UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen

Katharina Bräunlich et al.

Nr. 11/2011

Arbeitsberichte aus dem Fachbereich Informatik

Universität Koblenz-Landau • Campus Koblenz • Universitätsstraße 1 • 56070 Koblenz
Telefon +49 261 287-0 • http://www.uni-koblenz.de

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Grimm

Kontaktdaten der Verfasser

Katharina Bräunlich, Rüdiger Grimm, Andreas Kasten, Sven Vowé, Nico Jahn
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
Email: hupfi@uni-koblenz.de, grimm@uni-koblenz.de, stultissimum@uni-koblenz.de, nicojahn@uni-koblenz.de, sven.vowe@sit.fraunhofer.de

Der neue Personalausweis zur Authentifizierung von Wählern bei Onlinewahlen

Verbesserungsvorschlag zur sicheren Geheimhaltung der Wahl

Katharina Bräunlich[1], Rüdiger Grimm[1], Andreas Kasten[1], Sven Vowé[2] und Nico Jahn[1]

[1]Insitut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau
[2]Fraunhofer-Institut für Sichere Informationstechnologie

Zusammenfassung

In diesem Arbeitsbericht werden zuvor nicht identifizierte Bedrohungen bezüglich des Wahlgeheimnisses des in [BKG11] vorgeschlagenen Konzeptes zur Authentifizierung von Wählern bei elektronischen Wahlen mittels des neuen Personalausweises aufgezeigt. Überdies wird mit der Einführung einer zwischengelagerten Anonymisierungsschicht eine Lösung vorgeschlagen, wie eben diese Bedrohungen abgewehrt werden können.

1 Einleitung

Im November 2010 wurde der neue elektronische Personalausweis deutschlandweit eingeführt. In seiner Grundfunktion bleibt er als staatlich anerkanntes Ausweisdokument bestehen, besitzt aber zusätzliche elektronische Funktionen. Hierzu zählt die eID-Funktion, die eine Online-Authentifizierung des Bürgers gegenüber einem Dienstanbieter im Internet ermöglicht.

In [BKG11] wird ein Konzept zur Wählerauthentifizierung bei Onlinewahlen mittels der eID-Funktion des neuen Personalausweises (nPA) im Rahmen von politischen Wahlen wie etwa Bundestagswahlen vorgeschlagen. Die Onlinewahl wird dabei als zusätzliche Wahlmöglichkeit zur herkömmlichen Präsenzwahl verstanden, die die Briefwahl als Fernwahl ersetzt. Jeder Wahlberechtigte kann seine Stimme entweder vom heimischen Computer oder vor Ort im Wahllokal abgeben. Die zugrundeliegende Idee in [BKG11] ist die Verwendung der sogenannten Restricted-ID, um berechtigte Wähler sicher zur Onlinewahl zuzulassen und dabei gleichzeitig die Geheimhaltung der Stimmabgabe zu gewährleisten. Der Wähler authentifiziert sich mittels der eID-Funktion des neuen Personalausweises gegenüber der Onlinewahlanwendung, die dem Dienstanbieter entspricht. Dabei wird der Wähler lediglich anhand der Restricted-ID authentifiziert, die

während der eID-Funktion vom Personalausweis berechnet wird. Im weiteren Verlauf der Wahlhandlung wird die Restricted-ID als eine Art Sitzungsnummer verwendet. Bei jedem Schritt des Wahlvorganges sendet der Wähler seine Restricted-ID mit. Jeder Schritt – darunter zählt auch die Stimmabgabe – kann somit genau einem Wähler zugeordnet werden. Nach [BKG11, Abschnitt 3.2] erfolgt die Berechnung der Restricted-ID derart, „dass die resultierende Restricted-ID nicht auf die ursprünglichen Datenfelder zurückgeführt werden kann." Damit ist selbstverständlich gemeint, dass die Restricted-ID nicht auf die bürgerliche Identität des Wählers verweist. Aufgrund dieser Voraussetzung wird die Restricted-ID dort zur Wählerauthentifzierung verwendet und mit der elektronischen Stimme verknüpft in der digitalen Urne abgelegt.

In diesem Ansatz wird also davon ausgegangen, dass aus der Restricted-ID die bürgerliche Identität des Personalausweisinhabers nicht abgeleitet werden kann. Leider kann davon aber aufgrund der Spezifikation des neuen Personalausweises nicht ausgegangen werden. Bei einer Kooperation zwischen dem eID-Server und der Zertifizierungsstelle des neuen Personalausweises können mindestens alle denkbaren Resticed-IDs dieser Wahlanwendung wiederholt berechnet werden und dann die gesuchte Restricted-ID durch Vergleich herausgefunden werden. Ein solches Zusammenspiel zwischen dem eID-Server und der Zertifizierungsstelle ist aufgrund des Konzeptes der „Separation-of-Duty" zwischen diesen beiden Parteien so lange als unwahrscheinlich anzusehen, als diese Parteien nicht ein gemeinsames manipulatives Interesse haben. Bei Wahlen außerhalb des Interessensbereichs des Bundes wie etwa Vereinswahlen oder Gremienwahlen im Sozial- oder Bildungsbereich kann von divergierenden Interessen ausgegangen werden. Bei Wahlen im Interessensbereich des Bundes wie etwas Bundestags- oder Landtagswahlen dagegen muss die Möglichkeit der manipulativen Kooperation zwischen dem eID-Service sowie den zentral kontrollierten Zertifizierungsinstanzen des neuen Personalausweises berücksichtigt werden. Dies ist in [BKG11] nicht geschehen.

In diesem Artikel wird daher das in [BKG11] vorgeschlagene Konzept unter diesen Voraussetzungen neu analysiert und bewertet. Es werden dabei nicht berücksichtigte Bedrohungen bezüglich der Gefährdung des Wahlgeheimnisses identifiziert, welche sich aus einer manipulativen Kooperation zwischen eID-Service und Zertifizierungsinstanzen ergeben. Darüber hinaus wird mit der Einführung einer zwischengeschalteten Anonymisierungsschicht eine Lösung zur Abwehr eben dieser Bedrohungen aufgezeigt.

Dieser Artikel gliedert sich wie folgt. In Abschnitt 2 wird das in [BKG11] veröffentlichte Konzept zur Wählerauthentifizierung mittels des nPA vorgestellt. In Abschnitt 3 wird auf die Rückführbarkeit der Restricted-ID eingegangen. In Abschnitt 4 wird ein Verbesserungsvorschlag des in [BKG11] vorgestellten Konzeptes beschrieben. Dieser wird anschließend hinsichtlich möglicher Bedrohungen analysiert und bewertet. Der Artikel schließt mit einem Fazit.

2 Wählerauthentifizierung mittels des nPA nach [BKG11]

Ein Online-Wahlsystem ist eine verteilte Anwendung, die sich aus einer clientseitigen Wahlanwendung (Wahlclient) und einer serverseitigen Wahlanwendung

(Wahlserver) zusammensetzt. Der Bürger verwendet den Wahlclient, um die Wahlhandlung auf seinem Computer auszuführen. Der Wahlclient kommuniziert über das Internet mit dem Wahlserver. Der Wahlserver implementiert die digitale Urne, das digitale Wählerverzeichnis und das Bulletin Board. Die Urne speichert die abgegebenen Stimmen, das Wählerverzeichnis registriert alle Wahlberechtigten und den Status ihrer Stimmberechtigung und das Bulletin Board [Ben87] ist ein öffentlicher Kanal wie etwa eine Webseite. Auf diesen öffentlichen Kanal kann jeder lesend zugreifen, aber nur berechtigte Parteien können Daten schreiben. Zudem können bereits geschriebene Daten weder gelöscht noch verändert werden.

Um einen Wähler eindeutig zu identifizieren und zu authentifizieren, erfordert die Wahlhandlung eine Anmeldung. Das in [BKG11] beschriebene Konzept zur Wählerauthentifikation verwendet die eID-Funktion des nPA.

2.1 Benötigte Funktionen des nPA

Im Folgenden werden diejenigen Datenfelder und Funktionen des nPA beschrieben, welche für die Wählerauthentifizierung nach [BKG11] benötigt werden.

2.1.1 Überprüfung der Wahlberechtigung

In der Regel sind bei politischen Wahlen in Deutschland alle deutschen Staatsbürger wahlberechtigt, die am Tag der Wahl das 18. Lebensjahr vollendet haben. Die deutsche Staatsangehörigkeit ergibt sich bereits durch den Besitz eines neuen Personalausweises.[1] Um die Volljährigkeit des Wählers sicherzustellen, kann die Altersverifikation verwendet werden. Mittels der Altersverifikation kann überprüft werden, ob ein Bürger ein bestimmtes Alter erreicht hat oder nicht. Bei der Altersverifikation wird ein Vergleichsdatum an den Personalausweis gesendet. Dieses Datum gibt denjenigen Tag an, an dem der Ausweisinhaber spätestens geboren sein muss. Liegt das Datum vor dem gespeicherten Geburtsdatum, schlägt die Altersverifikation fehl und der Ausweis sendet ein „nein“ zurück. Andernfalls sendet der Ausweis ein „ja“ zurück. Das genaue Geburtsdatum des Wählers ist bei der Altersverifikation nicht relevant und wird nur vom Personalausweis selbst verarbeitet.

