TECHNISCHE
UNIVERSITÄT
DARMSTADT

Anbindung eines externen Authentifizierungsdienstes an ein Online-Wahlsystem

Christian Backs

Januar 2010

Diplomarbeit
Fachbereich Informatik
Fachgebiet Theoretische Informatik
Kryptographie und Computeralgebra
Prof. Dr. Johannes Buchmann
Betreuerin: Dr. Melanie Volkamer

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Diplomarbeit ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, Januar 2010

Christian Backs

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

1 Einleitung

1.1 Beschreibung

Im Laufe der Geschichte haben sich neue Wahlformen entwickelt. Während bei den ersten Wahlen alle Wähler am selben Ort sein mussten, ermöglichte später die Wahl mit Briefen eine Distanzwahl. Durch den technischen Fortschritt entwickelten sich zusätzlich elektronische Wahlformen. Die als Online-Wahl bekannte Wahlform nutz das Internet für die ortsunabhängige Stimmabgabe. Bei dieser Distanzwahl benötigt der Wähler oft nur einen Browser und einen Internet-Zugang.

Die freie Wahl des Ortes für den Wahlvorgang stellt besondere Herausforderungen an das Wahlsystem, da im Gegensatz zu einer Präsenzwahl die Identitätsprüfung des Wählers nicht persönlich beim Wahlvorgang erfolgen kann. Im Vergleich zu einer Briefwahl kann jedoch der Nachweis der Identität mit schwerer fälschbaren Merkmalen als einer eigenhändigen Unterschrift erfolgen.

Häufig werden hierfür wissensbasierte Authentifizierungsmerkmale wie Benutzernamen und Passwörter eingesetzt. Bei einer solchen Lösung ist allerdings die Sicherheit der Zugangsdaten einzig von deren Geheimhaltung abhängig, wodurch sich die sichere Verteilung der Passwörter als schwierig erweist. Wenn diese mit Hilfe von so genannten PIN-Briefen mit Rubbelfeld verteilt werden, dann besteht die Gefahr des Abfangens dieser Briefe. Falls ein Unberechtigter einen solchen Brief einsehen kann, dann erfährt er das für den Wahlvorgang nötige Geheimnis. Eine weitere Bedrohung für diese Art der Authentifizierung stellt ein Phishing-Angriff dar. Hierbei versucht der Angreifer den Wähler dazu zu bringen, seine Zugangsdaten auf einer gefälschten Seite einzugeben.

Eine Verteilung von besitzbasierten Authentifizierungsmerkmalen wie Smartcards verursacht noch höhere Wahlkosten als die der PIN-Briefe. Zusätzlich benötigt jeder Wahlberechtigte ein Kartenlesegerät. Besonders bei Wahlen mit sehr vielen Wahlberechtigten entstehen dadurch extreme Kosten.

Das Ziel dieser Arbeit ist, die Authentifizierung der Wahlberechtigten sicher zu gestalten, ohne dass kostenintensive PIN-Briefe, Smartcards oder ähnliches verteilt werden müssen. Die Authentifizierung beim Wahlvorgang wird externen Authentifizierungsdiensten, die vielen Wahlberechtigten schon aus anderer Nutzung bekannt

sind, übergeben, so dass eine für den Wahlberechtigten vertraute Prüfung erfolgt. Da die Authentifizierungsdienste von dem Wahlsystem selbst unabhängig sind und der Wahlberechtigte persönlich entscheiden kann, welchen er für den Wahlvorgang benutzen möchte, entsteht eine deutliche Trennung zwischen dem Vorgang der Identitätsprüfung und dem eigentlichen Wahlvorgang.

Darüber hinaus soll jeder Wahlberechtigte seine eigene Wahlteilnahme überprüfen können, ohne dass dies auch anderen Wahlberechtigten oder Dritten möglich ist. Somit entsteht ein Mechanismus zur Überprüfung der Wahl, ohne dass die Geheimhaltung der Wahlteilnehmer gefährdet wird.

1.2 Aufbau des Dokuments

In dieser Arbeit wird, nach einer kurzen Einführung in die Wahlthematik und die Möglichkeiten der Authentifizierung, eine Lösung für ein Online-Wahlsystem entwickelt, vorgestellt und untersucht. Danach wird dessen Realisierbarkeit mit Hilfe einer Referenzimplementierung nachgewiesen. Abschließend folgt ein Fazit und Ausblick. Dieses Dokument gliedert sich wie folgt:

Im nächsten Kapitel werden die existierenden Wahlformen unterschieden und die Anforderungen an Wahlen auch im Hinblick auf die Online-Varianten beschrieben.

Im dritten Kapitel werden die möglichen Merkmale für die Identitätsprüfung eines Wahlberechtigten beschrieben. Nach einer allgemeinen Schilderung von *Single-Sign-On-Diensten (SSO)* mit deren Vor- und Nachteilen werden die häufig eingesetzte *SSO*-Lösung Kerberos und der webbasierte Authentifizierungsdienst OpenID vorgestellt. Anschließend werden Kerberos und OpenID bezüglich ihrer Eignung zur Anbindung an Online-Wahlsysteme untersucht.

Das nächste Kapitel enthält eine Schilderung der für eine Online-Wahl nötigen Identifizierungs-, Authentifizierungs- und Autorisierungsverfahren unter Einbeziehung von OpenID und eine abstrakte Beschreibung einer Online-Wahl mit OpenID.

Danach werden im fünften Kapitel die Auswahlkriterien für die Zulassung von OpenID-Providern bei einer Online-Wahl erklärt und die Unterschiede bei der Registrierung und Nutzung von verschiedenen OpenID-Providern gezeigt. Hierbei werden die resultierenden Vor- und Nachteile bei der Zulassung für eine Online-Wahl von allen bis zu einem OpenID-Provider betrachtet.

Im Kapitel sechs folgt eine Sicherheitsbetrachtung von Online-Wahlsystemen und OpenID-Providern, bei der zwischen den server- und clientseitigen Komponenten unterschieden wird. Anschließend werden die Erkenntnisse für den Einsatz eines Online-Wahlsystems mit OpenID geschildert.

Im nachfolgenden Kapitel werden Gründe für weitere Authentifizierungsmerkmale bei der Registrierung und dem Wahlvorgang in speziellen Einsatzszenarien geschildert. Hierbei werden Merkmale, die diese Probleme lösen, vorgestellt und deren Verteilung und Verwendung beschrieben.

Im achten Kapitel wird der Verlauf einer Online-Wahl mit OpenID, beginnend bei den Voraussetzungen bis zur Auszählung und Dokumentation, beschrieben. Hierbei wird jede Phase einzeln dargestellt und alle vorgestellten Varianten werden berücksichtigt.

Die praktisch mögliche Umsetzung der bis dahin beschriebenen Überlegungen wird in einer als Proof-of-Concept erstellten Referenzimplementierung gezeigt. Das neunte Kapitel beschreibt diese Implementierung sowie den Ablauf der Registrierung einer Wählerkennung und des Wahlvorgangs Schritt für Schritt aus Sicht des Wahlberechtigten.

Am Ende des Dokuments folgt ein Fazit über alle beschriebenen Lösungen und ein Ausblick mit einer Beschreibung der Einsetzbarkeit des Wählerregistrierungs- und Online-Wahlsystems mit OpenID.

Aus Gründen der Lesbarkeit wurde explizit auf die weibliche Form, wie zum Beispiel „Wählerin“, verzichtet. Mit männlichen Formen sind in diesem Dokument deshalb immer gleichermaßen die männliche und weibliche Person gemeint.

2 Wahlen

Es gibt eine Vielzahl von Wahlen. Neben den Wahlen erster Ordnung wie Bundestags-, Landtags- und Kommunalwahlen, gibt es auch viele Wahlen zweiter Ordnung wie Personal-, Betriebsrats-, Sozial-, Studentenvertretungs- und Vereinswahlen. Somit gibt es für Bürger in demokratischen Ländern öfters die Gelegenheit, an einer Wahl teilzunehmen.

Die einzelnen Wahlen können bezüglich ihrer Wahlform unterschieden werden. Folgend werden sie einzeln beschrieben und die Verwendung des Begriffs „Online-Wahlen“ in diesem Dokument wird erklärt. Alle Wahlen müssen entsprechend ihrer Wahlverordnung sicher und ordnungsgemäß durchgeführt werden, wobei das Umfeld großen Einfluss auf die jeweilige Durchführungsart einer Wahl ausübt. Am Ende dieses Kapitels werden die Anforderungen an Wahlen und Online-Wahlsysteme geschildert.

2.1 Unterscheidung von Wahlformen

Neben den zwei wesentlichen Grundformen der *Distanz-* und *Präsenzwahl*, die sich durch den Ort der Stimmabgabe bzw. die Anwesenheit von Wahlhelfern unterscheiden, bildet das Medium der Stimmabgabe ein dazu orthogonales Unterscheidungskriterium. Dabei spricht man von *papierbasierter-* bzw. *elektronischer Wahl*. Durch die Unterscheidungsmerkmale ‚Ort‘ und ‚Medium‘ der Stimmabgabe lassen sich folgende vier Grundformen und zwei Mischformen unterscheiden. [VK06]

2.1.1 Papierbasierte Wahl

Urnenwahl Bei der Urnenwahl geht der Wähler am Wahltag in das ihm zugeteilte Wahllokal, um seine Stimme auf einem normierten oder eigens für die Wahl produzierten Papierstimmzettel abzugeben. Es handelt sich dabei um eine *Papier-Präsenzwahl*.

Briefwahl Hier füllt der Wähler seinen Stimmzettel an einem von ihm gewählten Ort aus und versendet ihn über den Postweg an die Wahlzentrale. Da hierbei Papier als Medium verwendet wird, handelt es sich um eine *Papier-Distanzwahl*.

2.1.2 Elektronische Wahl

Wahlgeräte Der Wähler geht wie bei der Urnenwahl am Wahltag in das ihm zugeteilte Wahllokal, um seine Stimme mit Hilfe eines elektronischen Geräts abzugeben. Die dort eingesetzten Apparate lassen sich unterteilen in *Stand-alone-Wahlgeräte*, die die abgegebenen Stimmen lokal speichern und am Ende der Wahl auszählen, und in *vernetzte Wahlgeräte*, die entweder die Wahlberechtigungsprüfung, Stimmabgabe oder beides online abwickeln. Ein Hersteller für *Stand-alone-Wahlgeräte* ist das niederländische Unternehmen Nedap [Ned], deren umstrittene Wahlsysteme für politische Wahlen unter anderem in den Niederlanden und Deutschland eingesetzt wurden. Beim Einsatz von Wahlgeräten der zweiten Kategorie entsteht eine Online-Wahl im Wahllokal. Bei allen Varianten erfolgt der Wahlvorgang mit elektronischer Unterstützung an einem vorgegebenen Ort, daher werden diese Wahlformen auch als *elektronische Präsenzwahl* bezeichnet.

Remote-Online-Wahl Eine Remote-Online-Wahl erfolgt von einem nicht festgelegten Ort. Die Wahlberechtigungsprüfung sowie die Stimmabgabe erfolgen durch einen Online-Kanal von einem beliebigen elektronischen Endgerät. Überwiegend werden hierbei PCs als Endgeräte und das Internet als Kanal verwendet. Daher wird diese Wahlform auch als Internetwahl, Remote-E-Voting und Mobil-Voting bezeichnet und repräsentiert eine *elektronische Distanz-Wahl*. In Deutschland wurde die erste rechtsverbindliche Remote-Online-Wahl mit dem Wahlsystem Polyas [Pol] des Unternehmens Micromata GmbH durchgeführt.

2.1.3 Mischformen

Auszählungsautomat Mit Hilfe von Auszählungsautomaten werden die Papierstimmzettel elektronisch eingelesen, ausgewertet und das Ergebnis berechnet. Beispiele hierfür sind die kalifornischen Wahlgeräte von AccuVote [Pre] und der Wahlstift von dotVote [dot], der in Hamburg eingesetzt werden sollte. Da hierbei Papier und elektronische Geräte verwendet werden, handelt es sich um eine Mischform.

Online-Wahl am Kiosk Die hierbei eingesetzten *vernetzten Wahlgeräte* werden nicht in Wahllokalen unter Aufsicht der Wahlhelfer sondern in öffentlich zugänglichen Gebäuden und Räumen wie Bibliotheken, Schulen und Einkaufszentren aufgestellt. Daher müssen sie ähnlich den Geldausgabeautomaten besonders gegen Vandalismus, Manipulation und Ausspähung der Stimmabgabe geschützt sein. Aufgrund des Standortes der Wahlgeräte ist es eine Mischform aus elektronischer Präsenz- und Distanzwahl.

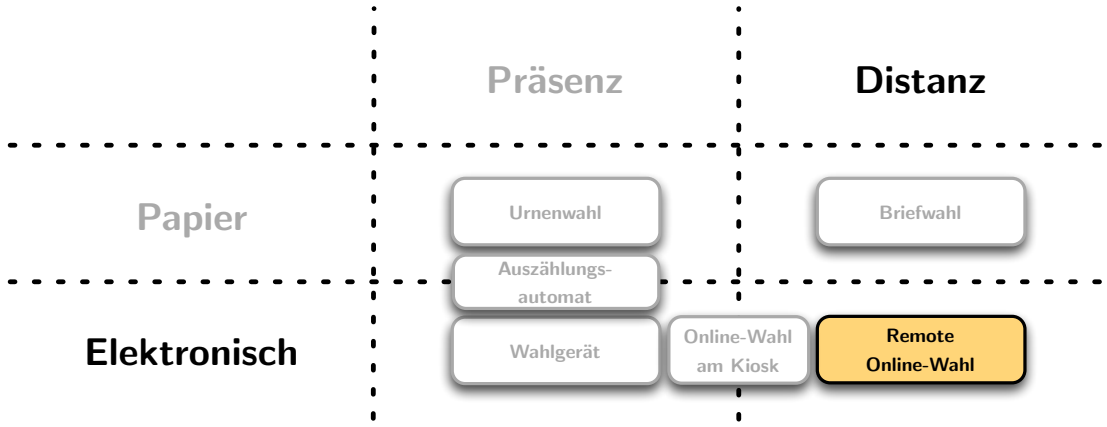

Abbildung 2.1: Die unterschiedlichen Wahlformen

Eine graphische Einordnung der einzelnen Wahlformen ist in Abbildung 2.1 zusammengefasst.

Die Aufstellung zeigt, dass mit dem Begriff „Online-Wahl“ die verschiedenen Wahlformen *Online-Wahl im Wahllokal*, *Online-Wahl am Kiosk* und *Remote-Online-Wahl* gemeint sein können. Diese drei Wahlformen nutzen eine direkte Verbindung zwischen dem Endgerät beim Wähler und einem zentralen Server zur Übermittlung der Wahlberechtigung oder Stimmabgabe, jedoch mit vollkommen unterschiedlichen Problemstellungen. In diesem Dokument wird der Begriff „Online-Wahl“ im Zusammenhang mit der *Remote-Online-Wahl* verwendet, da dies die technisch herausforderndste Wahlform ist.

2.2 Anforderungen an Wahlen

Grundsätzlich sollten Anforderungen an eine Wahl so gestellt sein, dass die Interessen der Wähler möglichst genau abgebildet werden und diese Abbildung nicht manipuliert werden kann. Es existieren generelle Anforderungen an Wahlen, die für jedes Wahlsystem gelten sollten, und weitergehend spezielle Anforderungen an Online-Wahlsysteme. In den folgenden Abschnitten werden beide Kategorien beschrieben.

