Ergebnis	Förderantrag an die Hasler Stiftung *SwissVote: Secure Internet Voting in Switzerland* zwecks Finanzierung zweier Doktoranden.
22	14.05.09	Ereignis	Besuch des Workshops „Elektronische Wahlen“ in Darmstadt.
23	20.05.09	Meeting	Besuch der Staatskanzlei des Kantons Genf, Herrn Michel Warynski, durch Ulrich Ultes-Nitsche, Stephan Fischli und Eric Dubuis. Herr Warynski erläutert uns das Genfer E-Voting-System.
24	22.05.09	Ereignis	Der Forschungsbericht „*A Hybrid E-Voting System for Large-Scale Elections*“, eingereicht an der Tagung VoteID 2009, wurde *nicht* akzeptiert.
25	29.05.09	Ergebnis	In der Zeitung „Der Bund“ erscheint ein kritischer Artikel zum Thema „E-Voting“, welcher auf der Basis eines Interviews des Autors mit Bernhard Anrig, Eric Dubuis und Rolf Haenni verfasst wurde.
26	05.06.09	Ergebnis	Organisation und Durchführung des ersten Swiss E-Voting Workshops im Schloss Münchenwiler: • Mehr als 60 Teilnehmer, aus den Bereichen Administration, Akademie und Wirtschaft • 5 wissenschaftliche Präsentationen, mit zum Teil Referenten aus dem Ausland • Präsentationen der 3 Schweizerischen Systeme • Podiumsgespräch, Leitung Peter Fischer, Informatikstrategieorgans des Bundes • Einnahmen: 13'300 CHF • Ausgaben: 10'300 CHF • Einnahmeüberschuss: 3'000 CHF • Organisationsaufwand: 470 Personenstunden
27	05.06.09	Ergebnis	Rolf Haenni referiert anlässlich des Swiss E-Voting Workshops über das Thema: „*Signatures aveugles: une approche pour éviter la confiance aveugle*“. Ausgehend von den allgemeinen Anforderungen an elektronische Wahlsysteme präsentiert Rolf Haenni das TrustVote-Protokoll und zeigt, dass es die Anforderungen bis auf einen Punkt erfüllt.
28	05.06.09	Ergebnis	Die erste Version der TrustVote-Implementation, basierend auf Web-

			Services und mehreren Java EE-Anwendungsservern, wird anlässlich des Swiss E-Voting Workshops vorgeführt.
29	9.6.09 ff.	Ereignis	Michel Warynski und Michel Chevallier, Staatskanzlei Genf, verlangen eine Erklärung, wieso unsere Meinung im Artikel des Bundes vom 29.05.09 so negativ sei. Erklärung erfolgte; der Kooperationswille seitens des Kantons Genf ist vermutlich nicht (mehr) vorhanden. Mit der E-Mail vom 19.06.09 von Eric Dubuis, in der versprochen wird, dass in Zukunft im Umgang mit den Medien Vorsicht zu walten sein, ist die Angelegenheit erledigt.
30	Im Juni 09	Ergebnis	Radio Fribourg sendet ein Kurzinterview mit Rolf Haenni.
31	30.06.09	Ereignis	Formelles Ende des Projekts Es werden keine geleisteten Stunden auf das Projektkonto gebucht.
32	08.07.09	Ergebnis	Bewilligung des Fördergesuchs durch die Hasler Stiftung. Sie finanziert für eine Dauer von drei Jahren zwei Doktoranden mit dem Betrag von CHF 351'000.
33	01.08.09	Ergebnis	Publikation des Forschungsberichts BFH-TI Nr. 6 vom 1.08.09, *TrustVote: A Proposal for a Hybrid E-Voting System*. Autoren sind: Rolf Haenni, Reto Koenig, Stephan Fischli und Eric Dubuis.
34	10.08.09 – 11.08.09	Ergebnis	Präsentation des TrustVote-Implementation (monolithische Version) anlässlich der EVT-WOTE 2009 in Montreal, Kanada.
35	07.09.09	Ereignis	Besuch der Konferenz VoteID 2009 durch Eric Dubuis und Reto Koenig
36	01.10.09	Ereignis	Die Doktoranden, Oliver Spycher und Reto Koenig, beginnen mit ihrer dreijährigen Dissertation. Die Betreuer sind: Ulrich Ultes-Nitsche, Universität Fribourg, und Rolf Haenni und Eric Dubuis, BFH.
37	27.10.08	Meeting	Sitzung bei der Bundeskanzlei. Teilnehmer seitens BK: Hans-Urs Wili, Ardita Driza Maurer, Daniel Mustern; seitens Akademie: Ulrich Ultes-Nitsche, Rolf Haenni, Eric Dubuis. Themen: Nachbesprechung des Workshops vom 5. Juni 2009, neuer Workshop.
38	28.10.09	Ereignis	Peter Ryan, Professor an der Universität Luxemburg, E-Voting-Spezialist und Mit-Organisator der Tagung VoteID 2009, ist an einer Zusammenarbeit mit uns interessiert. Erste konkrete Möglichkeit: Referat anlässlich des Workshops 2010, siehe unten.
39	24.11.08	Meeting	Sitzung bei der Bundeskanzlei. Teilnehmer seitens BK: Hans-Urs Wili, Daniel Mustern; seitens Akademie: Ulrich Ultes-Nitsche, Rolf Haenni, Eric Dubuis. Thema: Workshops 2010 und 2011. Der Workshop 2010 soll anfangs September stattfinden; er richtet sich eher an Techniker; die inhaltliche Verantwortung wird durch die Akademie wahrgenommen. Der Workshop 2011 soll im Februar oder März 2011 stattfinden; er richtet sich eher an Politiker, Juristen und Medienfachleute; die inhaltliche Verantwortung wird durch die Bundeskanzlei wahrgenommen.