2.1.2 Ermitteln des Wahlkreises

Untergliedert sich eine politische Wahl in Erst- und Zweitstimme wie etwa bei Bundestagswahlen, so wählt der Wähler mit der Erststimme den Direktkandidaten seines Wahlkreises. Dieser Wahlkreis kann im Rahmen der eID-Funktion mittels der Wohnortabfrage ermittelt werden. Die Wohnortabfrage überprüft, ob ein Wähler in einer bestimmten Gemeinde wohnt oder nicht. Die genaue Anschrift des Bürgers wird bei der Wohnortabfrage nicht ausgelesen. Aus dem Ergebnis dieser Abfrage können dann die Direktkandidaten abgeleitet werden. Voraussetzung hierfür ist, dass eine Gemeinde genau einem Wahlkreis zugeordnet werden kann und es somit keine Gemeinde gibt, die in mehr als zwei Wahlkreisen liegt. Eine direkte Abfrage der Gemeinde ist nicht möglich. Daher

[1] Reicht dies zur Überprüfung der Staatsangehörigkeit nicht aus, kann zusätzlich noch das Datenfeld des ausstellenden Staates ausgelesen werden.

kann folgendes Verfahren verwendet werden: Der Wähler erhält mit seiner Wahlbenachrichtigung eine Information darüber, welchem Wahlkreis er zugeordnet ist. Möchte er elektronisch wählen, so stellt ihm die Wahlanwendung eine Liste aller Wahlkreise zur Verfügung. Der Wähler wählt im Wahlinterface denjenigen Wahlkreis aus, der ihm laut der Wahlbenachrichtigung zugeordnet wurde. Die Wohnortabfrage wird anschließend dazu verwendet, um die Eingabe des Wählers zu überprüfen. Schlägt diese Überprüfung fehl, muss die Auswahl des Wahlkreises korrigiert werden. Anderenfalls wurde der Wahlkreis korrekt erfasst und die zugehörigen Direktkandidaten können dem Wähler angezeigt werden.

2.1.3 Pseudonymisierung der Wahl

Die Pseudonymisierung der Wahl beruht in [BKG11] auf der Verwendung der Restricted-ID. Die Restricted-ID ist ein Pseudonym, das direkt an eine Kombination aus einem Personalausweis und einem Dienstanbieter gebunden ist. Die Restricted-ID wird errechnet aus einem geheimen Datum des Personalausweises und einem öffentlichen Datum des Berechtigungszertifikats[2] der Wahlanwendung. Unter der Voraussetzung, dass für die Wahlanwendung genau ein Berechtigungszertifikat existiert, identifiziert die Restricted-ID jeden Wähler eindeutig. Die Restricted-ID wird dann als eine Art Sitzungsnummer verwendet. Bei jedem Schritt des Wahlvorganges sendet der Wähler seine Restricted-ID mit. Jeder Schritt kann somit genau einem Wähler zugeordnet werden.

2.2 Ablauf der Wahlhandlung nach [BKG11]

Im Folgenden wird die Wählerauthentifizierung gemäß [BKG11] beschrieben. Für ein besseres Verständnis wird die Wählerauthentifizierung in den Gesamtablauf einer Wahlhandlung eingebettet. Überdies wird der Ablauf der Wahlhandlung anhand von Abbildung 1 verdeutlicht.[3]

Zunächst ruft der Wähler über seinen Webbrowser die Webseite des Wählerverzeichnisses auf. Das Wählerverzeichnis initiiert die Durchführung der eID-Funktion wie in [Bun10b] beschrieben. Im vorletzten Schritt der eID-Funktion liegen beim eID-Server die Restricted-ID sowie alle weiteren zur Überprüfung der Wahlberechtigung notwendigen Daten vor (siehe Abschnitt 2.1). Im letzten Schritt leitet der eID-Server diese Daten schließlich über eine gesicherte Verbindung an das Wählerverzeichnis weiter. Die Übertragung erfolgt dabei verschlüsselt und signiert.

Das Wählerverzeichnis überprüft nun die Wahlberechtigung des Wählers. Anschließend leitet das Wählerverzeichnis die Restricted-ID zusammen mit dem Stimmzettel an den Wähler weiter.

Der Wähler gibt seine Stimme ab, indem er seinen Stimmzettel verschlüsselt und diesen zusammen mit seiner Restricted-ID an die Wahlurne sendet. Die Urne fragt daraufhin beim Wählerverzeichnis nach, ob der zu der Restricted-ID zugehörige Wähler bereits eine Stimme abgegeben hat. Hat der Wähler bereits eine Stimme abgegeben, wird die Stimme von der Urne verworfen und

[2] Ein solches Berechtigungszertifikat identifiziert den Dienstanbieter gegenüber dem Personalausweis. Zugleich enthält es eine Auflistung derjenigen Datenfelder, die der Dienstanbieter vom Ausweis auslesen darf. Das Auslesen zusätzlicher Datenfelder ist nicht möglich.

[3] Der Übersicht halber wurde der Ablauf der eID-Funktion in der Abbildung vereinfacht dargestellt. Der eID-Client und der Personalausweis sind daher nicht explizit aufgeführt.

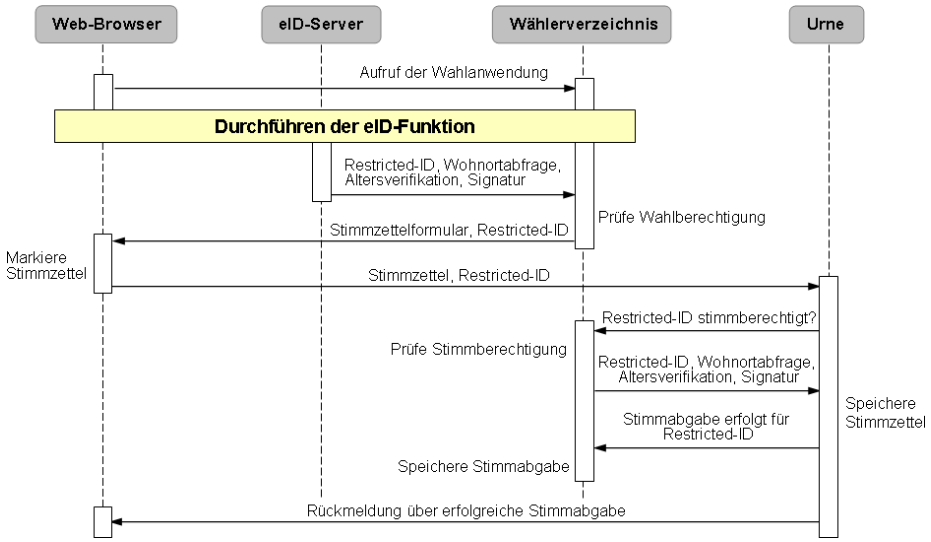

Abbildung 1: Sequenzdiagramm über den Ablauf der Wahlhandlung [BKG11]

der Wähler erhält eine Rückmeldung über seine fehlende Stimmberechtigung. Anderenfalls speichert die Urne die verschlüsselte Stimme und die zugehörige Restricted-ID. Anschließend sendet die Urne die Restricted-ID an das Wählerverzeichnis und teilt diesem dadurch mit, dass der zugehörige Wähler seine Stimme nun erfolgreich abgegeben hat. Das Wählerverzeichnis aktualisiert daraufhin den Status der Stimmberechtigung zu dieser Restricted-ID.

Nach Beendigung der Wahl werden auf dem Bulletin Board folgende Daten veröffentlicht: alle vom eID-Server signierten Restricted-IDs aus dem Wählerverzeichnis sowie alle verschlüsselten Stimmzettel aus der Urne zusammen mit der Restricted-ID des zugehörigen Wählers.

3 Rückführbarkeit der Restricted-ID

Wie in Anhang A beschrieben, kann die Restricted-ID theoretisch zurückgeführt und der Identität eines Bürgers zugeordnet werden. Anhand der Daten des Bulletin Boards kann damit jeder Bürger mit einer abgegebenen Stimme verknüpft und so das Wahlgeheimnis aufgehoben werden. Dies ist allerdings nur dann möglich, wenn der eID-Server und die Zertifizierungsstelle des neuen Personalausweises kooperieren. Dies ist im Rahmen herkömmlicher eID-Anwendungen wie etwa im e-Commerce aufgrund divergierender Interessen als unwahrscheinlich anzusehen. Im Zuge von Onlinewahlen – insbesondere auf Bundesebene – kann eine derartige manipulative Kooperation jedoch nicht ausgeschlossen werden und muss dementsprechend bei einer Bedrohungsanalyse berücksichtigt werden.

4 Einführung einer zwischengeschalteten Anonymisierungsschicht

Im Folgenden wird das in [BKG11] vorgestellte Konzept zur Wählerauthentifizierung um eine zwischengelagerte Anonymisierungsschicht nach Vorbild des eCash-Verfahrens [Cha81, Cha83, Cha85, CFN90, Cha92] ergänzt.

Mit der Einführung dieser Anonymisierungsschicht findet ein fundamentales Prinzip für Sicherheitsfragen in offenen Kommunikationsumgebungen Anwendung. Demnach muss ein Sicherheitsmechanismus so ausgelegt sein, dass derjenige, der ein Interesse an einer Sicherheitsanforderung hat, auch die zugehörigen Sicherheitsmaßnahmen kontrolliert [GN02, Abschnitt 4]. In dem geschilderten Kontext von Onlinewahlen darf die Unverknüpfbarkeit von Stimme und Wähleridentität demnach nicht außerhalb des Machtbereichs des Wählers liegen. Vielmehr muss der Wähler die Unverknüpfbarkeit seiner Identität mit der von ihm abgegebenen Stimme selbst durchsetzen können. Eben dies leistet die Restricted-ID des neuen Personalausweises nicht direkt. In Hinblick auf die Restricted-ID hängt die Anonymität des Wählers davon ab, dass sich zwei der drei beteiligten Parteien (eID-Server und Zertifizierungsstelle) wohlverhalten. Deshalb muss – und kann – eine Anonymisierungsschicht zwischengeschaltet werden. Diese zwischengelagerte Anonymisierungsschicht wahrt auch dann das Wahlgeheimnis, wenn alle anderen beteiligten Parteien sich illegal verhalten. Mittels der Anonymisierungsschicht wird nicht die Restricted-ID selbst, sondern ein vom Wahlclient erzeugtes, nicht-aufdeckbares Pseudonym als Kennzeichen der abgegeben Stimme verwendet. Dieses nicht-aufdeckbare Pseudonym wird im Folgenden mit Wahlstimmen-ID bezeichnet.