2.2.1 Generelle Anforderungen an Wahlen

Die generellen Anforderungen an Wahlen ergeben sich aus Artikel 38 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland [GG]: *„Die Abgeordneten*

des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.“ In vielen Wahlordnungen westlicher Gesellschaften befinden sich ähnliche Formulierungen, da eine verbindliche und rechtgültige Wahl grundsätzlich diese Anforderungen erfüllen muss.

Die Anforderungen im Überblick:

Allgemein: Alle prinzipiell wahlberechtigten Personen (und nur diese) haben die Möglichkeit zur Wahl.

Unmittelbar: Eine verbindlich abgegebene Stimme kann nicht mehr verändert oder vernichtet werden. Es dürfen keine Stimmen von nicht berechtigten Personen oder mehr als die pro Wähler vorgesehenen Stimmen pro Person abgegeben werden. Mittelsmänner sind nicht zulässig.

Frei: Jeder Wähler gibt seine Stimme unabhängig von öffentlichen oder sozialen Zwängen ab.

Gleich: Jeder Wähler hat die gleiche Anzahl von Stimmen. Die Zugangsvoraussetzungen sind einheitlich, die Wahlumstände sind gleich.

Geheim: Es ist nicht zu ermitteln, welche Stimme ein Wähler abgegeben hat. Dies gilt selbst dann, wenn der Wähler dies explizit möchte (Gefahr der Bestechung oder Erpressung).

2.2.2 Spezielle Anforderungen an Online-Wahlsysteme

Neben den generellen Anforderungen an Wahlen ergeben sich für Online-Wahlsysteme noch weitere spezielle Anforderungen [Men08].

Diese sind im Einzelnen:

Einfach: Das Wahlsystem darf dem Wähler keine außergewöhnlichen Kenntnisse abverlangen.

Flexibel: Das System sollte im Idealfall für verschiedene Wahlszenarien konfigurierbar sein. Sicherheitsmaßgaben müssen unter unterschiedlichen Konfigurationsvarianten gültig sein.

Zuverlässig: Das System muss robust und hochverfügbar arbeiten. Abgegebene Stimmen dürfen an keiner Stelle verloren gehen.

Integer: Wählerstimmen dürfen nicht veränderbar, fälschbar oder löschbar sein. Sollten technische Fehler am System auftreten, dürfen diese die Integrität nicht beeinträchtigen.

Skalierbar: Das Verhalten und die Bedienung des Wahlsystems muss unabhängig vom Umfang der Wahl sein.

Exakt: Stimmen dürfen nicht falsch gezählt werden oder durch andere Umstände vom Wählerwillen abweichen. Das Wahlergebnis soll eine möglichst genaue Abbildung des Wählerwillens darstellen.

In dieser Arbeit wird ein *Remote-Online-Wahlsystem* beschrieben und erweitert. Dabei werden die *generellen Anforderungen an Wahlen* und die *speziellen Anforderungen an Online-Wahlsysteme* stets berücksichtigt.

3 Wählerauthentifizierung

An einer Online-Wahl dürfen nur berechtigte Personen teilnehmen, daher muss sich jeder Wähler authentifizieren. Durch die Authentifizierung [Sch06] wird verhindert, dass unberechtigte Personen sich als berechtigte ausgeben können. Jeder Wähler erhält dafür Authentifizierungsmerkmale aus den in Abschnitt 3.1 beschrieben Kategorien, mit denen er sich gegenüber dem Authentifizierungsdienst ausweisen kann.

Es gibt spezielle Dienste, die die Authentifizierung von Benutzern für andere angeschlossene Anwendungen und Systeme übernehmen. Dadurch ist es einem Benutzer möglich, sich an einem System anzumelden und anschließend alle angeschlossenen Anwendungen und Systeme verwenden zu können. Nach einer allgemeinen Beschreibung solcher *Single-Sign-On* genannten Lösungen mit deren Vor- und Nachteilen in Abschnitt 3.2 werden zwei Lösungen genauer vorgestellt und abschließend deren Eignung für die Anbindung an ein Online-Wahlsystem untersucht. Das Kapitel endet mit einer Entscheidung für einen externen Authentifizierungsdienst, der für die Anbindung an ein Online-Wahlsystem geeignet ist.

3.1 Authentifizierung

Aus den im vorherigen Kapitel beschriebenen Anforderungen folgt unter anderem, dass bei einer Wahl die Identität und die Wahlberechtigung jedes Wählers geprüft werden muss. Um die so genannte Basisanforderung *Wählerauthentifizierung* erfüllen zu können bedarf es einer technischen Lösung. Bevor eine detaillierte Lösung vorgestellt wird, werden folgend kurz die verwendeten Grundlagen beschrieben.

Die Authentifizierungsmerkmale (auch Credentials genannt) lassen sich nach [Sch06], [Eck05] in folgende Kategorien unterteilen:

Wissen: Diese Authentifizierungsart ist in der Praxis am häufigsten anzutreffen. [Eck05] Dabei dient allein ein Geheimnis zur Authentifizierung des Nutzers. Da ein Geheimnis leicht weitergegeben werden kann, muss der Integrität des Nutzers voll vertraut werden. Wissensbasierte Verfahren benutzen beispielsweise Login/Passwort oder PIN/TAN.

Besitz: Hierbei erfolgt die Authentifizierung durch den materiellen Besitz eines Merkmals. Der Nutzer wird nicht weiter geprüft. Typische Besitzmerkmale sind Schlüssel in physikalischer oder digitaler Form und Zugangskarten. Es können aber auch persönliche Telefonnummern verwendet werden.

Da diese personenbezogenen Merkmale durch eine gewollte oder unfreiwillige Weitergabe an eine unberechtigte Person auch dieser eine erfolgreiche Authentifizierung ermöglichen, kann dieses Verfahren nur bei vollem Vertrauen auf die Integrität des Nutzers verwendet werden. Wenn dieses Vertrauen nicht ausreichend sichergestellt werden kann, sollte dieses Verfahren mit weiteren Authentifizierungsverfahren kombiniert werden.

Biometrische Merkmale: Für die Authentifizierung werden von der Natur erzeugte eindeutige Merkmale des Nutzers verwendet. Im Gegensatz zu Merkmalen, die bei der Authentifizierung durch Besitz eingesetzt werden, können biometrische Merkmale nicht weitergegeben werden. Beispielhaft für solche Verfahren sind Fingerabdruckvergleich, Stimmerkennung, Iris- oder Handflächenvenen-Scan.

Auch diese Methode kann mit weiteren Authentifizierungsverfahren kombiniert werden, um Schwachstellen zu beheben.

Die Verwendung von zwei oder mehreren Merkmalen aus unterschiedlichen Kategorien wird als **Zwei-Faktor-Authentifizierung** [Eck05] oder **Multi-Faktor-Authentifizierung** bezeichnet. Häufig werden wissensbasierte Merkmale mit besitzbasierten kombiniert.

Die Zugangsprüfung bei Online-Wahlsystemen erfolgt in vielen Fällen mit Hilfe von wissensbasierten Merkmalen. Dabei werden Benutzernamen und Passwörter oder PINs und TANs verwendet, da sie sich normalerweise leichter verteilen lassen als besitzbasierte Merkmale.

Die Authentifizierung des Wählers muss vor der verbindlichen Abgabe der Stimme erfolgen und kann daher vor oder nach dem Erhalt des Stimmzettels durchgeführt werden. Wenn die Prüfung vorgelagert wird, dann kann sie entweder vom Wahlsystem selbst oder einem externen Authentifizierungsdienst vollzogen werden. Authentifizierungsdienste werden häufig für *Single-Sign-On*-Lösungen verwendet.

3.2 Single-Sign-On

Mit dem Begriff *Single-Sign-On (SSO)* wird die zentrale einmalige Anmeldung für die Nutzung von mehreren zugangsbeschränkten Anwendungen und Systemen bezeichnet. Ein Benutzer muss sich nur an einem System authentifizieren und kann danach alle angeschlossenen Systeme nutzen ohne dort weitere Zugangsdaten eingeben zu müssen.

Somit braucht ein Benutzer nur Authentifizierungsmerkmale mit einem System zu vereinbaren. Dies bietet mehr Komfort und erleichtert die Benutzerverwaltung.

In einer Umgebung, in der den Benutzern verschiedene Systeme und Dienste zur Verfügung stehen, die alle eine Authentifizierung erfordern, kommen oft *SSO*-Lösungen zum Einsatz. Diese können als Portal-, Ticket- oder lokale Lösungen eingesetzt werden.

Ein Web-Portal ist ein Beispiel für eine solche Portal-Lösung. Dabei meldet sich der Benutzer einmal am Portal an und kann, nachdem er korrekt authentifiziert wurde, alle an das Portal angegliederten Dienste nutzen.

Eine Ticket-Lösung kann beispielsweise mit dem im Abschnitt 3.3 beschriebenen Protokoll Kerberos erstellt werden. Dabei erhält der Benutzer eine Art Eintrittspass für die weiteren Systeme.

Ein Beispiel für eine lokale Lösung ist die Anmeldung an einem Arbeitsplatzrechner. Nachdem sich der Benutzer dort authentifiziert hat, kann er die von dort erreichbaren zugangsgeschützten Programme benutzen, ohne sich bei diesen erneut anmelden zu müssen.

3.2.1 Vor- und Nachteile

Wie bei jeder Lösung ergeben sich auch durch den Einsatz von *Single-Sign-On* Vor- und Nachteile. Die folgende Gliederung beschreibt diese für allgemeine *SSO*-Systeme.

Vorteile

Für den Benutzer entsteht eine Zeitersparnis, da nur eine einzige Authentifizierung für die Nutzung aller angeschlossenen Dienste und Systeme notwendig ist. Er muss sich nicht mehr an jedem Dienst oder System einzeln authentifizieren, braucht daher auch nicht mehrere Authentifizierungsmerkmale.

Folglich entsteht daher ein Gewinn an Sicherheit für den Anwender, da er seine Credentials nicht an mehrere Stellen übertragen muss. Auch *Phishing*-Attacken werden erschwert, da die Zugangsdaten nur an einer einzigen Stelle eingegeben werden und nicht an zahlreichen, verstreuten Stellen. Diese eine Authentifizierungsstelle kann leichter auf Korrektheit (mittels URL, SSL-Serverzertifikaten etc.) überprüft werden.

Studien haben gezeigt, dass viele Anwender für unterschiedliche Systeme und Dienste die gleichen Authentifizierungsmerkmale nutzen. Daher ist es nach einem erfolgreichen Angriff, bei dem die Zugangsdaten bekannt werden, nicht unwahrscheinlich, dass diese Zugangsdaten auch für andere vom Anwender genutzten Systeme und Dienste funktionieren. In einem solchen Szenario reicht ein gezielter Angriff auf das schwächste System oder den unsichersten Dienst aus, um Zugang zu allen anderen zu erlangen. Es ist leichter dem Anwender sichere Authentifizierungsmerkmale für nur eine Anmeldung anstatt für viele zu geben. Dies führt so zu einem Sicherheitsgewinn bei den Authentifizierungsmerkmalen.

Weiterhin ist es auch für die Benutzerverwaltung ein großer Vorteil, wenn die Benutzer an nur einer zentralen Stelle gepflegt werden. Da Änderungen an den Benutzerdaten nicht an mehreren Stellen vorgenommen werden, sinkt auch die Fehlerwahrscheinlichkeit. Auch die Kosten für die Benutzerverwaltung und Authentifizierung können durch *Single-Sign-On* gesenkt werden, wobei gleichzeitig die Sicherheit erhöht werden kann.

Nachteile

Durch die Authentifizierung an nur einer Stelle ergeben sich auch Gefahren. Der Authentifizierungsdienst muss sehr sicher arbeiten, denn falls er kompromittiert wird, ist die Sicherheit aller angeschlossenen Systeme und Dienste gefährdet.

Weiterhin entsteht durch *Single-Sign-On* auch ein *Single-Point-of-Failure*. Das bedeutet eine Störung aller angeschlossenen Dienste und Systeme bei einem Ausfall des Authentifizierungsdienstes. Somit ist die Verfügbarkeit eines angeschlossenen Systems oder Dienstes nicht nur von der eigenen, sondern auch von der Verfügbarkeit des *Single-Sign-On*-Systems abhängig.

Die Authentifizierungsmerkmale sollten auch sehr sicher gewählt werden, denn falls ein Angreifer die Authentifizierungsmerkmale eines Anwenders erfahren und missbrauchen kann, erhält er nicht nur Zugriff auf eines sondern auf alle angeschlossenen Systeme und Dienste.

3.3 Kerberos

Bei Kerberos handelt es sich um eine ticketbasierende *Single-Sign-On*-Lösung. Das Protokoll trägt den Namen des mehrköpfigen Höllenhundes aus der griechischen Mythologie, der den Eingang zur Unterwelt bewacht. Entwickelt wurde der verteilte Authentifizierungsdienst im Rahmen des Projekt Athena am MIT [Ath] und erst die Version 4 wurde Ende der 1980er Jahre außerhalb des MIT verwendet. Heutzutage

wird Kerberos in der aktuellen Version 5 sowie in seiner Vorgängerversion für eine sichere und einheitliche Authentifizierung in einem ungesicherten TCP/IP-Netzwerk mit sicheren Hostrechnern eingesetzt.

3.3.1 Beschreibung

Ein Kerberos-System besteht aus einem *Authentication Server* (AS) mit einer Schlüsseldatenbank und einem *Ticket Granting Server* (TGS) für die Ticketausstellung. Die Komponenten eines solchen Systems sind in Abbildung 3.1 dargestellt. Für die Verwendung einer Anwendung oder eines Systems des Servers benötigt der Benutzer einen *Authentikator*. Um diesen zu erhalten wird vom Client des Benutzers zuerst ein Schlüssel beim *Authentication Server* angefordert und danach ein Ticket vom *Ticket Granting Server*. Dieser Ablauf ist in Abbildung 3.2 dargestellt und die zugehörigen Protokollschritte sind in Tabelle 3.1 aufgelistet.

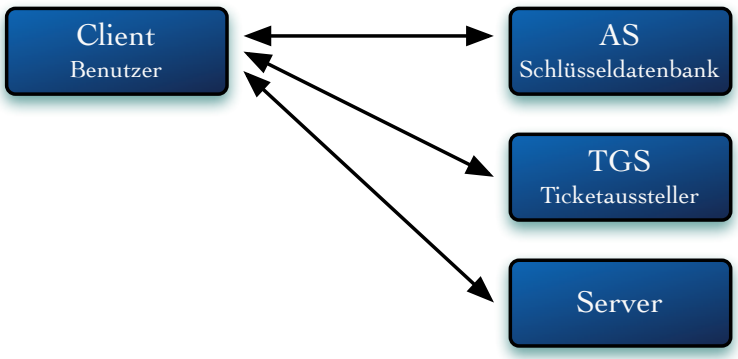

Abbildung 3.1: Komponenten von Kerberos

Folgende Informationen müssen vorher bekannt sein:

- Client/User und AS kennen K_{User}
- TGS und AS kennen K_{TGS}
- Server und AS kennen K_{Server}

Folgende Informationen werden während des Protokollablaufs bekannt:

- Zufallszahlen gegen Replay-Attacks: Nonce1, Nonce2
- Sitzungsschlüssel: $K_{User,TGS}$, $K_{User,Server}$
- Tickets: $T_{User,TGS}$, $T_{User,Server}$
- Authentikator: A_{User}

Die Uhrzeiten aller teilnehmen Systeme müssen synchronisiert sein, da die Tickets eine Zeitinformation enthalten. Hierzu wird üblicherweise das *Network Time Protocol* (NTP) eingesetzt.