3 Valorisierung

In diesem Kapitel wird die erreichte Valorisierung aufgelistet. Die Auflistung erfolgt in absteigender Priorität in Bezug auf die Wichtigkeit der Erreichten, wobei die Priorisierung unser Selbsteinschätzung ist.

Priorität	Nr.	Was
1	26	Organisation und Durchführung des ersten Swiss E-Voting Workshops im Schloss Münchenwiler Das Echo der Teilnehmer war sehr positiv. Die Rückmeldungen haben ergeben, dass im Jahre 2010 wieder ein Workshop gewünscht wird.
2	10, 37, 39	Kontakt mit der Bundeskanzlei Dank diesem Kontakt sind wir in der Schweiz bekannt. Wir werden wahrgenommen, allerdings zur Zeit noch als (unangenehme) Kritiker.

3	20, 24, 33	Das TrustVote-Protokoll Unser erster Versuch, ein E-Voting-Protokoll, das Transparenz verspricht, zu definieren. Leider hat es nicht zur Publikation bei der VoteID 2009 gereicht. Die Reviewer fanden Schwachstellen, die wir in wesentlichen Teile beheben konnten, siehe Forschungsbericht BFH-TI Nr. 6 vom 1.08.09 (33).
4	34	TrustVote-Implementation Die zweite Version der Implementation des TrustVote-Protokoll erlaubt es, auf einfache Art und Weise zu demonstrieren, wie das TrustVote-Protokoll funktioniert. Diese Implementation konnten wir in Kanada vorführen. Dabei konnten wir wertvolle Kontakte knüpfen.
5	21, 32	SwissVote, Förderung der Hasler-Stiftung Mit dem Förderantrag an die Hasler Stiftung konnte wir die Finanzierung von zwei Doktoranden für drei Jahre erreichen.
6	37, 39	Weitere Workshop bzw. Tagungen zum Thema E-Voting Zusammen mit der Bundeskanzlei sind Workshops bzw. Tagungen im 2010 und 2011 geplant bzw. die Vorbereitungen laufen.
7	11, 22, 34, 35	Vernetzung Dank zahlreichen Kontakten und Konferenzbesuchen konnten wir uns vernetzen. Dies erleichtert zum Beispiel stark das Organisieren eines E-Voting-Anlasses in der Schweiz.
8	23, 29	Kontakt mit Genf Aus unsere Sicht war der Kontakt mit Genf sehr nachhaltig. Leider sehen das die Genfer Kollegen nicht ganz so.
9	17	Übersichtsbericht Der Forschungsbericht beschreibt die modernen Ansätze beim E-Voting und erleichtert den Einstieg ins Thema.

4 Schlusswort und Ausblick

Das Projekt hat für jeden einzelnen einen Schub an Erfahrung gebracht. Wir haben unsere Kompetenzen in den Themen kryptographische Anwendungen, Sicherheit und Schutz der Privatsphäre festigen und ausbauen können, was sich im Bereich Lehre (Unterricht) und im Bereich Forschung (Akquisition) auszahlen wird.

Aus der Sicht der Dritt-Finanzierung von Folgeprojekten ist das Thema E-Voting ein Spezialfall: Zwar ist es, unserer Meinung nach, von grosser Wichtigkeit, aber die Hauptforderung, nämlich nach dem Bau von offenen (z.B. Open Source) und transparenten (das heisst, auf modernsten kryptographischen Erkenntnissen aufbauend) E-Voting-Systemen, hindert die Privatwirtschaft, in dieses Geschäft einzusteigen. Also bleibt „nur“ die öffentliche Hand; und da sind wir am Ball.

Zum Ausblick können wir im Moment festhalten, dass wir das Thema in Form von Betreuung von Doktoranden weiter bearbeiten, und dass wir im Bereich Valorisierung die Workshops 2010 und 2011 durchführen werden. Eine weitere Idee, nämliche das Etablieren eines interkantonalen Konsortiums für den Bau eines neuen, transparenten E-Voting-Systems, ist erst angedacht; es könnte frühestens in der zweiten Hälfte 2010 greifen.