Die anonyme Stimmabgabe mittels der Wahlstimmen-ID beruht auf der Technik der Münztoken wie sie beispielweise im eCash-Verfahren der Deutschen Bank von 1996 bis 2001 auf dem Markt technisch erfolgreich eingesetzt wurde [GZ96, Gri01, Net01]. Solche nicht-aufdeckbaren Pseudonyme sind mit Hilfe der blinden Signatur sicher herzustellen. In [Cha81, Cha83, Cha85, CFN90, Cha92] ist das Verfahren auf der Basis der „Blinden Signatur“ ausführlich beschrieben, welches das anonyme Ausgeben digitaler Münzen (DigiCash, eCash) sowie die gleichzeitige Abwehr von „Double Spending“ von Münzen erlaubt. Wie schon in [Cha81] prinzipiell angedacht, lässt sich das Verfahren entsprechend auf die anonyme Stimmabgabe bei gleichzeitiger Abwehr der mehrfachen Stimmabgabe übertragen. Dies wird im Folgenden detailliert geschildert und zum besseren Verständnis in den Ablauf der Wahlhandlung eingebettet.

4.1 Benötigte Funktionen des nPA

Für die Wählerauthentifizierung mit einer zwischengeschalteten Anonymisierungsschicht werden alle der in Abschnitt 2.1 geschilderten Daten und Funktionen des nPA benötigt.

In [BKG11] wird die Annahme getroffen, dass der eID-Server vertrauenswürdig ist. Es besteht weiterhin die Möglichkeit, den eID-Server als nicht vertrauenswürdig vorauszusetzen. Der eID-Server könnte etwa fiktive Identitäten erzeugen, indem er eigene Restricted-IDs generiert, und mit diesen eine Stimme abgeben. Um dies zu verhindern, könnte der eID-Server einer sozialen Kontrolle unterzogen werden. Durch eine derartige Kontrolle könnten die fiktiven Identi-

täten erkannt werden, wodurch auch die Stimmabgaben mit solchen Identitäten unterbunden wäre. Um eine manuelle Überprüfung der bürgerlichen Identität eines Wählers zu ermöglichen, würden zusätzlich zu den in Abschnitt 2.1 geschilderten Funktionen weitere Daten benötigt werden. Der Einfachheit halber sei im Folgenden davon ausgegangen, dass diese Überprüfung anhand von Vor- und Nachname des Wählers erfolgt. Dies dient in erster Linie einer transparenteren Wahlgestaltung. Dadurch kann der Wähler überprüfen, dass sein Status der Stimmabgabe korrekt erfasst wurde. Ebenso kann jeder Bürger für andere Bürger aus seinem sozialen Umfeld (zum Beispiel für Familienmitglieder oder Personen aus dem Bekanntenkreis) ebenfalls den Status der Stimmberechtigung überprüfen. Die Überprüfbarkeit beschränkt sich hierbei jedoch lediglich auf die Tatsache, ob eine Stimme abgegeben wurde oder nicht. Der Inhalt der Stimme bleibt weiterhin geheim. Darüber hinaus können auch die Stimmabgaben fiktiver Identitäten leichter erkannt werden. Schließlich erleichtert eine derartige zusätzliche Information auch den manuellen Abgleich mit der Papierwahl.

Sollte der eID-Server weiterhin als vertrauenswürdig angesehen werden, ist eine derartige zusätzliche Information nicht notwendig.

4.2 Modifizierter Ablauf der Wahlhandlung

Ebenso wie in [BKG11] wird hier kein vollständiges Wahlprotokoll beschrieben, sondern das dort vorgestellte Konzept zur Wählerauthentifizierung mittels des nPA in Hinblick auf das Wahlgeheimnis optimiert. Für ein besseres Verständnis wird die Wählerauthentifizierung jedoch in den Gesamtablauf einer Wahl eingebettet.

Die ersten Schritte der Wahlhandlung sind analog zu dem in Abschnitt 2.2 geschilderten Verfahren. Der Wähler ruft über seinen Webbrowser die Webseite des Wählerverzeichnisses auf. Die eID-Funktion wird vom Wählerverzeichnis gestartet und von den beteiligten Parteien durchgeführt. Nach der Durchführung der eID-Funktion liegen die Restricted-ID sowie alle weiteren benötigten Daten beim eID-Server vor. Der eID-Server signiert diese und leitet diese an das Wählerverzeichnis weiter. Das Wählerverzeichnis überprüft nun anhand der erhaltenen Daten die Wahlberechtigung des Bürgers. Zum einen wird anhand dieser Daten überprüft, ob es sich um einen im Wählerverzeichnis registrierten Wähler handelt und somit die Stimmabgabe mittels fiktiver Restricted-IDs durch den eID-Server verhindert. Zum Anderen wird die Wahlberechtigung des Bürgers anhand der im Wählerverzeichnis gespeicherten Stimmabgabevermerke überprüft. Ist der Bürger wahlberechtigt, so leitet das Wählerverzeichnis die Restricted-ID an den Bürger weiter. Anderenfalls erhält der Bürger eine entsprechende Rückmeldung und wird abgewiesen.

Das Wählerverzeichnis besteht aus den Restricted-IDs. Diese sind jedoch anders als in [BKG11] mit den Namen der Wähler verknüpft. Damit enthält dieses Online-Wählerverzeichnis Namen und Restricted-IDs derjenigen wahlberechtigten Wähler, die online wählen wollen. Genau wie bei der herkömmlichen Papierwahl stellt dies keine Kompromittierung des Wählerverzeichnisses dar, da das Wählerverzeichnis nicht anonym sein muss.

Hingegen müssen die Stimmzettel anonym bleiben, unabhängig davon, ob die Wahlorganisatoren und/oder Zertifizierungsinstanzen sich wohlverhalten oder nicht. Deshalb werden die Stimmzettel mit Wahlstimmen-IDs versehen. Diese Wahlstimmen-IDs werden vom Wahlclient selbst erzeugt. Dazu generiert der

Wahlclient eine Zufallszahl, die sogenannte Wahlstimmen-ID. Diese wird entsprechend zu den Berechnungen einer Blinden Signatur [Cha81, Cha83, Cha85, CFN90, Cha92] durch Einrechnung eines Blendfaktors verdeckt. Die so verdeckte Wahlstimmen-ID wird zusammen mit der Restricted-ID an das Wählerverzeichnis gesendet. Das Wählerverzeichnis kann nun anhand der Restricted-ID überprüfen, ob es sich um einen bereits authentifizierten Wähler handelt. Überdies kann auf Grund der Eindeutigkeit der Restricted-ID so das Erzeugen mehrerer Wahlstimmen-IDs zur mehrfachen Stimmabgabe durch ein und denselben Wähler unterbunden werden. Ist alles korrekt, so signiert das Wählerverzeichnis die vom Wahlclient erzeugte Wahlstimmen-ID blind. Durch diese blinde Signatur hat das Wählerverzeichnis keine Möglichkeit, eine Verbindung zwischen den originären Wahlstimmen-IDs und den Restricted-IDs der wählenden Bürger herzustellen. Das Wählerverzeichnis weiß lediglich, dass ein berechtigter Wähler unter Verwendung seiner Restricted-ID eine Wahlstimmen-ID angefordert hat (und kann ihn daran hindern, dies ein zweites Mal zu tun). Es weiß aber nicht, wie diese Wahlstimmen-ID aussieht, denn es signiert diese ja nur blind. Anschließ-end sendet das Wählerverzeichnis die blind signierte Wahlstimmen-ID zurück an den Wahlclient des Wählers, der unter Verrechnung des Blendfaktors die originäre Wahlstimmen-ID zurückrechnet.

Bei der späteren Stimmabgabe übermittelt der Wähler statt der Restricted-ID wie in [BKG11] diese vom Wählerverzeichnis signierte Wahlstimmen-ID an die Urne. Die Urne kann anhand dessen verifizieren, dass die vorgelegte Wahlstimmen-ID eine korrekte Signatur des Wählerverzeichnisses enthält. Sie kann sie daher anerkennen und jede spätere Wiederverwendung erkennen. Damit ist auch eine Korrektur von älteren Wahlstimmen völlig anonym möglich. Soll eine zuvor abgegebene Stimme korrigiert werden, so kann die Urne die für diese Wahlstimmen-ID gespeicherte Stimme identifizieren und durch die neue Stimme ersetzen. Nach erfolgreicher Stimmabgabe bzw. Korrektur der Stimme erhält sowohl der Wähler als auch das Wählerverzeichnis eine entsprechende Rückmeldung über die Stimmabgabe. Das Wählerverzeichnis vermerkt nun, dass für die entsprechende Wahlstimmen-ID eine Stimmabgabe erfolgt ist.