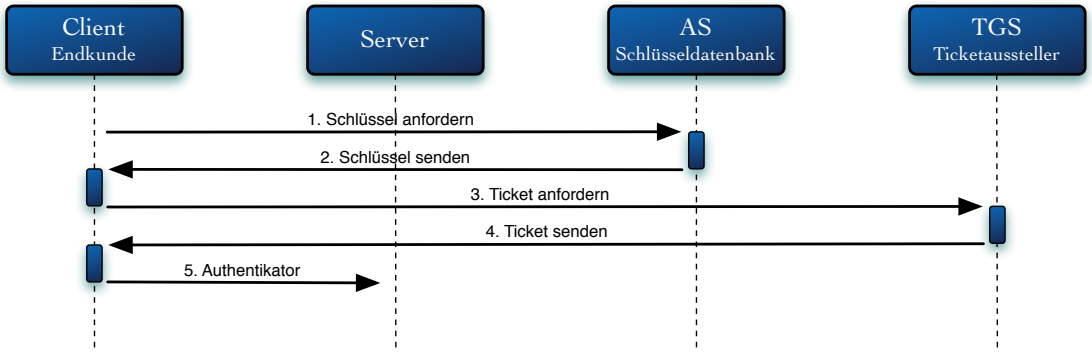

Abbildung 3.2: Anmeldung mit Kerberos

Schritt	Von	An	Nachricht
1.	Client	AS	User, TGS, Nonce1
2.	AS	Client	$\{K_{User,TGS}, Nonce1\}^{K_{User}}$, $\{T_{User,TGS}\}^{K_{TGS}}$
3.	Client	TGS	$\{A_{User}\}^{K_{User,TGS}}$, $\{T_{User,TGS}\}^{K_{TGS}}$, Server, Nonce2
4.	TGS	Client	$\{K_{User,Server}, Nonce2\}^{K_{User,TGS}}$, $\{T_{User,Server}\}^{K_{Server}}$
5.	Client	Server	$\{A_{User}\}^{K_{User,Server}}$, $\{T_{User,Server}\}^{K_{Server}}$

Tabelle 3.1: Kerberos Protokollschritte

Ticket: $T_{User,Server}$ = Server, User, addr, timestamp, lifetime, $K_{User,Server}$

Authentikator: A_{User} = User, addr, timestamp

3.3.2 Verwendung

Kerberos wird vorwiegend in großen Unternehmen mit vielen Clients eingesetzt. Die zentrale Benutzerverwaltung erleichtert besonders bei einer Vielzahl an Benutzern die

Administration. Durch die Ticketbasierung können neue Systeme und Anwendung mit geringem Aufwand in ein bestehendes Kerberos-System eingegliedert werden. Da die Kommunikation zwischen den Komponenten verschlüsselt erfolgt, können auch unsichere Netze verwendet werden.

3.4 OpenID

Viele Webseiten und webbasierte Anwendungen erfordern eine Benutzerauthentifizierung. Bei solchen Diensten muss sich ein Benutzer vor der ersten Verwendung registrieren. Hierbei wählt er üblicherweise einen freien Benutzernamen und vereinbart ein Geheimnis für die Authentifizierung wie beispielsweise ein Passwort. Nach Abschluss der erfolgreichen Registrierung kann er sich bei dem Dienst anmelden und die zugangsgeschützten Funktionen nutzen.

Wenn ein Nutzer viele voneinander unabhängige Dienste verwenden möchte, dann benötigt er für jeden eigene Zugangsdaten. Bei der Registrierung kann er denselben Benutzernamen nur wählen, falls dieser nicht schon von einem anderen Benutzer verwendet wird. Folglich gehört ein Benutzername bei verschiedenen Diensten nicht immer derselben Person und der Benutzer muss sich für jeden Dienst seinen dortigen Benutzernamen merken. Häufig werden für die Authentifizierung wissensbasierte Merkmale wie Passwörter eingesetzt. Einige Benutzer verwenden aus Bequemlichkeit dasselbe Passwort bei jeder Registrierung oder wählen unsichere Passwörter, die leichter merkbar sind. Gelingt es einem Angreifer in einem solchen Szenario die Zugangsdaten bei nur einem Dienst zu erfahren, dann kann er sich bei allen anderen Diensten, bei denen die gleichen Zugangsdaten verwendet werden, ebenfalls anmelden und sich als das Opfer ausgeben. Weiterhin bieten viele Dienste keine anderen Authentifizierungsmerkmale als Benutzername und Passwort, so dass eine sicherere Authentifizierung dort nicht möglich ist.

Der offene Standard OpenID ermöglicht die Registrierung und Anmeldung bei allen teilnehmenden Webseiten und Webanwendungen mit nur einem Benutzerkonto. Vor dem Erhalt einer OpenID muss sich der Benutzer bei dem von ihm gewählten OpenID-Provider registrieren. Die dezentralisierte Gestaltung des Protokolls erlaubt beliebig viele OpenID-Provider, so dass jeder Benutzer frei wählen kann. Bei der Registrierung vereinbart er die Zugangsdaten für die dortige Anmeldung. Einige OpenID-Provider ermöglichen die Verwendung von sehr sicheren Authentifizierungsmerkmalen und teilweise auch eine Multi-Faktor-Authentifizierung.

Nach der erfolgreichen Registrierung kann der Benutzer einen OpenID-Identifier erstellen. Dieser repräsentiert seine Online-Identität und ist wie eine E-Mail-Adresse

weltweit einmalig. Viele OpenID-Provider erlauben den Benutzern mehrere OpenID-Identifier an ein Benutzerkonto zu binden, so dass der Benutzer für verschiedene Anwendungszwecke unterschiedliche Identifier verwenden kann. Da diese alle zu einem Benutzerkonto gehören, werden für die Verwendung keine weiteren Zugangsdaten benötigt.

Webseiten und webbasierte Anwendungen, die die Authentifizierung mittels OpenID erlauben, werden Relying-Party oder Konsumenten genannt. Wenn ein Benutzer sich bei einem dieser Konsumenten anmelden möchte, gibt er auf dessen Webseite seinen OpenID-Identifier ein. Der Konsument überprüft, zu welchem OpenID-Provider der Identifier gehört und leitet den Browser des Anwenders dorthin weiter. Der Benutzer meldet sich beim OpenID-Provider an und wird anschließend gefragt, ob er den angegebenen OpenID-Identifier für den Konsumenten benutzen möchte. Danach wird er automatisch zurück zum Konsumenten weitergeleitet. Dort wird überprüft, ob die Authentifizierung beim OpenID-Provider erfolgreich war. Im Erfolgsfall ist der Benutzer beim Konsumenten angemeldet.

Wenn ein Konsument mehr als nur den Identifier von einem Benutzer erfahren will, dann kann er seinen Wunsch nach beispielsweise dem Namen oder der E-Mail-Adresse bei der Weiterleitung zum Provider mitsenden. Nach der Anmeldung bei seinem Provider wird der Benutzer automatisch nach den geforderten Attributen gefragt. Da viele Konsumenten die gleichen Attribute verlangen, ermöglichen viele Provider das Hinterlegen von vorausgefüllten Kontaktdaten zu einer OpenID. Bei der Nachfrage nach den gewünschten Attributen kann der OpenID-Besitzer diese Kontaktkarten falls vorhanden auswählen oder die Angaben per Hand in die angezeigten Formularfelder eintragen. Da diese Angaben in der Regel nicht vom OpenID-Provider auf Korrektheit überprüft werden, darf ihnen bei einer Online-Wahl nicht vertraut werden.

Weitergehend wird in dieser Arbeit eine Lösung vorgestellt, bei der die Identität des Wählers bestmöglich geschützt wird, daher ist hier die Frage nach persönlichen Daten nicht erlaubt. Aus diesen Gründen wird dieses Feature in dieser Arbeit nicht weiter behandelt und wurde nur der Vollständigkeit wegen beschrieben.

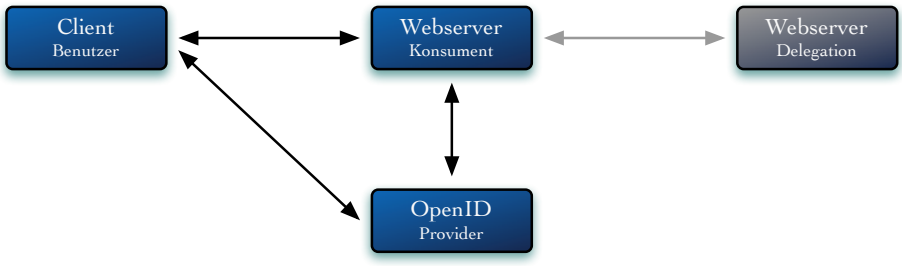

Abbildung 3.3: Die Komponenten von OpenID

3.4.1 Beschreibung

Die Kommunikation zwischen dem Konsumenten und dem OpenID-Provider kann in zwei verschiedenen Weisen erfolgen.

Im *Dumb Mode* fragt der Konsument, nachdem der Benutzer vom OpenID-Provider zu ihm zurück geleitet wurde, den OpenID-Provider, ob die Authentifizierung erfolgreich war. Dazu wird eine direkte Verbindung zwischen dem Konsumenten und dem OpenID-Provider aufgebaut, die vom Benutzer unabhängig ist. Der OpenID-Provider prüft mit Hilfe der übergebenen Parameter den Status der Authentifizierung des Benutzers und sendet dem Konsumenten als Antwort eine positive oder negative Bestätigung.

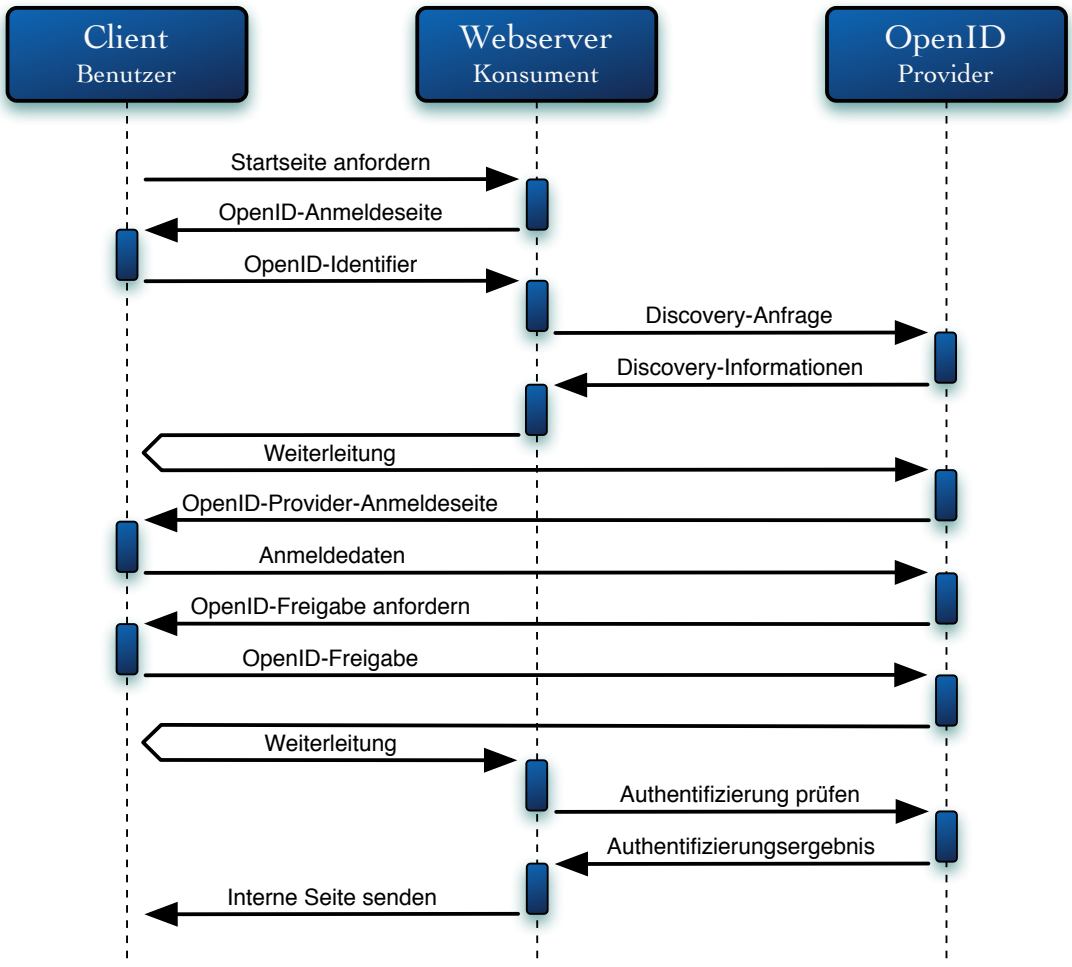

Abbildung 3.4: Ablauf OpenID im Dumb Mode

Im *Smart Mode* baut der Konsument, bevor er den Benutzer zum OpenID-Provider weiterleitet, eine direkte Verbindung zu diesem auf und vereinbart ein gemeinsames Geheimnis mit ihm. Mit Hilfe dieses Geheimnisses kann der Konsument, nachdem der Benutzer vom OpenID-Provider wieder zu ihm weitergeleitet wurde, selbst die erfolgreiche Authentifizierung prüfen, ohne den OpenID-Provider erneut kontaktieren zu müssen. Falls der Konsument mit dem OpenID-Provider schon bei einer vorherigen Authentifizierung ein gemeinsames Geheimnis vereinbart hat und dieses noch gültig ist, wird keine direkte Verbindung benötigt und das vorhandene Geheimnis zur Prüfung verwendet.

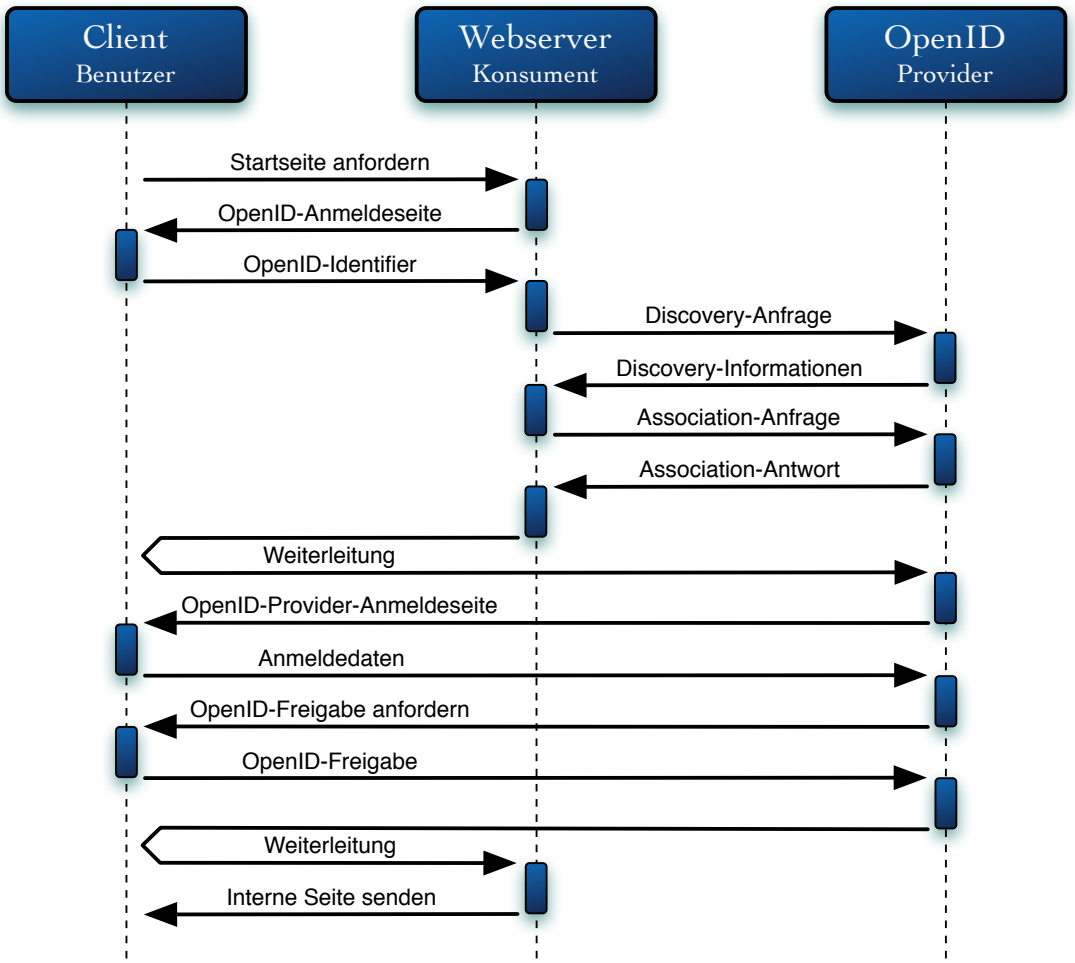

Abbildung 3.5: Ablauf OpenID im Smart Mode

3.4.2 Ablauf

OpenID-Identifier: Ein OpenID-Identifier repräsentiert die Online-Identität des Besitzers. Jeder Identifier ist weltweit eindeutig und besitzt das Format einer URL. Die Anmeldeseite eines Konsumenten enthält ein Textfeld, welches mit einem kleinen OpenID-Symbol gekennzeichnet ist. Der Benutzer gibt dort seinen OpenID-Identifier ein und klickt auf „Anmelden“.