Nach Beendigung der Wahl werden auf dem Bulletin Board die Daten veröffentlicht, die eine Überprüfbarkeit des korrekten Wahlablaufs ermöglichen sollen. Dies umfasst alle Restricted-IDs aus dem Wählerverzeichnis zusammen mit Vor- und Nachname des zugehörigen Wählers sowie alle verschlüsselten Stimmen aus der Urne zusammen mit den zugehörigen (anonymen) Wahlstimmen-IDs einschließlich deren Signatur. In Abhängigkeit des zugrundeliegenden Wahlprotokolls erfolgt die Veröffentlichung der Stimmen verschlüsselt bzw. unverschlüsselt.

5 Bedrohungsanalyse

Nachfolgend werden mögliche Bedrohungen für das vorgestellte Konzept der Wählerauthentifizierung vorgestellt und analysiert. Hierbei werden zum einen Bedrohungen bezüglich der Geheimhaltung der Wahl betrachtet und zum anderen Bedrohungen, welche sich konkret in Hinblick auf die Wählerauthentifizierung ergeben.

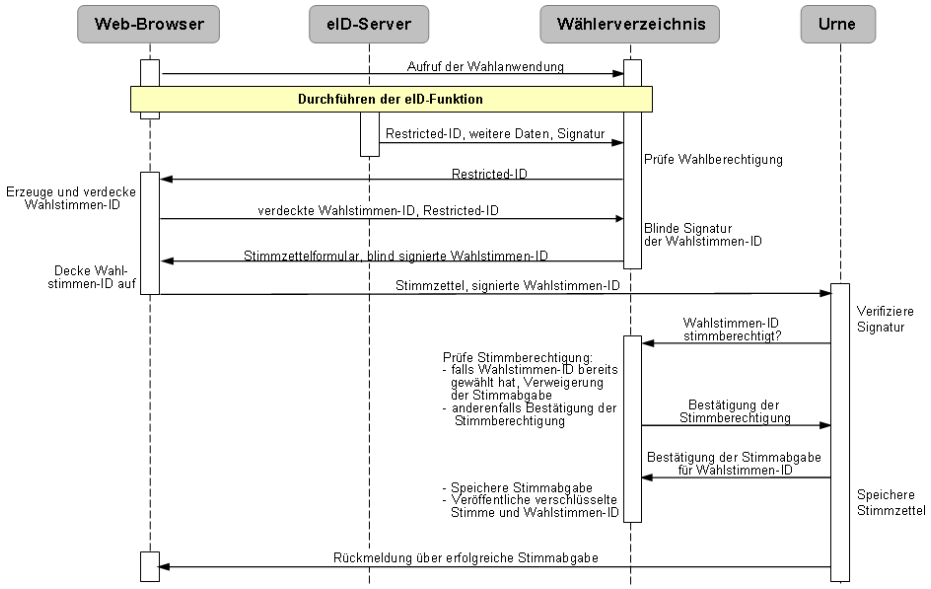

Abbildung 2: Sequenzdiagramm über den Ablauf der Wahlhandlung mit zwischengelagerter Anonymisierungsschicht

5.1 Bedrohungen in Hinblick auf die Wählerauthentifizierung

Wie in [BKG11] geschildert, erfüllt die Wählerauthentifizierung die Funktion, dass (a) nicht wahlberechtigten Personen eine Stimmabgabe verwehrt wird und dass (b) kein Wähler mehr als eine (wirksame) Stimme abgeben kann. Zusätzlich muss gelten, dass (c) keinem wahlberechtigten Bürger sein Stimmrecht unberechtigter Weise verwehrt wird und dass (d) (z.B. durch eine manipulierte Wahlanwendung) keine Stimmzettel gelöscht oder hinzugefügt werden können. Im Folgenden wird das modifizierte Konzept mit zwischengelagerter Anonymisierungsschicht bezüglich dieser Bedrohungen betrachtet. Die stark vereinfachende Annahme, dass der eID-Server vertrauenswürdig ist, wird hier im Gegensatz zu [BKG11] jedoch nicht vorausgesetzt.

(a) Stimmabgabe durch Nicht-Wahlberechtigte

Zur erfolgreichen Stimmabgabe muss sich ein Bürger mit seinem Personalausweis gegenüber dem Wählerverzeichnis authentisieren. Hierzu benötigt er neben dem Ausweis selbst noch die zugehörige eID-PIN. Ist die Authentifikation zwischen dem Personalausweis und dem eID-Server gemäß [Bun10a] erfolgt, kann eine Manipulation des Ausweises oder das Verwenden eines gefälschten Ausweises ausgeschlossen werden.[4]

Nach der Authentifikation des Bürgers wird für die Überprüfung der Wahlberechtigung die Restricted-ID verwendet und zur Erzeugung der anonymen Wahlstimmen-ID herangezogen. Nicht-Wahlberechtigten würde die Erzeugung

[4] Der Verbindungsaufbau zwischen dem Personalausweis und dem eID-Server enthält ein Protokoll, das speziell die Echtheit und Unversehrtheit des Personalausweises sicherstellt.

der Wahlstimmen-ID verwehrt werden. Das illegitime Erzeugen von Wahlstimmen-IDs ist allerdings nicht ohne Weiteres möglich. Da die Wahlstimmen-IDs vom Wählerverzeichnis (blind) signiert wurden, würde dies ein Fälschen der Signatur des Wählerverzeichnisses erfordern.

Eine Stimmabgabe durch Nicht-Wahlberechtigte ist so lange nicht möglich, wie das Wählerverzeichnis als vertrauenswürdig angenommen werden kann.

(b) Mehrfache Stimmabgabe durch den Wähler

Die Wählerauthentifizierung erfolgt anhand der Restricted-ID. Diese wird direkt auf dem Personalausweis berechnet und ist an eine Kombination aus einem Personalausweis und einem Dienstanbieter gebunden. Während einer Wahl kann ein Personalausweis somit auch nur eine Restricted-ID erzeugen. Ein Eingriff in die Berechnung der Restricted-ID mit dem Ziel, mehrere Restricted-IDs zu erzeugen, ist nicht möglich. Dies erfordert eine Manipulation des Personalausweises, welche aus den in (a) genannten Gründen ausgeschlossen werden kann. Die Erzeugung der Wahlstimmen-ID ist unmittelbar an die Restricted-ID gebunden. Nach dem in Abschnitt 4.2 beschriebenen Verfahren kann pro Restricted-ID genau eine Wahlstimmen-ID erzeugt werden. Demnach kann jeder Wähler genau eine Wahlstimmen-ID erzeugen und mit dieser genau eine Stimme abgeben. Das Erzeugen von Wahlstimmen-IDs durch berechtigte Wähler erfordert analog zu (a) das Fälschen der Signatur des Wählerverzeichnisses.

Verschafft sich ein Angreifer Zugang zu mehreren Personalausweisen, so kann er sich mit diesen am System anmelden. Folglich verfügt er über mehr als eine Restricted-ID und kann somit mehrfach eine Stimme abgeben. Hier sind zwei Szenarien denkbar. Zum einen könnte ein Angreifer sich physischen Zugriff auf mehrere Personalausweise zverschaffen. Um mit diesen jedoch tatsächlich wählen zu können, benötigt der Angreifer die eID-PIN des jeweiligen Personalausweises, welches die Praktikabilität des Angriffes stark einschränkt. Zum anderen könnte ein Angreifer den Verlust seines Personalausweises vortäuschen und einen neuen Personalausweis beantragen. Je nach Dauer der Stimmabgabephase und Bearbeitungszeitraum zum Ausstellen des neuen Personalausweises könnte er dann sowohl mit dem alten als auch mit dem neuen Personalausweis eine Stimme abgeben. Dies ist bei der Organisation der Wahl, insbesondere bei der Festlegung der Dauer der Stimmabgabephase, zu berücksichtigen. Ein derartiger Angriff kann demnach auf organisatorischem Wege verhindert werden.

Demnach ist eine mehrfache Stimmabgabe durch (berechtigte) Wähler so lange nicht möglich, wie das Wählerverzeichnis als vertrauenswürdig angenommen werden kann.

(c) Verweigerung des Stimmrechts

Wird einem wahlberechtigten Bürger sein Stimmrecht in unberechtigter Weise verwehrt, so kann dieser im Wahllokal sein Stimmrecht einfordern und dort seine Wahl tätigen.

(d) Hinzufügen oder Löschen von Stimmzetteln

Hierbei muss unterschieden werden, welches die korrumpierten Parteien sind, durch die ein Hinzufügen oder Löschen von Stimmzetteln erfolgt. Mögliche Parteien sind hierbei der eID-Server, das Wählerverzeichnis und die Wahlurne.

(d.i) Hinzufügen von Stimmzetteln durch den eID-Server
Der eID-Server könnte versuchen, wirksam Stimmen abzugeben und in der Urne zu speichern. Dazu müsste der eID-Server für jede Stimme eine Restricted-ID sowie Vor- und Nachnamen des zugehörigen Wählers erzeugen. Das Wählerverzeichnis prüft anhand der erhaltenen Daten die Wahlberechtigung. Es kann jedoch nicht erkennen, ob es sich um eine „echte“ oder um eine vom eID-Server erzeugte Restricted-ID handelt. Da jedoch zusätzlich zur Restricted-ID Vor- und Nachname des Wählers übermittelt werden, kann das Wählerverzeichnis anhand dieser Daten überprüfen, ob es sich um einen im Wählerverzeichnis registrierten Wähler handelt oder nicht.

Das Hinzufügen von Stimmzetteln durch den eID-Server ist demnach dann nicht möglich, wenn das Wählerverzeichnis vertrauenswürdig ist und dementsprechend nicht mit dem eID-Server kooperiert.

(d.ii) Hinzufügen von Stimmzetteln durch das Wählerverzeichnis
Möchte das Wählerverzeichnis weitere Stimmen einfügen, muss es hierzu fiktive Restricted-IDs erzeugen. Dies erfordert das Fälschen der Signatur vom eID-Server. Anderenfalls könnten die fiktiven Restricted-IDs durch den Bürger aufgedeckt werden, da diese nach Beendigung der Wahl auf dem Bulletin Board veröffentlicht werden. Ein derartiger Angriff ist genau dann erkennbar, wenn der eID-Server vertrauenswürdig ist – und zwar auch dann, wenn das Wählerverzeichnis selber korrumpiert ist.

Bricht der Wähler nach der Authentifizierung aber vor Erzeugung der Wahlstimmen-ID die Wahlhandlung ab, könnte das Wählerverzeichnis an seiner Stelle eine Wahlstimmen-ID erzeugen und diese zur Stimmabgabe nutzen. Die Urne besitzt keine Möglichkeit dies aufzudecken, da sie lediglich anhand der Signatur des Wählerverzeichnisses auf den Wahlstimmen-IDs die Stimmberechtigung überprüft. Dieser potenzielle Angriff kann durch zusätzliche organisatorische Maßnahmen verhindert werden. Zum Beispiel könnte das Bulletin Board nach Beendigung der Wahl jeden wahlberechtigten Bürger darüber informieren, ob für ihn eine Stimmabgabe vermerkt ist oder nicht. Somit wird gewährleistet, dass nicht diejenige Systemkomponente Informationen über den Status der Stimmabgabe verschickt, der diesbezüglich nicht vertraut wird. Zur weiteren Erhöhung der Sicherheit kann zusätzlich ein Medienbruch eingefügt werden. Das heißt, statt per E-Mail kann die Benachrichtigung per SMS oder per Post erfolgen.

(d.iii) Hinzufügen oder Löschen von Stimmzetteln durch die Urne
Die Urne hat als einzige Komponente die Möglichkeit, Stimmen zu löschen. Nach der Wahl werden auf dem Bulletin Board sowohl die Daten aus dem Wählerverzeichnis als auch aus der Urne veröffentlicht. Das Wählerverzeichnis enthält eine Liste aller Bürger, die eine Stimmte abgegeben haben, die Urne enthält die zugehörigen Stimmen. Durch einen Vergleich beider Datensätze kann daher unmittelbar erkannt werden, dass Stimmen aus der Urne gelöscht wurden.

Andererseits könnte die Urne versuchen, Stimmen einzufügen. Diese Manipulation würde jedoch unmittelbar nach Beendigung der Wahl auffallen, da dann im Abgleich mit dem Wählerverzeichnis zu viele Stimmen in der Urne wären. Darüber hinaus müsste die Urne hierfür die Signatur des Wählerverzeichnisses auf den Wahlstimmen-IDs der eingefügten Stimmen fälschen.

Weder das Löschen noch das Hinzufügen der Stimmen durch die Urne ist unbemerkt möglich, so lange das Wählerverzeichnis vertrauenswürdig ist.

(d.iv) Hinzufügen oder Löschen von Stimmzetteln durch Urne und Wählerverzeichnis

Wie in (d.iii) beschrieben, könnte die Urne Stimmen löschen. Bei einer Kooperation von Urne und Wählerverzeichnis könnte das Wählerverzeichnis dahingehend angeglichen werden, dass keine Differenz zwischen den Daten aus Urne und Wählerverzeichnis mehr besteht.

Weiterhin könnten Urne und Wählerverzeichnis versuchen, Stimmen einzufügen. Dieser Fall verhält sich analog zu dem in (d.ii) beschriebenen Angriffsszenario. Bricht der Wähler seine Stimmabgabe ab, so kann das Wählerverzeichnis eine Wahlstimmen-ID erzeugen und diese zur Stimmabgabe nutzen. Die zeitliche Beschränkung wie in (d.ii) beschrieben existiert durch die Kooperation von Urne und Wählerverzeichnis nicht mehr. In (d.ii) konnte das Wählerverzeichnis nur vor Erzeugung der Wahlstimmen-ID sicher sein, dass der Wähler noch keine Stimme abgegeben hat. In diesem Fall könnte die Urne das Wählerverzeichnis über die Anzahl der eingegangenen Stimmen informieren. Anhand dessen könnte das Wählerverzeichnis die Anzahl der abgebrochenen Wahlhandlungen ableiten und entsprechend Stimmen einfügen. Analog zu (d.ii) kann auch dieser Angriff durch Benachrichtigung aller Wahlberechtigten verhindert werden.

Die obige Erörterung der Bedrohungen verdeutlicht erneut die Notwendigkeit einer konsequenten Umsetzung des Konzeptes der „Separation-of-Duty“. Es zeigt sich, dass entweder das Wählerverzeichnis oder aber der eID-Server vertrauenswürdig sein muss. In Anlehnung an die herkömmliche Papierwahl bietet es sich an, Verwaltung und Betrieb des Wählerverzeichnisses von allen beteiligten politischen Parteien und zusätzlich von unabhängigen Organisationen wie zum Beispiel der Gesellschaft für Informatik (GI) oder dem Chaos Computer Club (CCC) durchführen zu lassen. Auf diese Weise könnte sichergestellt werden, dass das Wählerverzeichnis dem Einflussbereich des Wahlausrichters – in diesem Fall des Bundes bzw. des jeweiligen Bundeslandes – entzogen wird und so eine „echte“ Trennung der Belange erreicht wird.

5.2 Bedrohungen bezüglich der Geheimhaltung der Wahl

In diesem Abschnitt werden Bedrohungen bezüglich der Geheimhaltung der Wahl betrachtet, welche durch eine manipulative Kooperation zwischen eID-Server und den Zertifizierungsinstanzen des neuen Personalausweises ermöglicht werden und die in [BKG11] keine Berücksichtigung gefunden haben. Erfolgt eine Wahl geheim, so darf der Inhalt der Stimme für niemanden (außer dem Wähler selber) mit der bürgerlichen Identität des Wählers verknüpft werden können. Im Folgenden wird aufgezeigt, dass eben diese Bedrohungen durch die zwischengelagerte Anonymisierungsschicht abgewehrt werden.

(a) Manipulative Kooperation von eID-Server und Zertifizierungsinstanzen

In [BKG11] wird davon ausgegangen, dass aus der Restricted-ID die bürgerliche Identität des Personalausweisinhabers nicht abgeleitet werden kann. Wie in Abschnitt 3 geschildert, kann dies bei einer manipulativen Kooperation zwischen

eID-Server und Zertifizierungsinstanzen jedoch nicht vorausgesetzt werden. Da bei dem ursprünglichen Konzept die Stimmen mit den Restricted-IDs des jeweiligen Wählers verknüpft sind, wäre somit eine Zuordnung von Wähleridentität zu Klartextstimme zumindest für die oben genannten Parteien prinzipiell möglich.

In dem hier modifizierten Konzept zur Wählerauthentifizierung ermöglicht die durch den Personalausweis berechnete Restricted-ID eine sichere Authentifizierung berechtigter Wähler. Gleichzeitig wird die nicht-aufdeckbare Anonymität der Wahlstimmen gewährleistet. Dies erfolgt, indem die Restricted-ID in keiner Weise mit der Klartextstimme verknüpft wird. Während die Restricted-ID die Wählerauthentifizierung ermöglicht, garantiert die blinde Signatur der Wahlstimmen-ID die Unverknüpfbarkeit zwischen Wähler und Stimme.

Der Anonymitätsmechanismus wird durch die Erzeugung einer Zufallszahl vom Wahlclient durchgeführt und wirkt auch dann, wenn eID-Server, Wählerverzeichnis, Urne und nPA-Zertifizierungsinfrastruktur korrupt wären und miteinander kooperierten. Allerdings ist darauf hinzuweisen, dass der Wahlclient seinerseits nicht manipuliert sein darf. Hier sind Open-Source-Entwicklungen in der Hand der Bürger erforderlich, so wie etwa das Rosecat-Projekt [EKN+11, Jah11] dieses befördert.

(b) Manipulation durch Verwendung privilegierter Inspektionsterminals

Eine weitere Manipulationsmöglichkeit des in [BKG11] vorgestellten Konzepts besteht darin, dass sich eine korrumpierte Wahlanwendung sowohl als sogenanntes Inspektionsterminal als auch als autorisierte Wahlanwendung ausgibt. Ein Inspektionsterminal ist ein privilegiertes Terminal, das zur hoheitlichen Kontrolle zum Beispiel von Polizei- oder Grenzbeamten eingesetzt wird. Das Inspektionsterminal hat lesenden Zugriff auf die Biometrieanwendung des nPA und bei einem entsprechenden Berechtigungszertifikat auf die Daten der eID-Anwendung [Bun11]. Ein Inspektionsterminal arbeitet in der Regel offline und liest optisch die auf dem Ausweis aufgedruckte Machine Readable Zone (MRZ) aus. Diese wird an Stelle der eID-PIN zur Absicherung der Kommunikation mit dem Ausweis verwendet.

Eine manipulierte Wahlanwendung könnte (zeitlich) hintereinander als privilegiertes Inspektionsterminal und als Wahlanwendung agieren. In der Rolle des privilegierten Inspektionsterminals könnte es ohne Zustimmung des Bürgers dessen wahre Identität auslesen. In der Rolle der Wahlanwendung könnte es weiterhin die Restricted-ID des Wählers auslesen, um sie anschließend zunächst mit der wahren Identität und letztendlich mit der Klartextstimme zu verknüpfen.