Die Daten werden per *HTTP-POST*, je nach Dienst *SSL*-verschlüsselt oder im Klartext, übertragen.

Discovery: Nachdem der Konsument den OpenID-Identifier des Benutzers erhalten hat, sucht er nach dem zugehörigen OpenID-Provider und dessen unterstützte OpenID-Protokollversion [OA1], [OA2]. Dieser Vorgang wird als Discovery bezeichnet.

Dazu überführt der Konsument zuerst den empfangenen OpenID-Identifier in eine kanonische Form und benutzt den daraus resultierenden URL, der zu einer OpenID-Identity-Page führt. Dies ist eine Webseite mit beliebigem Inhalt, die in ihrer *HEAD-Sektion* das Tag *openid.server* mit der URL zum zugehörigen OpenID-Provider enthält. Bei einer delegierten OpenID wird dort zusätzlich das Tag *openid.delegate* mit dem Identifier beim Provider abgegeben. Danach erfragt der Kosument vom zugehörigen Provider dessen unterstützte Protokollversion.

Der Besuch der Identity-Page erfolgt mit einem *HTTP-* bzw. *HTTPS-Request*. Die Kommunikation zwischen dem Konsumenten und dem OpenID-Provider erfolgt per *POST*.

Association: Im *Smart Mode* wird bei der Association ein gemeinsames Geheimnis zwischen dem Konsumenten und dem OpenID-Provider vereinbart. Dazu baut der Konsument eine direkte Verbindung zu diesem auf. Falls schon ein Geheimnis zwischen dem Konsumenten und dem OpenID-Provider vereinbart wurde und diese noch gültig ist, dann wird kein neues Geheimnis vereinbart.

Im *Dumb Mode* wird dieser Schritt ausgelassen.

Weiterleitung zum Provider: Der Konsument sendet dem Browser des Benutzers eine Weiterleitung, so dass dieser automatisch zu seinem OpenID-Provider geleitet wird. Dabei werden als Parameter unter anderem der OpenID-Identifier und die Rücksprung-URL vom Konsumenten mitgesendet. Im *Smart Mode* wird zusätzlich ein Teil des vereinbarten gemeinsamen Geheimnisses mitgesendet.

Die Weiterleitung erfolgt mittels eines *HTML-Redirects*, die Parameter werden per *GET* übertragen.

Anmeldung beim OpenID-Provider: Nachdem der Benutzer zu seinem OpenID-Provider geleitet wurde, sendet dieser ihm eine Authentifizierungsaufforderung. Der Benutzer meldet sich mit seinen Zugangsdaten bei seinem OpenID-Provider an. Die dafür verwendeten Authentifizierungsmerkmale wurden bei der Registrierung des Benutzers beim OpenID-Provider festgelegt. Welche Merkmale dafür verwendet werden können ist vom jeweiligen OpenID-Provider abhängig.

Für den Fall, dass der Benutzer schon beim OpenID-Provider angemeldet und diese Anmeldung noch gültig ist, wird diese nur geprüft und der Benutzer muss keine weiteren Daten übermitteln.

OpenID-Freigabe: Nach der erfolgreichen Anmeldung beim OpenID-Provider fragt dieser den Benutzer, ob er den erhaltenen OpenID-Identifier für die Verwendung beim Konsumenten erlauben möchte. Damit diese Frage nicht bei jeder Anmeldung erscheint, kann der Benutzer diese Erlaubnis auch dauerhaft erteilen. Falls bereits eine dauerhafte Freigabe für die Verwendung des Identifiers bei diesem Konsumenten existiert, entfällt diese Frage.

Weiterleitung zum Konsumenten: Sobald der OpenID-Provider alle nötigen Informationen vom Benutzer erfahren hat, sendet er dem Browser des Benutzers eine Weiterleitung zum Konsumenten. Dabei wird die vom Konsumenten erhaltene Rücksprung-URL verwendet.

Wie bei der Weiterung zum OpenID-Provider wird auch hierbei ein *HTML-Redirect* verwendet und die Parameter werden per GET übertragen.

Authentifizierung verifizieren: Wenn der Benutzer wieder beim Konsumenten angekommen ist, dann fragt im *Dump Mode* der Konsument den OpenID-Provider, ob die Authentifizierung des Benutzers erfolgreich war. Dazu baut er eine unabhängige direkte Verbindung zum OpenID-Provider auf und übermittelt die Parameter für die Abfrage per *POST*.

Im *Smart Mode* nutzt der Konsument das bei der Association vereinbarte gemeinsame Geheimnis für die Verifizierung der erfolgreichen Authentifizierung des Benutzers beim OpenID-Provider. Somit wird keine weitere Verbindung zum OpenID-Provider benötigt.

3.4.3 Verwendung

OpenID wurde anfangs verstärkt für die Anmeldung bei *Blogs* verwendet. Ein Nutzer, der hier einen Kommentar zu einem bestimmten Thema abgeben möchte, muss sich üblicherweise zuvor an dem betreffenden Blog anmelden, um Missbrauch zu verhindern. Daher brauchte ein Nutzer, der in vielen Blogs Einträge kommentiert, viele Zugangsdaten. Durch den offenen Standard OpenID wurde dieses Problem

gelöst. Der Leser braucht nur noch die Zugangsdaten für seinen OpenID-Provider und kann sich bei jedem Blog, der die Authentifizierung mit OpenID unterstützt, ohne weitere Zugangsdaten anmelden. Ein weiterer großer Vorteil ist die Einmaligkeit der OpenID-Identifier. Im Gegensatz zu klassischen Benutzernamen kann der Identifier nicht von einem anderen Nutzer belegt sein. Somit kann ein Kommentarschreiber bei allen Blogs denselben Identifier verwenden, um deutlich zu machen, dass alle Einträge von ihm stammen. Dabei bleibt, falls er es nicht anders wünscht, seine wirkliche Identität geheim.

Den Versuch, eine *Single-Sign-On*-Lösung für das Internet zu etablieren, haben schon vor OpenID viele große Firmen unternommen, jedoch haben sich deren Lösungen nicht übergreifend durchgesetzt. Aktuell gibt es über 500.000.000 OpenID-Konten und über 25.000 Webseiten, die eine Verwendung von OpenID ermöglichen [Jan]. Große Unternehmen wie *Sun Microsystems*, *IBM*, *Microsoft*, *Yahoo*, *MySpace*, *Facebook* und viele mehr haben sich der Technologie von OpenID angeschlossen und die Zahl der Benutzer, Konsumenten und OpenID-Provider wächst seit Beginn ständig.

3.5 Vergleich von Kerberos und OpenID

In diesem Abschnitt werden die Eignung von Kerberos und OpenID in Verbindung mit einem Online-Wahlsystem verglichen.

Aus den Anforderungen an ein Online-Wahlsystem geht hervor, dass es für einen Benutzer möglichst intuitiv bedienbar sein muss und ihm keine außergewöhnlichen Kenntnisse abverlangen darf. Daher darf auch im Vorfeld von den Benutzern keine Installation von zusätzlichen Programmen oder Plug-Ins gefordert werden, denn falls ein Wahlberechtigter an dieser Hürde scheitern würde, könnte er folglich nicht an der Wahl teilnehmen.

Kerberos wurde im Gegensatz zu OpenID nicht für die Authentifizierung bei webbasierten Diensten entwickelt, daher wird für die Authentifizierung ein Plug-In benötigt. Für die Nutzung von OpenID benötigt der Anwender nur einen Browser, so dass er nichts Zusätzliches installieren oder konfigurieren muss.

Eine Lösung mit Kerberos ist nicht dezentral. Es gibt für alle Benutzer nur ein einziges Kerberos-System. Daher kann der einzelne Benutzer nicht entscheiden, von welchem Server er authentifiziert werden möchte. Weiterhin müssen in der Schlüsseldatenbank alle Schlüssel der Wahlberechtigten hinterlegt sein. Diese müssen mit jedem Wahlberechtigten vor einer Wahl vereinbart werden. Auf das Format dieser Schlüssel hat der Benutzer keinen Einfluss, er kann nur die erhaltenen Authentifizierungsmerkmale verwenden und keine zusätzlichen vereinbaren.

Das Protokoll von OpenID hingegen ermöglicht eine dezentrale Serverstruktur, so dass grundsätzlich jeder OpenID-Provider für die Authentifizierung verwendet werden kann. Somit kann der Benutzer entscheiden, welchem Provider er seine Daten anvertrauen möchte. Entsprechend den Möglichkeiten des Providers kann der Benutzer entscheiden welche Authentifizierungsmerkmale er für die Nutzung seiner OpenID mit seinem Provider vereinbart. Dabei ist auch eine *Multi-Faktor-Authentifizierung* möglich. Die Kategorie der Authentifizierungsmerkmale muss nicht bei allen Wahlberechtigten gleich sein. So kann ein Wahlberechtigter, der im Besitz einer Smartcard und einem entsprechenden Lesegerät ist, diese für die Authentifizierung verwenden, jedoch werden nicht alle Wahlberechtigten gezwungen, sich diese zu beschaffen. Bei OpenID kann der Benutzer direkten Einfluss auf die Sicherheit seiner Authentifizierung nehmen.

Durch die Vielzahl der OpenID-Provider ist es besonders wichtig, dass der Wahlberechtigte sich einen vertrauenswürdigen OpenID-Provider auswählt. Der OpenID-Provider erfährt, bei welchen Konsumenten ein Benutzer seine OpenID verwendet. Daher sollte besonders im Hinblick auf den Datenschutz der OpenID-Provider sorgfältig geprüft werden. Im Kapitel 5 werden Auswahlkriterien für OpenID-Provider beschrieben.

Im Gegensatz zu Kerberos handelt es sich bei OpenID um einen offenen Standard, so dass das Protokoll zwar vollständig bekannt, aber nicht wie bei Kerberos sicherheitszertifiziert ist.

Unter dem Begriff *Single-Sign-Out* wird das Abmelden bei allen teilnehmenden Systemen bezeichnet. Wenn ein Benutzer ein Kerberos-Ticket erhalten hat, ist dieses bis zum Ende seiner Gültigkeitsdauer verwendbar. Bei OpenID braucht ein Benutzer nur seinen Browser schließen oder seine Session-Cookies löschen, um sicher von allen Systemen abgemeldet zu sein. Er kann sich auch von einzelnen Diensten gezielt abmelden.

Bei OpenID entscheidet der Benutzer für jeden Konsumenten einzeln, ob er dort seine OpenID zur Authentifizierung verwenden möchte. Er wird für jeden Konsumenten gefragt ob er seine Freigabe erteilt, falls er diese nicht schon dauerhaft erteilt hat. Eine dauerhafte Freigabe eines Konsumenten kann der Benutzer zu jeder Zeit bei seinem OpenID-Provider zurückziehen. Bei Kerberos hat der Benutzer keinen direkten Einfluss auf die Nutzung seiner Authentifizierung.

Im Gegensatz zu Kerberos ermöglicht OpenID nur die Authentifizierung eines Benutzers, es gibt keine Autorisierungsfunktionen. Ein Konsument kann nur nachfragen, ob sich ein Benutzer korrekt authentifiziert hat, die Autorisierung für seine Dienste vergibt er selber.

Bei Kerberos werden die Benutzer an einer zentralen Stelle gepflegt, so dass jeder einzelne Benutzer dieser Stelle vertrauen muss. Jedoch vereinfacht die Zentralisierung die Überprüfung.

Bei Kerberos kann der Benutzer keinen Einfluss auf seinen Benutzernamen, der dem Wahlsystem gemeldet wird, nehmen. Sollte aus seinem Benutzernamen Rückschlüsse auf seine Identität möglich sein, dann kann er nur auf den Datenschutz des Wahlsystems vertrauen. Da von einem OpenID-Identifier nicht auf die zugehörige Person geschlossen werden kann, ist für den Wahlberechtigten ersichtlich, dass seine Identität beim Wahlsystem geschützt ist. Selbst bei einem erfolgreichen Angriff auf das Wahlsystem kann der Angreifer nicht erkennen welcher Wahlteilnehmer gewählt hat und daher auch auf keinen Fall, wie ein Wahlteilnehmer gewählt hat.

Die Benutzerzentralisierung von OpenID ist ein entscheidender Vorteil bei der Verbindung mit einem Online-Wahlsystem. Der Wahlberechtigte erhält somit eine für ihn sichtbare Trennung von seiner Authentifizierung und dem Wahlvorgang. Er selber kann entscheiden, welchen OpenID-Provider und welchen OpenID-Identifier er für die Wahl verwenden möchte. Entsprechend der Möglichkeiten seines OpenID-Providers kann er seine Authentifizierungsmerkmale wählen und somit direkten Einfluss auf die Güte seiner Authentifizierung ausüben. Da er sich beim Wahlvorgang bei seinem OpenID-Provider anmeldet, geschieht dies an einer ihm vertrauten Stelle. Die Weiterleiterung vom Wahlsystem zu seinem OpenID-Provider sorgt für einen intuitiven Handlungsablauf und der Wahlberechtigte benötigt für die Teilnahme an einer Online-Wahl mit OpenID keine ungewohnten Programme. Im Gegensatz zu Kerberos stellt auch eine Network Address Translation (NAT), die bei vielen Internetzugängen üblich ist, kein Hindernis dar. Da nur HTTP und/oder HTTPS verwendet wird, entstehen auch keine Probleme mit existierenden Firewalls. Bei einem Online-Wahlsystem mit OpenID-Authentifizierung benötigt der Wahlberechtigte nur einen Browser und Internetzugang.