Soll ein manipuliertes Inspektionsterminal auch online arbeiten können, muss es hierzu die MRZ des Ausweises kennen. Unter der Annahme, dass das Inspektionsterminal die MRZ auch ohne einen direkten Sichtkontakt mit dem Ausweis ermitteln kann, müssen generell zwei mögliche Angriffsszenarien unterschieden werden. Zum einen kann der Wähler seine Stimme vom heimischen Computer aus abgeben und zum anderen kann er dies im Wahllokal tun.

Bei der Stimmabgabe vom heimischen Computer aus kann sich der Wähler selbst den zur Stimmabgabe verwendeten Wahl- und eID-Client aussuchen. Da der eID-Client die Kommunikation zwischen dem Ausweis und einer anderen Komponente steuert, kann er prinzipiell alle ausgetauschten Nachrichten

mitlesen. Diese Nachrichten setzen sich aus einem Nachrichtenkopf und einem Nachrichtenrumpf zusammen. Der Nachrichtenkopf beinhaltet Steuerungsinformationen und wird unverschlüsselt übertragen, wohingegen der Nachrichtenrumpf verschlüsselt übertragen wird. Anhand der unverschlüsselten Informationen aus dem Nachrichtenkopf kann ein nicht manipulierter eID-Client erkennen, dass das angeschlossene Terminal als Inspektionsterminal agiert. Der eID-Client kann dieses sowohl anzeigen als auch verhindern, indem er die Verbindung abbricht. Deshalb sei hier erneut auf die Wichtigkeit unmanipulierter eID-Clients und Wahlclients hingewiesen. An der Umsetzung eines solchen Clients auf Open-Source-Basis arbeitet die Universität Koblenz im Rosecat-Projekt [EKN+11, Jah11] in Kooperation mit dem Fraunhofer SIT.

Bei der Stimmabgabe im Wahllokal besteht allerdings keine solche Kontrollmöglichkeit. Zur Abwehr dieses Angriffs kann aber die zwischengeschaltete Anonymisierungsschicht beitragen. Mit den blind signierten Wahlstimmen-IDs wäre die Zuordnung zwischen der Identität eines Wählers und seiner abgegebenen Stimme nicht mehr möglich. Die Stimme wäre zwar der Wahlstimmen-ID zuordenbar, allerdings könnte daraus nicht die Identität des Wählers abgeleitet werden.

(c) Erpressbarkeit des Wählers durch das Wählerverzeichnis

Das Wählerverzeichnis könnte versuchen, die Wähler zu einer vom Wählerverzeichnis gewünschten Stimmabgabe zu bestechen oder gar zu erpressen. Dazu müsste das Wählerverzeichnis die Wähler dazu bewegen, ihre Wahlstimmen-ID aufzudecken, indem diese ihre Blendfaktoren aufdecken, damit das erpressende (bestechende) Wählerverzeichnis den Erfolg seiner Erpressung (Bestechung) im Nachhinein überprüfen kann. Die Kenntnis des Blendfaktors würde es dem Wählerverzeichnis erlauben, zunächst die Wahlstimmen-ID zu berechnen und diese mit der Identität des Wählers zu verknüpfen. In Abhängigkeit von den nach der Wahl auf dem Bulletin Board veröffentlichten Daten wäre dann gegebenenfalls weiterhin eine Verknüpfung mit der (Klartext-)Stimme möglich.

Diese Wahlmanipulation ist aber deshalb als unwahrscheinlich zu bewerten, weil sie eine Kooperation zwischen Wählerverzeichnis und Wähler voraussetzt, die eine viel einfachere Manipulation der Wählerstimme durch das Wählerverzeichnis eröffnen würde. Würde nämlich das Wählerverzeichnis eine Wahlmanipulation in Kooperation mit (bestochenen oder erpressten) Wählern anstreben, so würde es am Einfachsten dem in Abschnitt 5.1 unter (d.ii) beschriebenen Prozedere folgen. Demnach würde das Wählerverzeichnis den Wähler zum Abbruch der Wahlhandlung zwingen und an seiner Stelle eine Wahlstimmen-ID erzeugen und diese gleich selbst zur Stimmabgabe nutzen. Unter der Voraussetzung, dass der Wähler mit dem Wählerverzeichnis kooperiert, ist diese Form der Wahlmanipulation für das Wählerverzeichnis mit weniger Aufwand verbunden und daher als wahrscheinlicher anzusehen. Weiterhin sei hier angemerkt, dass die beschriebene Manipulationsmöglichkeit sich analog zur Briefwahl verhält: Kooperiert der Wähler dort mit dem Wählerverzeichnis, indem er seine Briefwahlunterlagen beantragt und diese dem Wählerverzeichnis übergibt, so kann das Wählerverzeichnis diese Unterlagen ungehindert zur Stimmabgabe verwenden.

Das Wählerverzeichnis muss daher immer so organisiert sein, dass es vertrauenswürdig ist. Um Versuche von Stimmenkauf oder -erpressung zu unterbinden,

genügt eine Aufteilung seiner Aufgaben unter sich gegenseitig kontrollierenden voneinander unabhängigen Parteien, so wie es bei herkömmlichen Urnenwahlen üblich ist. In dem hier beschriebenen Lösungsvorschlag werden nach der Wahl alle in der Urne enthaltenen (verschlüsselten) Stimmen zusammen mit den zugehörigen Wahlstimmen-IDs auf dem Bulletin Board veröffentlicht. Um Stimmenkauf oder -erpressung zu verhindern, muss daher gewährleistet werden, dass nach der Entschlüsselung der Stimmen eine Zuordnung der Klartextstimme weder zu der verschlüsselten Stimme noch zu der Wahlstimmen-ID mehr möglich ist. Dies hat jedoch zum Nachteil, dass keine vollständige Verifizierbarkeit der Stimmen von Stimmabgabe bis Stimmauszählung gewährleistet wird. In dem beschriebenen Szenario (Onlinewahl ersetzt Briefwahl) mag dies hinreichend sein und übertrifft sogar die Verifikationsmöglichkeiten der Briefwahl. Sollte die Onlinewahl jedoch ausgeweitet werden, müssten weitere Sicherheitsmaßnahmen ergriffen werden.

6 Fazit

Im Rahmen dieser Arbeit wurde gezeigt, dass das in [BKG11] vorgestellte Konzept zur Wählerauthentifizierung mittels nPA um weitere Sicherheitsmechanismen zum Schutze des Wahlgeheimnisses erweitert werden muss und kann. Das ursprüngliche Konzept basiert auf der Wählerauthentifizierung mittels der Restricted-ID. Diese lässt sich jedoch bei einer manipulativen Kooperation von eID-Server und Zertifizierungsstellen zurückführen und somit der Wähleridentität zuordnen. Zum Schutze des Wahlgeheimnisses wurde das in [BKG11] vorgestellte Konzept um eine zwischengelagerte Anonymisierungsschicht nach Vorbild des eCash-Verfahrens [Cha81, Cha83, Cha85, CFN90, Cha92] erweitert. Die durchgeführte Bedrohungsanalyse zeigt, dass die für das ursprüngliche Konzept bestehenden Bedrohungen hinsichtlich des Wahlgeheimnisses abgewehrt werden können. Weiterhin unterstreicht die Bedrohungsanalyse die Wichtigkeit der Umsetzung grundlegender Prinzipien der IT-Sicherheit.

Zum einen muss derjenige eine Sicherheitsanforderung durchsetzen können, der auch ein Interesse an eben dieser hat. Im Kontext elektronischer Wahlen muss also der Wähler selber die notwendigen Mittel haben, um das Wahlgeheimnis durchsetzen zu können. In diesem Zusammenhang wird insbesondere die Bedeutung von Open-Source-Lösungen für den eID- und Wahlclient deutlich. Ein erster konkreter Schritt in diese Richtung wurde bereits im Rahmen des Rosecat-Projekts [EKN+11, Jah11] getätigt.

Zum anderen ist das Prinzip der „Separation-of-Duty“ für die beschriebene Anwendung von fundamentaler Bedeutung. Eine „wahre“ Trennung der Belange könnte zum Beispiel in Analogie zur herkömmlichen Papierwahl durch die öffentliche Kontrolle des Wählerverzeichnisses erreicht werden.

Es zeigt sich somit, dass Sicherheit nur im Zusammenspiel mit technischen und organisatorischen Maßnahmen erreicht werden kann.

A Zwei Wege zur Bildung der Restricted Identification des nPA

A.1 Zusammenfassung

Nach Aussage des Bundesamts für Sicherheit in der Informationstechnik (BSI) kann die Bildung des Dienste- und Kartenspezifische Kennwort (auch Restricted Identification, Restricted-ID oder einfach Pseudonym) ausschließlich auf dem Chip des nPA erfolgen. Die Technische Richtlinie BSI-TR-03110 [Bun10a] spezifiziert die Bildung des Pseudonyms sowie des Sperrmerkmals, wobei diese weitestgehend übereinstimmen. Bei der Erstellung der Sperrlisten wird deutlich, dass es theoretisch zwei Wege gibt, Pseudonyme zu bilden.

A.2 Schlüsselmaterial für Pseudonyme und Sperrmerkmale

Nach BSI-TR-3110 Kapitel 4.1.3 Key Agreement werden die folgenden Schlüssel und Protokolle verwendet:

- „The MRTD (Machine Readable Travel Document, hier der nPA) chip's static public key is PK_{ID}, the corresponding private key is SK_{ID}"
- „The sector's static public key is PK_{Sector}, the corresponding private key is SK_{Sector}"
- „The revocation sector public key is $PK_{Revocation}$, the corresponding private key is $SK_{Revocation}$"
- „The sector-specific identifier is I_{ID}^{Sector}"

A.3 Pseudonymfunktion des nPA

In BSI TR-03110 Kapitel 4.5 wird Berechnung der *Restricted Identification* des nPA beschrieben. Dieser kann nach der Durchführung der eID-Funktion ein Pseudonym ψ auf der Karte erzeugen und an den Diensteanbieter D übertragen.