Beim Einsatz von OpenID vereinbart der Wahlberechtigte die Authentifizierungsmerkmale mit seinem OpenID-Provider, daher ist es nicht nötig, Zugangsdaten für das Wahlsystem zu versenden. Somit entstehen wie gefordert keine Kosten für PIN-Briefe, Smartcards oder Ähnliches. Die Verwendung von OpenID ermöglicht eine sehr sichere Authentifizierung, schafft eine deutliche Trennung zwischen dem Vorgang der Wählerauthentifizierung und dem Wahlvorgang und befreit das Wahlsystem von personenbezogenen Daten. Weiterhin entsteht der beschriebene Mechanismus zur Überprüfung der Wahlteilnahme, ohne dass die Geheimhaltung der Wahlteilnahme gefährdet wird. Da eine Lösung mit OpenID mehr Vorteile in Verbindung mit einem Online-Wahlsystem bietet im Vergleich zu Kerberos und alle geforderten Ziele dieser Arbeit erfüllt, wird OpenID für die Authentifizierung gegenüber dem Wahlsystem verwendet.

4 Online-Wahl mit OpenID

Der Wähler muss sich bei der Wahl authentifizieren, damit keine unberechtigten Personen sich als berechtigte ausgeben können. Danach wird die Wahlberechtigung der Person geprüft, um sicherzustellen, dass die Person wählen darf.

In diesem Kapitel werden die für eine Online-Wahl nötigen Identifizierungs-, Authentifizierungs- und Autorisierungsmethoden beschrieben. Dabei werden die für den Wahlberechtigten nötigen Informationen im Zusammenhang mit OpenID geschildert. Es wird gezeigt, wie die Identität eines Wahlberechtigten geprüft werden kann, ohne dass mehr Informationen als nötig über ihn weitergegeben werden. Jede Komponente soll so wenig wie möglich über die Personen, die wählen dürfen, wissen, aber genügend, um sicher zu sein, dass keine Unberechtigten es ausnutzen können.

Am Ende des Kapitels folgt eine abstrakte Beschreibung einer Online-Wahl mit OpenID aus der Sicht des Wählers sowie eine kurze Zusammenfassung.

4.1 Wahlberechtigung

Die Wahlberechtigung von jeder Person, die an der Wahl teilnehmen will, muss geprüft werden, damit keine Unberechtigten wählen können. Für eine solche Prüfung muss bekannt sein, welche Personen für die Wahl zugelassen sind. Diese Information besitzt der Wahlveranstalter. Er kennt alle Personen und ist in der Lage diese auch zu identifizieren.

Im Gegensatz zu einer Präsenzwahl kann die Legitimierung der Wahlteilnehmer nicht persönlich mit Hilfe eines Personalausweises und einer Wählerkarte direkt vor dem Erhalt eines Stimmzettels geprüft werden. Daher wird dieser Schritt vorgezogen. Vor dem Wahlstart werden alle für die Wahl zugelassenen Personen identifiziert und erhalten im Erfolgsfall die nötigen Merkmale für die Authentifizierung beim Wahlvorgang.

Beim Wahlvorgang wird der Wähler erst authentifiziert und danach seine Wahlberechtigung geprüft. Dabei wird sichergestellt, dass jeder Wähler nur einen Stimmzettel abgeben kann. Solange der Wähler den Stimmzettel nicht verbindlich abgegeben hat, darf er seine Auswahl korrigieren. Er darf auch seine Wahl unterbrechen und

zu einem späteren Zeitpunkt fortsetzen. Erst wenn er den Stimmzettel verbindlich abgegeben hat, wandert dieser in die Urne und seine Wahlberechtigung erlischt. Bei einem erneuten Versuch, an einen Stimmzettel zu gelangen, erhält er einen Hinweis, dass er seine Stimme schon abgegeben hat und für ihn die Wahl beendet ist.

4.2 Wählerkennung

Jedem Wahlberechtigten ist für die Dauer der Wahl eine Wählerkennung fest zugeordnet. Diese Zuordnung ist bijektiv und kann während des Wahlzeitraums nicht geändert werden. Mit Hilfe dieser Kennungen werden die Wahlberechtigten identifiziert und unterschieden.

Bei jeder Online-Wahl muss das Grundprinzip der Überprüfbarkeit erfüllt werden, daher sollte dem Wähler die Möglichkeit gegeben werden, sich in der Dokumentation der Auszählung des Wählerverzeichnisses wiederzufinden. In dieser stehen alle Wählerkennungen der Wahlberechtigten und ob deren Stimme abgegeben wurde.

Wenn als Wählerkennung der volle Name des Wählers verwendet wird, kann jeder Wähler leicht seinen Eintrag finden, doch auch jeder andere, der seinen Namen kennt. Sollte dies nicht gewünscht sein, dann kann jedem Wahlberechtigten eine nur ihm bekannte Kennung zugeordnet werden. Somit kann ein Außenstehender die Zuordnung zwischen den Wahlberechtigten und deren Wählerkennung nicht vornehmen.

Der Wahldienstleister erhält nur eine Liste mit den Kennungen der Wahlberechtigten, folglich besitzt er keine Kenntnis über die erfolgte Zuweisung. In diesem Szenario können nur noch die einzelnen Wahlberechtigten ihre und die Zuordnungsstelle alle Verbindungen zwischen der Wählerkennung und dem Wahlberechtigten herstellen, dem Wahldienstleister ist dies nicht möglich.

Da diese Wählerkennungen keine personenbezogenen Merkmale enthalten, ergeben sich bei deren Verarbeitung keine Probleme mit dem Datenschutz. Trotzdem ist ein sorgfältiger Umgang mit diesen Daten notwendig.

In dieser Arbeit wird der offene Standard OpenID (siehe Abschnitt 3.4) für die Wählerkennung verwendet. Jeder Wahlberechtigte gibt vor dem Wahlstart seinen OpenID-Identifier an, den er für die Wahl benutzen möchte. Dieser Identifier wird, wie im nächsten Abschnitt beschrieben, geprüft und im Erfolgsfall dem Wahlberechtigten als Wählerkennung fest zugeordnet.

Ein Ziel der OpenID-Technologie ist die Verhinderung von Rückschlüssen vom Identifier auf den zugehörigen Benutzer. Daher ist es nicht möglich, von einem

sorgfältig gewählten und genutzten OpenID-Identifier auf den Wahlberechtigten zu schließen.

Die Identity-Page der verwendeten OpenID sollte daher keine Informationen enthalten, mit deren Hilfe ein Dritter auf den Besitzer schließen kann. Da jeder Wahlberechtigte seine Daten selbst beim zugehörigen Provider verwaltet, kann er selber sicherstellen, dass seine Identity-Page keine unerwünschten Informationen enthält. Zu Beginn sind diese Seiten leer, so dass dort keine Daten zu finden sind. Der einfachste Weg Seiteneffekte auszuschließen ist das Anlegen einer neuen OpenID oder eines OpenID-Identifiers. Viele OpenID-Provider erlauben die Erstellung mehrerer Identifier zu einem OpenID-Account. Da diese alle an denselben Besitzer gebunden sind, werden keine weiteren Zugangsdaten benötigt.

Es empfiehlt sich daher einzig für Online-Wahlen genutzte OpenID-Identifier zu verwenden. Der Wahlberechtigte kann durch den Einsatz von OpenID als Wählerkennung direkten Einfluss auf die Geheimhaltung seiner Identität und die Sicherheit bei der Authentifizierung nehmen.

4.3 Verteilung der Wählerkennungen

Vor jeder Wahl müssen alle Wählerkennungen erfasst werden und die einzelnen Wählerkennungen den jeweiligen Wahlberechtigten bekannt sein. Erst nachdem alle Kennungen erfasst wurden, wird das Wählerverzeichnis erstellt.

Das Versenden von Wählerkennungen an die Wahlberechtigten verursacht, besonders ohne vorhandene Infrastrukturen zur sicheren elektronischen Übertragung, hohe Kosten. Wenn für die Wählerkennungen OpenID-Identifier verwendet werden, die die Wahlberechtigten selber angeben, ist das Versenden von Wählerkennungen unnötig und es können die Kosten für die Erstellung und Versendung von Briefen mit Zugangsdaten eingespart werden. Weiterhin kann auch kein Wahlanschreiben mit Zugangsdaten oder PIN-Brief abgefangen oder verfälscht werden.

Wenn die OpenIDs der Wahlberechtigten schon bekannt sind, beispielweise von der Nutzung anderer Dienste des Wahlveranstalters, dann muss noch über die Sicherheitsanforderungen der zugehörigen OpenID-Provider entschieden werden. Kapitel 5 enthält eine Beschreibung der Auswahlkriterien hierfür. Falls diese den Wahlbedingungen entsprechen, steht der Verwendung dieser OpenIDs nichts im Wege. Sollten die Wahlberechtigten noch keine OpenIDs haben oder ihre OpenIDs zu nicht akzeptierten OpenID-Providern gehören, benötigen sie eine neue bzw. weitere nach den Wahlbestimmungen zugelassene OpenID.

Haben die Wahlberechtigten alle eine OpenID, denen der Wahlveranstalter vertraut, muss sichergestellt werden, dass jeder Wahlberechtigte nur eine OpenID zur Wahl benutzen kann. Sollte ein Wahlberechtigter eine weitere OpenID angeben, wird je nach Entscheidung des Wahlveranstalters die alte ersetzt oder die neue abgelehnt. Bei jeder Angabe einer OpenID muss die Identität des zugehörigen Wahlberechtigten zweifelsfrei geprüft werden, damit keine unberechtigten Personen Daten angeben können.

Die Erfassung der OpenID-Identifier kann persönlich erfolgen. Dabei geht der Wahlberechtigte zu einer mit der Erfassung beauftragten vertrauenswürdigen Person. Dort weist er seine Identität mit beispielsweise einem gültigen Ausweisdokument nach und gibt danach seinen OpenID-Identifier an. Für den Nachweis, dass es wirklich sein OpenID-Identifier ist und zur Prüfung der Zulassung des OpenID-Providers für die Wahl muss er sich vor Ort bei seinem OpenID-Provider anmelden. Wenn der Wahlberechtigte und seine OpenID alle Bedingungen erfüllt haben, dann wird der OpenID-Identifier in die Liste der Wählerkennungen aufgenommen.

Eine persönliche Prüfung erfordert jedoch, dass der Wahlberechtigte zu festgelegten Erfassungsstellen geht und ist daher nicht sehr komfortabel. Weiterhin ist diese Art der Prüfung bei einer großen Anzahl von Wahlberechtigten sehr zeit-, personal- und kostenintensiv. Daher empfiehlt sich bei einer Online-Wahl die Wählerkennungen online zu erfassen.

Bei einer Online-Erfassung der OpenID-Identifier wird ein nur dafür entwickeltes Registrierungssystem verwendet. Analog zur persönlichen Prüfung muss auch hier die Identität der Wahlberechtigten nachgewiesen werden. Dazu kann falls vorhanden eine Portallösung oder ein ähnliches System, welches die Benutzer zweifelsfrei authentifiziert, mit dem Registrierungssystem verbunden werden. Wenn die Identitäten der Benutzer zweifelsfrei geprüft und deren Wahlberechtigungen festgestellt wurden, werden sie direkt an das System zur Erfassung der Wählerkennungen weitergeleitet. Dort wird automatisch die OpenID und der zugehörige OpenID-Provider geprüft. Eine detaillierte Beschreibung eines solchen Registrierungssystems und dessen Verwendungsmöglichkeiten folgt in den Kapiteln 8 und 9.

Eine Verteilung der Wählerkennungen muss nicht stattfinden, wenn schon jeder Wahlberechtigte einen geprüften OpenID-Identifier besitzt. Diese können entweder durch frühere Wahlvorgänge oder andere Verwendungen, wie beispielsweise eine unternehmensweite *SSO-Lösung* mit OpenID, bekannt sein. Wenn das Vertrauen in schon bekannte und geprüfte OpenID-Identifier nicht geschwächt wurde, spricht nichts gegen deren Verwendung.

Vor der Erstellung des Wählerverzeichnisses muss die endgültige Zuordnung zwischen den Wahlberechtigten und den OpenID-Identifiern hergestellt sein. Diese kann

aus Sicherheitsgründen während der Wahldurchführungsphase nicht mehr geändert werden.

Für die Erstellung des Wählerverzeichnisses wird nur die Liste der OpenID-Identifier und nicht die der Wahlberechtigten weitergegeben.

4.4 Abstrakte Beschreibung aus Wählersicht

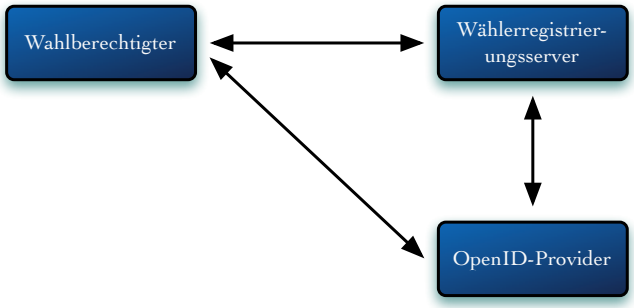

Abbildung 4.1: Die Komponenten des Registrierungssystems

1. **Registrierung der Wählerkennung.**
   a) Identität der Person wird geprüft.
   b) Teilnahmeberechtigung an der Wahl wird geprüft.
   c) Wahlberechtigter gibt seinen OpenID-Identifier an.
   d) OpenID-Identifier mit zugehörigem OpenID-Provider wird geprüft.
   e) Zugehörigkeit zwischen Wahlberechtigtem und OpenID wird geprüft.
   f) OpenID-Identifier wird als Wählerkennung für den Wahlberechtigten gespeichert.
2. **Wählerverzeichnis wird erstellt.**
3. **Wahl wird gestartet.**

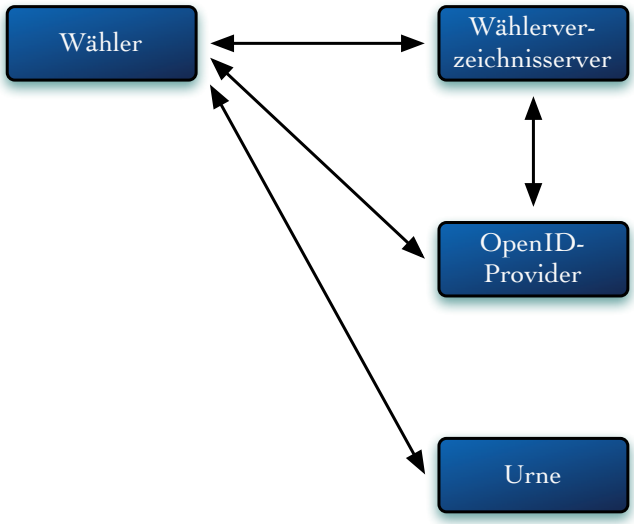

Abbildung 4.2: Die Komponenten des Online-Wahlsystems

4. **Wahlvorgang.**
   a) Wähler meldet sich mit seinem OpenID-Identifier am Wahlsystem an.
   b) Wähler authentifiziert sich bei seinem OpenID-Provider.
   c) Wahlsystem verifiziert Authentifizierung beim OpenID-Provider.
   d) Wahlberechtigung wird geprüft.
   e) Wähler erhält einen Stimmzettel.
   f) Wähler wählt und gibt seinen Stimmzettel verbindlich ab.
   g) Stimmabgabe des Wählers wird im Wählerverzeichnis vermerkt.
5. **Wahl wird beendet.**
6. **Wahl wird ausgezählt und Ergebnis veröffentlicht.**

Sollte ein Fehler auftreten, dann wird abgebrochen. Ein Fehler oder ein Abbruch durch den Teilnehmer während der Registrierung der Wählerkennung oder während des Wahlvorgangs unterbricht den Ablauf, so dass dieser Teil erneut vollständig durchlaufen werden muss.

4.5 Folgerung

Bei einer Online-Wahl mit OpenID kann der Wahlberechtigte direkten Einfluss auf die Sicherheit seiner Authentifizierung beim Wahlvorgang nehmen. Er kann (aus den für die Wahl zugelassenen OpenID-Providern) frei wählen, welchem OpenID-Provider er vertraut und diesen für die Wahl verwenden. Für die Authentifizierung bei seinem Provider kann er aus den dort angebotenen Methoden diejenige auswählen, die für ihn den besten Kompromiss aus Sicherheit und Verwendbarkeit darstellt. Falls ein Wahlberechtigter schon eine OpenID bei einem vertrauenswürdigen Provider besitzt, dann kann er auch diese für die Wahl verwenden. Somit kann die Authentifizierung beim Wahlvorgang einem ihm vertrauten Dienst übergeben werden und er muss nicht wie sonst auf die Güte der Authentifizierungsmechanismen des Wahlsystems vertrauen.

Da das Wahlsystem nur die OpenID-Identifier der Wahlberechtigten kennt, können von dort keine Rückschlüsse auf die teilnehmenden Personen gezogen werden. Deshalb ist auch bei einem erfolgreichen Angriff auf das Wahlsystem die Identität der Wahlteilnehmer geheim. Sollte ein Angreifer alle Komponenten des Wahlsystems unter seine Kontrolle bringen, kann er selbst dann nicht erfahren, welche Person an der Wahl teilgenommen hat oder wie diese gewählt hat. Er erfährt nur die OpenID-Identifier, aber nicht die Zuordnung zu den Personen. Um zu erkennen, welche Person wie gewählt hat, müsste er noch die verwendeten, vom Wahlsystem unabhängigen OpenID-Provider oder alle Bestandteile des Registrierungssystems vor dem Wahlstart erfolgreich angreifen. Sollte beim Registrierungssystem ein Angriff bemerkt werden, würde der Wahlstart nicht erfolgen.

Durch den Einsatz von OpenID-Identifiern als Wählerkennungen brauchen keine Zugangsdaten per Post verteilt werden. Daher können die Kosten für die Erstellung und Verteilung von PIN-Briefen eingespart und keine Briefe von Unberechtigten abgefangen werden.

Die Wahlberechtigten kennen nur ihren OpenID-Identifier und wissen nicht, welche Wahlberechtigten zu den anderen Identifiern gehören. Folglich kann die Dokumentation des Wählerverzeichnisses, in der zu jedem OpenID-Identifier vermerkt ist. ob mit diesem gewählt wurde oder nicht, veröffentlicht werden, ohne dass ein Wahlberechtigter erkennt, ob ein anderer gewählt hat. Jedoch kann jeder Wahlberechtigte erkennen ob mit seiner Wählerkennung eine Stimme verbindlich abgeben wurde oder nicht. Weiterhin kann jeder, der diese Dokumentation einsehen kann, überprüfen, ob die Anzahl der zur verbindlichen Stimmabgabe genutzten OpenID-Identifier mit der Anzahl der Stimmen aus der Urne übereinstimmt. Besonders im Bezug auf die geforderte Überprüfbarkeit einer Wahl ist dies ein großer Vorteil.

Die Sicherheit des vorgestellten Online-Wahlsystems hängt direkt von der Sicherheit der verwendeten OpenID-Provider ab. Daher kann die Zulassung der Provider für die Wahl eingeschränkt werden. Im nächsten Kapitel werden Kriterien, nach denen die Provider ausgewählt werden können, beschrieben.

5 Auswahlkriterien für OpenID-Provider

Der offene Standard OpenID wurde für vielfältige Einsatzgebiete entwickelt. Daher bieten einige OpenID-Provider Funktionen, wie beispielsweise die Verwendung von Infocards für das automatische Ausfüllen von Kontaktformularen beim Konsumenten. Solche für eine Wahl nicht relevanten Funktionen werden in den folgenden Abschnitten nicht betrachtet. Die Auswahlkriterien beziehen sich auf die im Zusammenhang mit einer Online-Wahl wichtigen Funktionen der OpenID-Provider.

In diesem Kapitel werden zuerst die Arten der Identifizierung bei der Registrierung eines OpenID-Accounts kategorisiert und danach die Authentifizierungsvarianten bei der Nutzung einer OpenID beschrieben. Nachfolgend werden die verschiedenen Arten der Zulassungsbeschränkungen von OpenID-Providern bei einer Online-Wahl vorgestellt und abschließend die Folgen für ein Online-Wahlsystem geschildert.

5.1 Identifizierung bei der Registrierung

Vor der Erstellung eines OpenID-Identifiers muss sich der Nutzer bei einem OpenID-Provider anmelden. Wenn er noch kein Benutzerkonto beim OpenID-Provider hat, muss er sich dort zuerst registrieren. Bei der Registrierung kann die Identität des neuen Nutzers in unterschiedlicher Güte geprüft werden. Die Intensität der Prüfung bei der Registrierung sollte bei der Auswahl der OpenID-Provider für eine Wahl berücksichtigt werden. OpenIDs, die ohne Personenprüfung erhältlich sind, werden zwecks Stimmenkauf leichter weitergegeben als personengebundene. Die Methoden der Registrierung lassen sich wie folgt kategorisieren.

Keine Identifizierung

Einige OpenID-Provider verlangen bei der Registrierung nur einen noch nicht vergebenen Benutzernamen und ein Authentifizierungsmerkmal. Somit werden keine personenbezogenen Daten gefordert und es findet keine Identitätsprüfung statt.

E-Mail

Bei der Registrierung verlangen viele OpenID-Provider neben einem freien Benutzernamen und einem Authentifizierungsmerkmal, eine E-Mail-Adresse, um diese für die Übermittlung eines Freischaltcodes oder -links nutzen zu können. Dabei findet keine wirkliche Identifizierung der Person selbst statt, da auch Einweg-E-Mail-Adressen erlaubt sind und eine E-Mail-Adresse keine zweifelsfreien Rückschlüsse auf deren wirklichen Besitzer ermöglicht. Die Verwendung von E-Mails bei der Registrierung soll das missbräuchliche Erstellen von Benutzerkonten verhindern und bietet keine sichere Identitätsprüfung.

Postident

Es gibt OpenID-Provider, die bei der Registrierung einen Identitätsnachweis mittels *Postident* verlangen. *Postident* ist ein Verfahren zur Personenidentifizierung der *Deutschen Post AG* [Pos]. Es gibt verschiedene Varianten des *Postident*-Verfahrens, die eine Identifizierung in der Filiale, am Empfängerort oder an der Haustür ermöglichen. Dabei wird je nach Variante die Identität des Empfängers nach den Vorgaben des Geldwäschegesetzes [GwG] oder Signaturgesetzes [Sig01] durch den Mitarbeiter einer Filiale oder den Briefzusteller geprüft. Zusätzlich kann auch ein personalisiertes Dokument zur Unterschrift verwendet werden. Mit Hilfe von Postident kann die Identität eines neuen Benutzers bei der Registrierung sicher geprüft werden.

Persönliche Identifizierung

Denkbar ist auch die Auflage einer persönlichen Identifizierung. In diesem Fall muss der Antragsteller für die Registrierung persönlich zum OpenID-Provider gehen und sich dort mit Hilfe von gültigen Ausweisdokumenten identifizieren. Erst nachdem seine Identität zweifelsfrei geprüft wurde, kann er eine OpenID erstellen. Dies ist bei sorgfältiger Prüfung eine sehr sichere Methode für die Identitätsfeststellung, jedoch nicht sehr komfortabel für die Benutzer, da sie persönlich zu einer Prüfungsstelle gehen müssen. Die Sicherheit dieser Methode hängt ausschließlich von der Qualität der Prüfung und der Arbeitsweise des Prüfers ab.

5.2 Authentifizierung bei der Nutzung

Der Fokus der OpenID-Technologie liegt eher auf der sicheren Authentifizierung bei der Nutzung als der Identifizierung bei der Registrierung. Da es sich bei OpenID wie

schon beschrieben um ein benutzerzentralisiertes Authentifizierungssystem handelt, gibt es vielfältige Möglichkeiten, für den OpenID-Nutzer sich zu authentifizieren. Eine sichere Authentifizierung des Nutzers vor der Freigabe zur Verwendung einer OpenID soll den Identitätsdiebstahl und -missbrauch verringern. Es stehen je nach OpenID-Provider folgende Merkmale zur Verfügung, die auch teilweise kombiniert werden können.

Bei der Registrierung werden die folgend beschriebenen Authentifizierungsmerkmale für die Anmeldung beim OpenID-Provider vereinbart. Welche Merkmale verwendet werden können, ist vom OpenID-Provider abhängig. Vielen OpenID-Provider bieten mehrere an, so dass der Benutzer auswählen kann.

Benutzername und Passwort

Bei dieser Variante wird vom Nutzer ein Benutzername mit zugehörigem Passwort gefordert. Dies ist die häufigste Methode bei der Anmeldung bei OpenID-Providern. Wie in Abschnitt 3.1 beschrieben, handelt es sich um ein Merkmal der Kategorie *Wissen* und ist gut geeignet für eine Multi-Faktor-Authentifizierung. Für die Verwendung solcher Authentifizierungsmerkmale sind keine zusätzlichen Geräte nötig. Da der Benutzer sein Passwort selbst wählen darf, besteht die Gefahr, dass er ein schwaches Passwort angibt. Oft werden auch die Passwörter von den Benutzern aufgeschrieben, damit sie nicht vergessen werden. Wenn ein Dritter das Passwort erfährt, dann kann er es unbemerkt kopieren.

SSL-Client-Zertifikat

Für die Anmeldung beim OpenID-Provider wird ein vorher vereinbartes SSL-Client-Zertifikat verwendet. Dieses Zertifikat kann entweder beim OpenID-Provider direkt oder bei einer anderen vertrauenswürdigen Stelle generiert werden. Es gibt mehrere Anbieter, die kostenlos solche sicheren Zertifikate herausgeben.

Ein SSL-Client-Zertifikat kann beispielsweise im Browser installiert werden und anstelle von Benutzername und Passwort für die Authentifizierung bei der Anmeldung genutzt werden. Es ist ein besitzbasiertes Merkmal und kann im Gegensatz zu Passwörtern nicht so einfach erraten werden. Da bei der Verwendung das Geheimnis nicht über die Tastatur eingeben wird, kann es nicht einfach abgeschaut und mittels Keylogger oder Schadsoftware abgegriffen werden. Zum Kopieren eines SSL-Client-Zertifikats benötigt der Angreifer Zugriff auf die Daten des Zertifikates. Es reicht nicht, die übertragenen Daten für die Authentifizierung zu kopieren.

Smartcard

Einige OpenID-Provider erlauben die Verwendung von Smartcards. Für die Authentifizierung beim OpenID-Provider benötigt der Benutzer eine Smartcard und ein passendes Lesegerät. Es gibt eine Vielzahl von Smartcards und Lesegeräten, die bei OpenID-Providern verwendet werden können, so dass ein Benutzer eventuell vorhandene Karten und Geräte nutzen kann. In einigen Ländern, wie Belgien und Finnland, gibt es vom Staat ausgegebene Smartcards (*Belgium Identity Card* & *FineID, Finland National ID Card*), die auch für die Authentifizierung verwendet werden können.

Smartcards gehören zu der Kategorie der besitzbasierten Authentifizierungsmerkmale und können nicht oder nur mit sehr großem Aufwand kopiert werden. Der Verlust einer solchen Karte fällt spätestens beim nächsten Nutzungsversuch auf.

Viele Smartcards lassen sich mit einer PIN kombinieren, so dass eine Zwei-Faktor-Authentifizierung entsteht.

Security-Token

Die Authentifizierung mit Security-Token ist bei einigen OpenID-Providern ebenfalls möglich. Einige Security-Token können direkt mit dem Computer verbunden werden, so dass kein zusätzliches Lesegerät benötigt wird. Andere arbeiten eigenständig und haben ein Display, das einen Zeichencode anzeigt. Dieser Code wechselt in festgelegten Intervallen, so dass der Benutzer bei der Verwendung den momentan angezeigten Code mittels Tastatur eingeben muss. Dabei wird auch kein Lesegerät benötigt.

Die Security-Token nutzen entweder Zertifikate, wie Smartcards, oder *Einmal-Passwörter*. Beim *Einmal-Passwort-Verfahren* wird der temporär angezeigte Code verwendet.

Ähnlich wie Smartcards sind Security-Token nicht oder nur mit sehr großem Aufwand kopierbar. Sie gehören ebenfalls in die Kategorie der besitzbasierten Authentifizierungsmerkmale und können mit anderen kombiniert werden.

Biometrie

Einige OpenID-Provider ermöglichen auch den Einsatz von biometrischen Merkmalen für die Authentifizierung. Dazu benötigt der Nutzer ein geeignetes Lesegerät und passende Software, die auch kostenlos erhältlich ist.

Beispielsweise der OpenID-Provider *TrustBearer OpenID* [Tru] ermöglicht eine Authentifizierung mit Smartcards, Security-Token oder Biometrie.

CallVerifID

Bei dieser Art der Benutzerprüfung hinterlegt der OpenID-Besitzer seine Telefonnummer beim zugehörigen OpenID-Provider.

Beispielsweise der OpenID-Provider *myOpenID* [myO] nutzt *CallVerifID* von *PhoneFactor* [Pho] zur Zwei-Faktor-Authentifizierung. Bei der Anmeldung wird zunächst ein Passwort oder Zertifikat gefordert und erst wenn dieses erfolgreich geprüft wurde, erhält der OpenID-Besitzer einen Anruf auf der angegeben Telefonnummer. Mit Hilfe seines Telefons authentifiziert er sich durch Drücken der #-Taste oder der Eingabe der zuvor festgelegten Nummer.

Die *CallVerifID* wird als zweites Merkmal zur Zwei-Faktor-Authentifizierung verwendet. Nur wenn die erste Stufe der Anmeldung erfolgreich durchgeführt wurde, wird eine telefonische Anfrage gestellt. Dies dient als Schutz vor Missbrauch. Der Besitzer der OpenID bekommt folglich nicht bei jedem unberechtigten Verwendungsversuch seiner OpenID eine Authentifizierungsanfrage per Telefon. Neben der Erhöhung der Sicherheit durch den zweiten Faktor, erfährt der OpenID-Besitzer auch sofort, falls sein Authentifizierungsmerkmal für den ersten Faktor überwunden wurde. Daher kann bei dieser Art der Anmeldung bei einem OpenID-Provider ein Missbrauchsversuch entdeckt werden, bevor dieser erfolgreich durchgeführt werden konnte.

5.3 OpenID-Provider

Bei einer Online-Wahl mit OpenID für die Authentifizierung der Wähler wird auch während der Wahl die Verbindung zu den verwendeten OpenID-Providern benötigt. Es muss also soweit als möglich sichergestellt sein, dass die OpenID-Provider während der Wahlphase auch erreichbar sind. Daher sollte die zu erwartende Verfügbarkeit der einzelnen OpenID-Provider bei deren Zulassungsprüfung für die Wahl berücksichtigt werden.

Ein weiteres Entscheidungskriterium ist die Art der Identifizierung der Personen, die ein OpenID-Provider vor der Vergabe einer OpenID durchführt. Die Prüfung reicht von der Angabe eines freien Benutzernamens bis zur persönlichen Überprüfung mit gültigen Ausweisdokumenten. Besonderen Einfluss auf die Entscheidung sollten auch die Authentifizierungsmerkmale haben, die einem Besitzer einer OpenID zur Verwendung derselbigen angeboten werden.