Das Terminalzertifikat des Dienstanbieters enthält den eindeutigen *sector public key* PK_{Sector}, der Chip des nPA selbst enthält den geheimen, eindeutigen *unique chip identifier* SK_{ID}. Der nPA nimmt die Berechnung des Pseudonyms lokal vor:

$$\psi_D = I_{ID}^{Sector} = H(KA(SK_{ID}, PK_{Sector}, \delta))$$

Dabei ist H auf dem nPA die Hashfunktion *SHA-1*, *KA* ein Diffie-Hellman Key-Agreement-Protokoll auf Basis von elliptischen Kurven. D bezeichnet die öffentlichen Domain Parameter. Nach Ablauf der Protokolle *PACE*, *Terminal Authentication* und *Chip Authentication* ist der Zugriff auf das Datenfeld *SecurityInfos* des nPA möglich, in der die vom nPA unterstützten Protokolle und Schlüssellängen hinterlegt sind.

Der gegenseitige Identitätsnachweis durch die Terminal Authentication und Chip Authentication gelingt, da eine Public Key Infrastruktur geschaffen wurde, deren Vertrauenswurzel die Country Verifying Certificate Authority (CVCA, in Deutschland das BSI) ist. Die CVCA zertifiziert die Document Verifying Certificate Authorities (DVCA) und diese stellen die Terminal-Berechtigungszertifikate

aus. Der Aufbau dieser Public Key Infrastruktur wird u. a. in der technischen Richtline BSI TR-03127 [Bun11] in Kapitel 5.2 beschrieben, in Anhang B wird außerdem der Aufbau eines Terminal-Berechtigungszertifikats beschrieben.

Die Spezifikation in der BSI TR-03110 sieht vor, dass die DVCA die Domainparameter D definiert und gemeinsam mit PK_{Sector} veröffentlicht. Laut den Änhängen C.3.2 und D.3 wird der Hash dieser Daten als Certificate Extension im Terminal-Berechtigungszertifikat hinterlegt. Vor der Berechnung von ψ muss der nPA diese Daten zwingend verifizieren. Der eigentliche öffentliche Schlüssel wird bei der Restricted Identification dem nPA übergeben.

In Kapitel 4.5.1 wird in der Protokollspezifikation als Schritt 2 und 3 beschrieben:

- „2. The MRTD chip verifies PK_{Sector}, computes and sends its sector-specific identifier I_{ID}^{Sector} to the terminal."
- „3. The terminal checks whether the received sector-specific identifier I_{ID}^{Sector} is in the list of revoked sector identifiers received from the document verifier."

Die Sperrliste enthält jeweils die Sperrmerkmale von als voerloren oder gestohlen gemeldeten Ausweisen. Das Sperrmerkmal wird analog zum Pseudonym erzeugt, dieses Mal allerdings nicht auf dem nPA.

A.4 Erzeugung von Sperrlisten

Die Vorgänge zur Erzeugung von Sperrlisten werden detalliert in der der technischen Richtline BSI TR-03127 in Kapitel 5.3 beschrieben. Die abzuwickelnden Protokolle werden allerdings weiterhin in der technischen Richtlinie BSI TR-03110 spezifiziert:

Die CVCA ist in Besitz des Revocation-Schlüsselpaars sowie der domänenspezifischen Parameter D:

$$Revocation = (PK_{Revocation}, SK_{Revocation}), D$$

$PK_{Revocation}$ und D werden veröffentlicht.
Jeder Document Verifier erzeugt einen zufälligen Sector Private Key SK_{Sector} und errechnet den Sector Public Key:

$$PK_{Sector} = KA(SK_{Sector}, PK_{Revocation}, D)$$

In Kapitel 4.5.3 wird eine Sperranfrage anhand eines eingehenden Restricted Identifier Public Key PK_{ID} beschrieben:

1. Die CVCA errechnet den Sperrschlüssel: $PK_{ID}^{Revocation} = KA(SK_{Revocation}, PK_{ID}, D)$. Dieser Sperrschlüssel wird an alle Document Verifying Certificate Authorities (DVCA) weitergereicht.
2. Jede DVCA erzeugt daraus die Dienstanbieter-spezifischen Sperrschlüssel: $I_{ID}^{Sector} = H(KA(SK_{Sector}, PK_{ID}^{Revocation}, D))$

A.5 Schlussfolgerung

Aufgrund der Tatsache, dass das Schlüsselmaterial zur Erzeugung der Restricted-ID um Schlüsselpaare mit jeweils öffentlichem sowie privatem Anteil handelt, ist ein zweiter Weg zur Errechnung der Restricted Identification theoretisch möglich.

Eine Anfrage beim BSI ergab, dass die Schlüsselpaare nur für die Sperrlisten gehalten werden, der private Teil der Restricted Identification des nPA jedoch nicht Teil eines Schlüsselpaars sei, sondern lediglich eine zufällige Zahl. Eine Rückrechnung sei daher weder vorgesehen noch möglich.

Zukünftig ist dennoch denkbar, dass die Entscheidung getroffen werden könnte, Pseudonyme des nPA zuordenbar zu machen, ohne dass dabei die Spezifikation angepasst werden müsste.

Literatur

[Ben87] Benaloh, Josh Daniel C.: *Verifiable secret-ballot elections*, Yale University, Department of Computer Science, Dissertation, 1987

[BKG11] Bräunlich, Katharina ; Kasten, Andreas ; Grimm, Rüdiger: Der neue Personalausweis zur Authentifizierung bei elektronischen Wahlen. In: *Sicher in die digitale Welt von morgen*, 2011, S. 211–225

[Bun10a] Bundesamt für Sicherheit in der Informationstechnik: Advanced Security Mechanisms for Machine Readable Travel Documents (v 2.05) / Bundesamt für Sicherheit in der Informationstechnik. 2010 (TR-03110). – Technische Richtlinie

[Bun10b] Bundesamt für Sicherheit in der Informationstechnik: eID-Server (v 1.3) / Bundesamt für Sicherheit in der Informationstechnik. 2010 (TR-03130). – Technische Richtlinie

[Bun11] Bundesamt für Sicherheit in der Informationstechnik: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel (v 1.14) / Bundesamt für Sicherheit in der Informationstechnik. 2011 (TR-03127). – Technische Richtlinie

[CFN90] Chaum, David L. ; Fiat, Amos ; Naor, Moni: Untraceable electronic cash. In: *Advances in Cryptology: Proceedings of Crypto '88* Bd. 403 Springer, 1990, S. 319–327

[Cha81] Chaum, David L.: Untraceable electronic mail, return addresses, and digital pseudonyms. In: *Communications of the ACM* 24 (1981), Nr. 2, S. 84–90

[Cha83] Chaum, David L.: Blind signatures for untraceable payments. In: *Advances in Cryptology: Proceedings of Crypto '82* Bd. 82, Springer, 1983, S. 199–203

[Cha85] Chaum, David L.: Security without identification: Transaction systems to make big brother obsolete. In: *Communications of the ACM* 28 (1985), Nr. 10, S. 1030–1044

[Cha92] Chaum, David L.: Achieving electronic privacy. In: *Scientific American* 267 (1992), Nr. 2, S. 96–101

[EKN+11] Ecker, Sven ; Knauf, Malte ; Normann, Johannes ; Roht, Olga ; Schlünss, Florian ; Taflinski, Ansgar ; Wolf, Andreas ; Zitz, Jonas: Dokumentation des Projektpraktikums ePA3 / Universität Koblenz-Landau. 2011. – Forschungsbericht

[GN02] Grimm, Rüdiger ; Nützel, Jürgen: Geschäftsmodelle für virtuelle Waren. In: *Datenschutz und Datensicherheit (DuD)* 5 (2002), Nr. 2002, S. 261–266

[Gri01] Grimm, Rüdiger: Electronic Payment Systems and Protocols. In: *Advanced security technologies in networking* (2001), S. 213–225

[GZ96] Grimm, Rüdiger ; Zangeneh, K.: Cybermoney in the Internet: An overview over new payment systems in the Internet. In: *Proceedings of the IFIP TC6/TC11 international conference on Communications and multimedia security II* Chapman & Hall, Ltd., 1996, S. 183–195

[Jah11] Jahn, Nico: *rosecat – Architektur und Implementierung eines Open-Source-eID-Clients*, Universität Koblenz-Landau, Diplomarbeit, 2011

[Net01] Netzwelt, Spiegel O.: *Deutsche Bank 24 stellt „eCash“ ein.* Online verfügbar; letzter Aufruf am 06.07.2011. `http://www.spiegel.de/netzwelt/tech/a-136015.html`. Version: 05 2001

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz-landau.de/koblenz/fb4/publications/Reports/arbeitsberichte)

Katharina Bräunlich, Rüdiger Grimm, Andreas Kasten, Sven Vowé, Nico Jahn, Arbeitsberichte aus dem Fachbereich Informatik 11/2011

Daniel Eißing, Ansgar Scherp, Steffen Staab, Formal Integration of Individual Knowledge Work and Organizational Knowledge Work with the Core Ontology *strukt*, Arbeitsberichte aus dem Fachbereich Informatik 10/2011

Bernhard Reinert, Martin Schumann, Stefan Müller, Combined Non-Linear Pose Estimation from Points and Lines, Arbeitsberichte aus dem Fachbereich Informatik 9/2011

Tina Walber, Ansgar Scherp, Steffen Staab, Towards the Understanding of Image Semantics by Gaze-based Tag-to-Region Assignments, Arbeitsberichte aus dem Fachbereich Informatik 8/2011

Alexander Kleinen, Ansgar Scherp, Steffen Staab, Mobile Facets – Faceted Search and Exploration of Open Social Media Data on a Touchscreen Mobile Phone, Arbeitsberichte aus dem Fachbereich Informatik 7/2011

Anna Lantsberg, Klaus G. Troitzsch, Towards A Methodology of Developing Models of E-Service Quality Assessment in Healthcare, Arbeitsberichte aus dem Fachbereich Informatik 6/2011

Ansgar Scherp, Carsten Saathoff, Thomas Franz, Steffen Staab, Designing Core Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 5/2011

Oleg V. Kryuchin, Alexander A. Arzamastsev, Klaus G. Troitzsch, The prediction of currency exchange rates using artificial neural networks, Arbeitsberichte aus dem Fachbereich Informatik 4/2011

Klaus G. Troitzsch, Anna Lantsberg, Requirements for Health Care Related Websites in Russia: Results from an Analysis of American, British and German Examples, Arbeitsberichte aus dem Fachbereich Informatik 3/2011

Klaus G. Troitzsch, Oleg Kryuchin, Alexander Arzamastsev, A universal simulator based on artificial neural networks for computer clusters, Arbeitsberichte aus dem Fachbereich Informatik 2/2011

Klaus G. Troitzsch, Natalia Zenkova, Alexander Arzamastsev, Development of a technology of designing intelligent information systems for the estimation of social objects, Arbeitsberichte aus dem Fachbereich Informatik 1/2011

Kurt Lautenbach, A Petri Net Approach for Propagating Probabilities and Mass Functions, Arbeitsberichte aus dem Fachbereich Informatik 13/2010

Claudia Schon, Linkless Normal Form for ALC Concepts, Arbeitsberichte aus dem Fachbereich Informatik 12/2010

Alexander Hug, Informatik hautnah erleben, Arbeitsberichte aus dem Fachbereich Informatik 11/2010

Marc Santos, Harald F.O. von Kortzfleisch, Shared Annotation Model – Ein Datenmodell für kollaborative Annotationen, Arbeitsberichte aus dem Fachbereich Informatik 10/2010

Gerd Gröner, Steffen Staab, Categorization and Recognition of Ontology Refactoring Pattern, Arbeitsberichte aus dem Fachbereich Informatik 9/2010

Daniel Eißing, Ansgar Scherp, Carsten Saathoff, Integration of Existing Multimedia Metadata Formats and Metadata Standards in the M3O, Arbeitsberichte aus dem Fachbereich Informatik 8/2010

Stefan Scheglmann, Ansgar Scherp, Steffen Staab, Model-driven Generation of APIs for OWL-based Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 7/2010

Daniel Schmeiß, Ansgar Scherp, Steffen Staab, Integrated Mobile Visualization and Interaction of Events and POIs, Arbeitsberichte aus dem Fachbereich Informatik 6/2010

Rüdiger Grimm, Daniel Pähler, E-Mail-Forensik – IP-Adressen und ihre Zuordnung zu Internet-Teilnehmern und ihren Standorten, Arbeitsberichte aus dem Fachbereich Informatik 5/2010

Christoph Ringelstein, Steffen Staab, PAPEL: Syntax and Semantics for Provenance-Aware Policy Definition, Arbeitsberichte aus dem Fachbereich Informatik 4/2010

Nadine Lindermann, Sylvia Valcárcel, Harald F.O. von Kortzfleisch, Ein Stufenmodell für kollaborative offene Innovationsprozesse in Netzwerken kleiner und mittlerer Unternehmen mit Web 2.0, Arbeitsberichte aus dem Fachbereich Informatik 3/2010

Maria Wimmer, Dagmar Lück-Schneider, Uwe Brinkhoff, Erich Schweighofer, Siegfried Kaiser, Andreas Wieber, Fachtagung Verwaltungsinformatik FTVI Fachtagung Rechtsinformatik FTRI 2010, Arbeitsberichte aus dem Fachbereich Informatik 2/2010

Max Braun, Ansgar Scherp, Steffen Staab, Collaborative Creation of Semantic Points of Interest as Linked Data on the Mobile Phone, Arbeitsberichte aus dem Fachbereich Informatik 1/2010

Marc Santos, Einsatz von „Shared In-situ Problem Solving“ Annotationen in kollaborativen Lern- und Arbeitsszenarien, Arbeitsberichte aus dem Fachbereich Informatik 20/2009

Carsten Saathoff, Ansgar Scherp, Unlocking the Semantics of Multimedia Presentations in the Web with the Multimedia Metadata Ontology, Arbeitsberichte aus dem Fachbereich Informatik 19/2009

Christoph Kahle, Mario Schaarschmidt, Harald F.O. von Kortzfleisch, Open Innovation: Kundenintegration am Beispiel von IPTV, Arbeitsberichte aus dem Fachbereich Informatik 18/2009

Dietrich Paulus, Lutz Priese, Peter Decker, Frank Schmitt, Pose-Tracking Forschungsbericht, Arbeitsberichte aus dem Fachbereich Informatik 17/2009

Andreas Fuhr, Tassilo Horn, Andreas Winter, Model-Driven Software Migration Extending SOMA, Arbeitsberichte aus dem Fachbereich Informatik 16/2009

Eckhard Großmann, Sascha Strauß, Tassilo Horn, Volker Riediger, Abbildung von grUML nach XSD soamig, Arbeitsberichte aus dem Fachbereich Informatik 15/2009

Kerstin Falkowski, Jürgen Ebert, The STOR Component System Interim Report, Arbeitsberichte aus dem Fachbereicht Informatik 14/2009

Sebastian Magnus, Markus Maron, An Empirical Study to Evaluate the Location of Advertisement Panels by Using a Mobile Marketing Tool, Arbeitsberichte aus dem Fachbereich Informatik 13/2009

Sebastian Magnus, Markus Maron, Konzept einer Public Key Infrastruktur in iCity, Arbeitsberichte aus dem Fachbereich Informatik 12/2009

Sebastian Magnus, Markus Maron, A Public Key Infrastructure in Ambient Information and Transaction Systems, Arbeitsberichte aus dem Fachbereich Informatik 11/2009

Ammar Mohammed, Ulrich Furbach, Multi-agent systems: Modeling and Virification using Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 10/2009

Andreas Sprotte, Performance Measurement auf der Basis von Kennzahlen aus betrieblichen Anwendungssystemen: Entwurf eines kennzahlengestützten Informationssystems für einen Logistikdienstleister, Arbeitsberichte aus dem Fachbereich Informatik 9/2009

Gwendolin Garbe, Tobias Hausen, Process Commodities: Entwicklung eines Reifegradmodells als Basis für Outsourcingentscheidungen, Arbeitsberichte aus dem Fachbereich Informatik 8/2009

Petra Schubert et. al., Open-Source-Software für das Enterprise Resource Planning, Arbeitsberichte aus dem Fachbereich Informatik 7/2009

Ammar Mohammed, Frieder Stolzenburg, Using Constraint Logic Programming for Modeling and Verifying Hierarchical Hybrid Automata, Arbeitsberichte aus dem Fachbereich Informatik 6/2009

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm, Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung, Arbeitsberichte aus dem Fachbereich Informatik 5/2009

Hannes Schwarz, Jürgen Ebert, Andreas Winter, Graph-based Traceability – A Comprehensive Approach. Arbeitsberichte aus dem Fachbereich Informatik 4/2009

Anastasia Meletiadou, Simone Müller, Rüdiger Grimm, Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS), Arbeitsberichte aus dem Fachbereich Informatik 3/2009

Ansgar Scherp, Thomas Franz, Carsten Saathoff, Steffen Staab, A Model of Events based on a Foundational Ontology, Arbeitsberichte aus dem Fachbereich Informatik 2/2009

Frank Bohdanovicz, Harald Dickel, Christoph Steigner, Avoidance of Routing Loops, Arbeitsberichte aus dem Fachbereich Informatik 1/2009

Stefan Ameling, Stephan Wirth, Dietrich Paulus, Methods for Polyp Detection in Colonoscopy Videos: A Review, Arbeitsberichte aus dem Fachbereich Informatik 14/2008

Tassilo Horn, Jürgen Ebert, Ein Referenzschema für die Sprachen der IEC 61131-3, Arbeitsberichte aus dem Fachbereich Informatik 13/2008

Thomas Franz, Ansgar Scherp, Steffen Staab, Does a Semantic Web Facilitate Your Daily Tasks?, Arbeitsberichte aus dem Fachbereich Informatik 12/2008

Norbert Frick, Künftige Anfordeungen an ERP-Systeme: Deutsche Anbieter im Fokus, Arbeitsberichte aus dem Fachbereicht Informatik 11/2008

Jürgen Ebert, Rüdiger Grimm, Alexander Hug, Lehramtsbezogene Bachelor- und Masterstudiengänge im Fach Informatik an der Universität Koblenz-Landau, Campus Koblenz, Arbeitsberichte aus dem Fachbereich Informatik 10/2008

Mario Schaarschmidt, Harald von Kortzfleisch, Social Networking Platforms as Creativity Fostering Systems: Research Model and Exploratory Study, Arbeitsberichte aus dem Fachbereich Informatik 9/2008

Bernhard Schueler, Sergej Sizov, Steffen Staab, Querying for Meta Knowledge, Arbeitsberichte aus dem Fachbereich Informatik 8/2008

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:"E-KRHyper", Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen", Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe"
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005