Je nach Wahl sind verschieden hohe Sicherheitsanforderungen nötig, daher kann eine *Whitelist* mit den für die Wahl zugelassenen OpenID-Providern erstellt werden. Folgende Arten der Zulassung sind damit möglich.

Jeder Provider

Es kann jeder OpenID-Provider zugelassen werden, sogar solche, die nur für einen einzigen Benutzer zuständig sind. Dabei wird der Sorgfalt aller Administratoren, die Zugriff auf die Authentifizierungsdienste haben, vertraut. In dieser Variante kann unmöglich jeder Provider überprüft werden. Dabei ist auch nicht sichergestellt, dass die OpenIDs zu realen Personen gehören, da die gemachten Angaben nicht zwingend korrekt sein müssen. Es ist nur sichergestellt, dass die OpenIDs eindeutig sind.

Ausgewählte Provider

Es können nur ausgewählte OpenID-Provider zugelassen werden. Dabei könnte die Auswahl auf diejenigen beschränkt werden, die ihre Mitglieder genauer prüfen. Beispielsweise könnten nur OpenIDs zugelassen werden, deren zugehörige Benutzer von den Providern per Post-Ident-Verfahren bestätigt wurden. Dadurch wird sichergestellt, dass die OpenIDs zu wirklichen Personen gehören.

Ein Provider

Die Auswahl kann auf nur einen OpenID-Provider beschränkt werden. Dieser kann intensiv auf Sorgfalt und Sicherheit geprüft werden. Somit ist sichergestellt, dass nur reale Personen eine OpenID bekommen und diese auch bei jeder Anmeldung entsprechend der Wahlverordnung genau geprüft werden.

Eigener Provider

Falls der Wahlveranstalter schon einen eigenen OpenID-Provider betreibt, kann er selbstverständlich auch diesen oder nur diesen zulassen. In diesem Fall kann er nach seinen Vorgaben die Wahlberechtigten eindeutig identifizieren, bevor er ihre OpenID für das Wählerverzeichnis freigibt.

Wahleigener Provider

Es ist auch denkbar, dass ein OpenID-Provider nur für die Wahl aufgesetzt wird. Dabei könnten alle Benutzer nach den Wünschen des Wahlbetreibers ausreichend identifiziert werden und erhalten erst danach einen Zugang. Nach der Wahl kann dieser Dienst wieder eingestellt werden, oder für die nächste Wahl gehalten werden.

Durch die Einschränkung auf wenige bis einen OpenID-Provider kann ein Gewinn an Sicherheit erreicht werden, aber die Flexibilität leidet. Es gilt einen Kompromiss entsprechend den jeweiligen Wahlanforderungen zwischen der nötigen Funktionssicherheit, dem Vertrauen in den ordnungsgemäßen Umgang mit den Benutzerdaten und den Wahlrechtsgrundsätzen zu finden.

6 Sicherheitsbetrachtung

Neben der funktionalen Korrektheit der verwendeten Systeme ist deren Sicherheit von entscheidender Bedeutung. Für die allgemeine Einteilung können die folgenden *Schutzziele* verwendet werden. Diese sind abhängig von der zu schützenden Anwendung beziehungsweise den Funktionen des zu schützenden Systems. In der Regel wird eine Kombination mehrerer *Schutzziele* gefordert, bei einem Online-Wahlsystem werden jedoch alle folgend genannten *Schutzziele* [Eck05] gefordert.

Datenintegrität: Keine Daten eines Online-Wahlsystems dürfen unautorisiert geändert werden.

Informationsvertraulichkeit: Es darf keine unautorisierte Informationsgewinnung möglich sein.

Verfügbarkeit: Ein Online-Wahlsystem muss den Wahlberechtigten zu jeder Zeit zur Verfügung stehen.

Verbindlichkeit: Bestimmte Aktionen, wie das Abgeben einer Stimme, müssen verbindlich erfolgen, so dass ein Akteur im Nachhinein die Durchführung einer solchen Aktion nicht abstreiten kann.

Authentizität: Die Echtheit und Glaubwürdigkeit der Teilnehmer, Dienste und Systeme muss anhand von eindeutigen Identitäten und charakteristischen Eigenschaften überprüfbar sein.

Anonymisierung und Pseudonymisierung: Die Verbindung zwischen dem Wähler und seinem Stimmzettel darf nicht für Dritte erkennbar sein.

Die *Schutzziele* werden von den nachfolgend beschriebenen Schwachstellen und Bedrohungen potentiell gefährdet. Daher gilt es, diese Gefahren soweit wie möglich zu vermeiden oder gering zu halten.

6.1 Sicherheit bei Online-Wahlsystemen

Entsprechend den Anforderungen an ein Online-Wahlsystem aus Abschnitt 2.2 muss ein Wahlsystem sicher sein sowie robust und hochverfügbar arbeiten, um jederzeit verwendbar zu sein. Hierzu zählen neben den Servern und Diensten des Online-Wahlsystems auch die Systeme bei den Wahlberechtigten. Folgend werden die potentiellen Bedrohungen für die Sicherheit eines Online-Wahlsystems beschrieben. Hierbei liegt der Fokus auf den für alle Online-Wahlsysteme existierenden Gefährdungen und es wird zwischen den server- und clientseitigen Komponenten unterschieden. Die Bedrohungen gelten ebenso für die OpenID-Provider und die zusätzlichen speziellen Bedrohungen bei OpenID-Providern werden in Abschnitt 6.2 beschrieben.

6.1.1 Sicherheitslücken

Komplexe Systeme sind oft nicht frei von Fehlern. Dadurch entstehende Sicherheitslücken können von Angreifern mit Exploits ausgenutzt werden. Rund die Hälfte der in den Jahren 2007 und 2008 analysierten neuen Schwachstellen eignen sich dazu Benutzer- oder Administratorrechte zu erlangen. Über drei Viertel der im Jahr 2008 neu entdeckten Schwachstellen können von einem entfernten Angreifer ausgenutzt werden. [Sec08] Derartige Schwachstellen müssen bei allen verwendeten Systemen inklusive der Clients beim Wähler ausgeräumt werden.

Da Schwachstellen von den Anwendern nicht verhindert werden können, bleibt nur die Möglichkeit, bekannte Lücken mit Updates schnellstmöglich zu schließen. In den letzten Jahren ist offenbar das Sicherheitsbewußtsein bei den Nutzern gestiegen, so dass viele regelmäßig wichtige Betriebssystem-Updates durchführen. Auf Seiten der Angreifer führt dies zur verstärkten Ausnutzung von Schwachstellen in weit verbreiteter Anwendungssoftware, da diese oft keine kurzfristigen Updates zur Verfügung stellen. Zusätzlich besitzt die Anwendungssoftware oft keine automatischen Update-Mechanismen, so dass eine manuelle Installation erforderlich ist. Leider sind einige Nutzer mit solchen manuellen Updates überfordert oder sie sind sich der Notwendigkeit nicht bewusst. [Bun09]

Sogenannte *Drive-by-Downloads* stellen eine zunehmende Gefahr dar. Dabei handelt es sich um Schadcode, der unbemerkt beim Opfer eingeschleust wird. Für die Verteilung werden vermehrt auch seriöse Webseiten manipuliert oder Sicherheitslücken im Webbrowser oder dessen Plug-Ins verwendet.

Bei einer Online-Wahl können Sicherheitslücken zu großen Problemen führen, daher müssen diese mit allen zur Verfügung stehenden Mitteln verhindert werden. Die Software des Online-Wahlsystems sollte daher unabhängig von den Entwicklern geprüft werden. Dazu sollten Experten das fertige Softwareprodukt und zusätzlich

dessen Quellcode auf Funktionssicherheit, Schwachstellen und Fehler untersuchen. Im Idealfall sollte jeder Interessierte gleich den Experten das Online-Wahlsystem analysieren dürfen, das kann allerdings in der Praxis aus betriebswirtschaftlicher Sicht zu Problemen führen. Da von einem Wahlberechtigten nicht das technische Wissen und die benötigte Zeit für solch eine komplexe und aufwändige Analyse gefordert werden kann, sollte die Experten-Prüfung von einer für die Wahlberechtigten vertrauenswürdigen Organisation durchgeführt werden. Eine Zertifizierung beispielsweise nach *Common Criteria* [CC] lässt erkennen, in welcher Weise und von welchen Experten das Wahlsystem geprüft wurde.

Neben der Online-Wahl können auch Sicherheitslücken in der Software der Betriebssysteme vorhanden sein. Um dieses Risiko zu minimieren, sollten zertifizierte Betriebssysteme in der aktuellsten Version verwendet werden. Empfohlen ist dabei auch (falls möglich) der ausschließliche Einsatz von zertifizierter Hardware.

Mit diesen Mitteln kann die Bedrohung durch Sicherheitslücken auf der Serverseite niedrig gehalten werden. Leider ist die clientseitige Absicherung erheblich schwerer. Dort ist nicht sichergestellt, dass nur vertrauenswürdige Komponenten zum Einsatz kommen. Das gestiegene Sicherheitsempfinden der Anwender führt zur verstärkten Nutzung von Schutzmechanismen wie Firewalls und Antivirensoftware. Auch die für eine Online-Wahl hauptsächlich benötigten Programme wie Betriebssystem und Web-Browser werden auf Grund von einfach bedienbaren Updatefunktionen regelmäßig aktualisiert. Trotzdem sollten die vielfältigen Bedrohungen für die Clientseite nicht unterschätzt werden.

6.1.2 Schadprogramme

Zu den Schadprogrammen gehören Viren, Würmer, Trojanische Pferde und Bots, wobei eine klassische Einteilung in diese Kategorien kaum noch möglich ist. Viele Programme sind modular aufgebaut und übernehmen Aufgaben aus verschiedenen Kategorien. So gibt es beispielsweise Trojanische Pferde, die auch für Bot-Netze genutzt werden können.

Die Anzahl der Schadprogramme nimmt ständig zu und deren Aufbau wird komplexer. Viele Schadprogramme besitzen eine Update-Funktion, um selbstständig neuen Schadcode oder neue Tarnmechanismen nachzuladen. Die leichte Erweiterbarkeit solcher Programme erlaubt eine einfache Anpassung für bestimmte Zwecke. Es existieren sogar Programme, die nach dem Baukastenprinzip die Erstellung eigener Schadprogramme für Nicht-Profis ermöglichen.

Trotz der Vielzahl an Schadprogrammen ist deren Verteilung gezielter geworden. Die Wahrscheinlichkeit, mit der eine solche vom Opfer ungewollte Software entdeckt wird, hängt unter anderem von deren Verbreitung ab. Bleibt sie länger unentdeckt, wird

sie erst später in die Erkennungssignaturen von Schutzprogrammen aufgenommen und kann somit länger erfolgreich eingesetzt werden. Für die Verteilung wurden vor wenigen Jahren noch verstärkt E-Mails versendet, heutzutage werden dazu häufig *Drive-by-Downloads* verwendet.

Die finanziellen Absichten, insbesondere der Autoren von Trojanischen Pferden und Bots, führt zu einer schnellen Entwicklung der Mechanismen gegen die Erkennung und Analyse des Schadcodes. Dazu werden kryptographische Verfahren verwendet und die Schadprogramme so erweitert, dass sie erkennen ob sie in einer typischen Testumgebung oder auf einem echten Opferrechner ausgeführt werden und ihr Verhalten dementsprechend anpassen können.

Zur Bekämpfung der Schadprogramme werden hauptsächlich signaturbasierende Schutzprogramme eingesetzt. Diese können aber nur schon bekannten Schadcode abwehren und benötigen eine häufige Aktualisierung der Signaturdatenbanken. Der Einsatz von Schutzprogrammen, die das Verhalten von Software untersuchen, führt oftmals zu unberechtigten Alarmen (*false positives*), die den ordnungsgemäßen Betrieb behindern. Dies kann soweit führen, dass eigentlich harmlose Teile eines Betriebssystems deaktiviert oder sogar gelöscht werden. Daher ist der Einsatz von verhaltensbasierter Erkennungssoftware umstritten. Sollte die Qualität der Schutzprogramme zu einer Gefahr der Schadprogramme werden, dann ist mit einer neuen Generation von Schadprogrammen zu rechnen. Diese könnten beispielsweise das eigentliche Betriebssystem in eine virtuelle Umgebung verschieben und so unbemerkt von herkömmlichen Schutzprogrammen zwischen der Hardware und dem Betriebssystem agieren.

Trojanische Pferde

Trojanische Pferde werden vorwiegend eingesetzt, um Zugangsdaten zu stehlen oder ein Opfer gezielt auszuspionieren. Sie installieren sich heimlich und ermöglichen dem Angreifer die Kontrolle über einzelne Rechner. Besonders bei gezielter Spionage wird diese Form der Schadprogramme eingesetzt. Dabei werden nicht wie früher hauptsächlich die zentralen Server einer Behörde, sondern ausgewählte Arbeitsplatzrechner angegriffen. Dort ist die unbemerkte Installation leichter durchzuführen und diese bieten eine gute Basis für weitere gezielte Angriffe.

Zum Einschleusen des Schadcodes könnten die unter dem Begriff *Social Engineering* bekannten Methoden genutzt werden. Beispielsweise kann das Opfer durch geschicktes Einwirken dazu gebracht werden, einen manipulierten E-Mail-Anhang zu öffnen oder einen präparierten USB-Stick anzuschließen. In einem solchen Fall kann Schadsoftware nebenbei und unbemerkt auf den Zielrechner gelangen, ohne dass das Opfer dies bemerkt.

Spyware

Das Ziel von Spyware-Programmen ist die Erfassung des Surfverhaltens des Opfers. Die gesammelten Daten können für zielgerichtete Werbung genutzt werden. Da einige dieser Programme nicht nur das Surfverhalten sondern auch die Anmeldedaten wie Benutzername und Passwort an den Angreifer melden, ist Spyware nicht als harmlos zu betrachten. Allerdings wird aus juristischer Sicht Spyware als „möglicherweise unerwünschte Software“ und nicht als Schadprogramm bezeichnet. Ähnlich wie Tronjanische Pferde werden Spyware-Programme häufig über manipulierte Webseiten oder Bot-Netze verteilt. In den letzten Jahren ist die Bedrohung durch Spyware weiter gestiegen, was hauptsächlich in der schweren Unterscheidbarkeit zwischen Spyware-Programmen und Trojanischen Pferden begründet ist.

Ähnlich wie bei Sicherheitslücken ist das Aufkommen von Schadprogrammen bei Online-Wahlsystemen auf den Servern leichter zu verhindern. Auf den Servern sollte einzig die für die Online-Wahl benötigte Software vorhanden sein. Da hier die Nachinstallation von Software oder auch nur der Download von Programmen verhindert werden kann, ist das Sicherheitsrisiko erheblich geringer als auf der Clientseite. Der Wahlberechtigte nutzt seinen Rechner für vielerlei Aufgaben und nicht ausschließlich für eine Online-Wahl. Daher ist es nicht ungewöhnlich, dass dort zusätzliche Software installiert wird. Einige Programme bestätigen ihre Integrität mit Hilfe von kryptographischen Verfahren, doch ein alleiniger Einsatz von verifizierter Software kann nicht vorausgesetzt werden. Eine unbedachte Handlung kann zur Installation von Schadprogrammen führen.

Die in den Anforderungen an eine Online-Wahl vorausgesetzte Geheimhaltung ist durch mögliche Trojanische Pferde und Spyware stark gefährdet. Somit ist ein sorgsamer auch technisch gestützter Umgang mit zusätzlichen Programmen nötig.

6.1.3 Denial of Service (DoS)

Mit einem Denial-of-Service-Angriff wird bewusst versucht, die Verfügbarkeit eines IT-Systems zu stören. Eine solche Attacke richtet sich entweder gegen das System, welches die betreffenden Dienste anbietet, oder gegen die Dienste selber. Ein direkter Angriff auf das System kann beispielsweise bei physikalischem Zugriff auf den Rechner erfolgen. Sollte das Zielsystem Sicherheitslücken aufweisen, kann auch dadurch ein DoS-Angriff stattfinden. Wenn der Rechner nicht mehr erreichbar ist, dann sind folglich auch die auf ihm laufenden Dienste nicht mehr verwendbar.

Eine andere Variante ist der Angriff durch Überlast. Dabei wird entweder das Zielsystem selbst oder der angebotene Dienst mit so vielen Anfragen wie möglich beschäftigt.

Die Anfragen sind meist unsinnig, verursachen aber eine Reaktion bei den attackierten Systemen bzw. Diensten. Durch die Masse an Anfragen kann die Verfügbarkeit des Dienstes derart beeinträchtigt werden, dass er seine normalen Aufgaben nicht mehr erledigen kann. Um einen solchen DoS-Angriff erfolgreich durchführen zu können, benötigt der Angreifer einen leistungsstarken Rechner und eine sehr schnelle Netzanbindung. Alternativ kann eine solche Attacke auch von mehreren Maschinen gleichzeitig ausgeführt werden. Dabei benötigen die einzelnen Rechner entsprechend der Anzahl eingesetzter Maschinen weniger Ressourcen. Solch eine verteilte Attacke wird als Distributed-Denial-of-Service-Angriff bezeichnet. [Hag03]

Distributed Denial of Service (dDoS)

Bei dieser verteilten Form des DoS-Angriffs werden viele mit dem Internet verbundene Maschinen benötigt. Wenn ein Angreifer die nötige Anzahl von Rechnern zur Verfügung hat, kann er mit allen gleichzeitig auf das Zielsystem bzw. die Zieldienste einwirken. Mit einer hohen Anzahl von Angriffssystemen kann er eine Überlast beim Opfer erreichen, so dass dieses seine Dienste nicht mehr zufriedenstellend anbieten kann. Hierbei werden oft ans Internet angeschlossene Rechner mit Sicherheitslücken verwendet. Der Angreifer attackiert (oft unbemerkt) verschiedene Maschinen und installiert dort seine Angriffswerkzeuge, um diese als Ausgangspunkte für seinen dDoS-Angriff nutzen zu können.

Für einen reibungslosen Ablauf der Wahl dürfen die für die Wahl benötigten Maschinen und Dienste nicht gestoppt werden. Die physikalischen Zugriffe müssen daher streng überwacht werden. Wenn ein Angreifer benötigte Komponenten erreichen kann, dann ist es ihm möglich die Wahl zu unterbrechen, gegebenenfalls sogar dauerhaft zu stoppen. Um dieses Ziel zu erreichen, würde ein physikalischer Zugriff auf die Strom- oder Netzwerkanbindung genügen. Sollte ein Angreifer sogar die Rechner mit den Diensten für die Online-Wahl erreichen, dann könnte er unter Umständen die Wahldaten kompromittieren oder vernichten.

Da ein physikalischer Zugriff verheerende Auswirkungen auf die Online-Wahl haben kann, muss dieser streng kontrolliert werden. Dazu empfiehlt es sich, alle nötigen Server in ein Hochsicherheitsrechenzentrum mit den entsprechenden Zugangskontrollen und überwachten Anbindungen für den Server zu stellen.

Weitergehend wird auch eine Verteidigung gegen DoS- und dDoS-Attacken über die Netzwerkanbindung benötigt. Mit Hilfe von speziell konfigurierten Firewalls kann ein erfolgreicher DoS-Angriff auf die Wahlserver verhindert werden. Dazu kann beispielsweise die Anzahl der zugelassenen Anfragen von einer IP-Adresse in einem festen Zeitraum limitiert werden. Wenn diese Grenze überschritten wird, dann

wird diesem möglichen Angreifer immer weniger Bandbreite zur Verfügung gestellt. Dieses Vorgehen hilft aber im Allgemeinen nicht gegen verteilte Angriffe. Bei einem dDoS-Angriff werden viele verschiedene Rechner mit unterschiedlichen IP-Adressen verwendet. Daher würde die eben beschriebene Vorgehensweise nur gegen mehrfache Attacken helfen, doch nicht bei der ersten Angriffswelle. Eine Möglichkeit sich gegen diese Bedrohung zu schützen hängt mit den Eigenarten eines Wahlsystems zusammen. Da bei einer Online-Wahl die Anzahl der nötigen Verbindungen von einem Client für einen ordnungsgemäßen Wahlvorgang überschaubar sind, kann man hierbei eine spezielle Firewallkonfiguration für den Serverschutz verwenden.

Gezielten Überlastungsversuchen der Firewall kann allerdings nur mit ausreichenden Ressourcen begegnet werden. Daher wird für eine Senkung der Wahrscheinlichkeit eines erfolgreichen DoS- oder dDoS-Angriffs deutlich mehr Rechnerleistung und Netzwerkbandbreite benötigt als für eine normale Wahl gebraucht würde.

Den Schutz der Clients muss der Wahlberechtigte übernehmen, doch eine Störung einer Online-Wahl mit Angriffen auf die Clients ist für einen Angreifer wesentlich schwerer. Zuerst müsste ein Angreifer die IP-Adressen der Wähler zum Zeitpunkt ihres Wahlvorgangs wissen. Dies gestaltet sich bei dynamisch verteilten IP-Adressen und langen Wahlzeiträumen als schwierig. Sollte ein Angreifer diese Hürde dennoch überwinden, bräuchte er sehr viele Angriffssysteme, um signifikante Störungen durch Überlast zu verursachen. Mit Hilfe von beim Wahlberechtigten installierter Schadsoftware wäre eine erfolgreiche Unterdrückung des Wahlvorgangs möglich, was jedoch einen vorherigen Angriff voraussetzt.

6.1.4 Innentäter

Neben den Bedrohungen von außen gibt es auch interne Gefahren. Sogenannte Innentäter besitzen oft ein detailliertes Wissen über die eingesetzten Systeme. Sie besitzen oft Zugänge zu vertraulichen Informationen und können diese unbemerkt mit Hilfe moderner Kommunikationsmittel aus dem Unternehmen schleusen. Einen gezielten Informationsdiebstahl kann man mit Firewalls und Antivirensoftware nicht verhindern. Mit 24 Prozent sind die Innentäter die größte Tätergruppe [Cor07]. Unabhängig vom Informationsdiebstahl können Innentäter auch bewusst mit gezielten Angriffen den Betriebsablauf einer Firma stören. Die Täter können von Motiven der Rache oder finanziellen Anreizen getrieben sein.

Die Gefahr der Innentäter ist bei einer Online-Wahl auf Wählerseite eher gering. Dort könnte nur eine Person aus dem näheren Umfeld der Wahlberechtigten eine Gefahr darstellen. Wenn der Wahlvorgang von einem privaten Rechner im heimischen Umfeld durchgeführt wird, ist die Anzahl der möglichen Innentäter überschaubar und bei einem Angriff der Schuldige leicht zu finden.

Eine erheblich höhere Gefahr geht von den Zugriffsberechtigten bei den Wahlkomponenten aus. So muss verhindert werden, dass Zugangsdaten für die Wahlberechtigten oder Wahlsysteme an Fremde weitergegeben werden. Weiterhin muss sichergestellt werden, dass mögliche Änderungen am Programm-Code oder der Wahlsystemkonfiguration auffallen und keine Spionagesysteme hinzugefügt werden können.

Die mit den für eine Online-Wahl benötigten Maschinen, Programmen und Daten vertrauten Personen müssen sorgfältig ausgewählt werden. In die Betrachtung sind auch alle externen Personen, die beispielsweise im Rechenzentrum arbeiten, mit einzubeziehen. Aufgrund der erforderlichen Sicherheit bei einer Online-Wahl dürfen nur vertrauenswürdige Personen an den Wahlprozessen beteiligt sein.

6.1.5 Irrtum & Nachlässigkeit

Die Sicherheit wird maßgeblich von der Qualität der Wartung beeinflusst. Nur wenn alle eingesetzte Hard- und Software regelmäßig von fachkundigen Betreuern aktualisiert, geprüft und bei Bedarf verbessert wird, ist ein sicherer Betrieb möglich. Irrtümer und Nachlässigkeiten stellen ein erhebliches Risiko dar und müssen vermieden werden.

Um den ordnungsgemäßen Ablauf einer Online-Wahl sicherstellen zu können, sollten die verwendeten Bestandteile möglichst einfach zu bedienen sein. Dies gilt für die Konfiguration des Wahlsystems genauso wie für den Wahlvorgang selbst. Durch klare strukturierte Prozesse können Irrtümer vermieden werden. Dabei können technische Vorrichtungen den richtigen Umgang begleiten und im Fehlerfall den Benutzer alarmieren. Hierzu eignen sich klare Anweisungen und Vorgehensweisen für die Installation, Konfiguration und Inbetriebnahme des Wahlsystems. Folglich sollte auch der Wahlvorgang und der Stimmzettel für den Wähler zweifelsfrei sein.

Um Nachlässigkeit zu verhindern, sollten nur fachkundige Personen mit den entsprechenden Aufgaben betraut werden, die sich der Verantwortung ihres Handelns bewusst sind. Auch hier helfen klare Abläufe, um Fehler zu vermeiden. Soweit es möglich ist, können auch technische Vorkehrungen unterstützend eingesetzt werden. Beispielsweise sollte ein Online-Wahlsystem einen *Übereilungsschutz* bei der Stimmabgabe haben, damit der Wähler nicht vorschnell den falschen Kandidaten wählt.

6.2 Sicherheit bei OpenID

Bei einem Online-Wahlsystem mit OpenID wirkt sich die Verfügbarkeit und Funktionssicherheit der OpenID-Provider auf das gesamte Wahlsystem aus. Daher darf

auch deren Schutz nicht unterschätzt werden. Neben den allgemeinen Gefährdungen gibt es auch spezielle für OpenID, die folgend geschildert werden.

Wie in Abschnitt 5.3 beschrieben, kann die Anzahl der zugelassenen OpenID-Provider beschränkt werden. Das vorgestellte Online-Wahlsystem ermöglicht eine *Whitelist* für OpenID-Provider.

6.2.1 Datenschutz

Besonders wichtig ist die Auswahl des OpenID-Providers. Neben der Verfügbarkeit und Funktionssicherheit ist auch der Umgang mit den Benutzerdaten ein wichtiges Auswahlkriterium. Der OpenID-Provider sollte sich an geltende Datenschutzbestimmungen halten und mit den Benutzerinformationen sensibel umgehen. Dabei sollte beachtet werden, dass die OpenID-Provider ihre Server auch in Ländern mit schwachen oder fehlenden Datenschutzanforderungen betreiben können.

Jeder OpenID-Identifier kann prinzipiell als eine eigene Online-Identität benutzt werden, somit ist es möglich, die Identität durch gezielte Verwendung zu beeinflussen. Wenn beispielsweise jemand einen Identifier für Einträge in Blogs und Foren zum Thema Angeln verwendet, dann ist es Dritten möglich Verbindungen zwischen diesen Einträgen zu ziehen. Da jeder OpenID-Identifier nur an eine Person gebunden ist, entsteht eine Identität, die sich mit dem Angeln beschäftigt. Sollte der selbe Mensch eine anderen OpenID-Identifier für Einträge zum Thema Segeln verwenden, dann ist es Dritten ohne weitere Informationen nicht möglich zu erkennen, dass beide Online-Identitäten derselben Person gehören. Aus diesem Grund ist es möglich, sich mehrere Online-Identitäten zu schaffen, um beispielsweise private von beruflichen Verhaltensweisen zu trennen. Damit kann das Benutzerverhalten beim Verwenden von OpenIDs ähnlich dem Umgang mit E-Mail-Adressen motiviert sein.

Durch das benutzerzentralisierte Identitätsmanagement von OpenID kann der Besitzer situationsabhängig die Nutzung seiner Online-Identitäten steuern. Es wird empfohlen für eine Wahl einen OpenID-Identifier zu verwenden, der keine ungewollten Rückschlüsse auf die Person ermöglicht. Viele OpenID-Provider erlauben das Binden mehrerer OpenID-Identifier an ein Benutzerkonto. Bei einem solchen Provider ist es leicht möglich, sich einen neuen Identifier für eine Online-Wahl zu erstellen. Allerdings ist es dem Provider möglich, die Verbindung zwischen den verschiedenen OpenID-Identifiern eines Benutzerkontos zu erkennen.

Für die Teilnahme an Online-Wahlen ist es deshalb besser ein neues OpenID-Benutzerkonto mit nur einem OpenID-Identifier zu erstellen. Bei einer Online-Wahl sollten nur sichere und vertrauenswürdige Systeme und Dienstleister eingesetzt werden, daher sollte man bei OpenID-Providern nicht anders verfahren.

Wenn der Wahlveranstalter seinen Wahlberechtigten nicht die volle Verantwortung bei der Auswahl geeigneter OpenID-Provider überlassen will, dann kann er die für seine Online-Wahl zugelassenen einschränken. Da bei der Erfassung der OpenIDs als Wählerkennung alle OpenIDs geprüft werden, wird vor dem Wahlbeginn automatisch ausgeschlossen, dass ein Wahlberechtigter einen nichtzugelassen OpenID-Provider bei der Wahl verwendet.

6.2.2 Phishing

Der Begriff Phishing bezeichnet den Versuch mittels gefälschter Webseiten an die Daten eines Benutzers zu gelangen. Phishing ist ein weit verbreitetes Phänomen bei Online-Banken, Kreditkartenunternehmen und anderen zugangsgeschützten Diensten. Bei Identitätsprovidern erhöht sich die Schadenswirkung bei einem erfolgreichen Angriff, da der Identitätsdieb Zugang zu allen vom Besitzer dauerhaft erlaubten Diensten hätte. Weiterhin könnte der Dieb sich als rechtmäßiger Besitzer ausgeben und diesem empfindliche Schäden zufügen.

In Verbindung mit einer Online-Wahl könnte der Dieb sogar unrechtmäßig die Stimme des Wahlberechtigten übernehmen, falls dieser noch nicht gewählt hat und keine weiteren Authentifizierungsmerkmale neben der OpenID verwendet werden. Daher ist ein Schutz vor Phishing-Angriffen sehr wichtig.

Da die Gefahr bekannt ist, kann ihr mit verschiedenen Mechanismen begegnet werden. Der Benutzer kann für die Anmeldung beim OpenID-Provider ein Browser-Zertifikat verwenden. Danach ist es fast unmöglich, dem Benutzer ohne Warnmeldung eine gefälschte Providerseite unterzuschieben. Solche Browser-Zertifikate sind von vielen Anbietern kostenlos erhältlich und werden sogar teilweise von OpenID-Providern direkt angeboten. Eine weitere Schutzmaßnahme ist die Multi-Faktor-Authentifizierung. Dabei werden mehrere sichere Mechanismen wie Cardspace, Smartcards, biometrische Verfahren (Fingerabdruck, Iris-Scan, Stimmerkennung, Handflächenvenenmuster etc.) zur Anmeldung hinzugenommen (siehe Abschnitt 5.2).

6.2.3 Profiling

Jedes System, das einen Benutzer mittels OpenID authentifizieren will, benötigt die Zustimmung des OpenID-Besitzers. Dieser kann wie in Abschnitt 3.4 beschrieben die Freigabe verweigern, einmalig gestatten oder dauerhaft erlauben. Dies ist einerseits ein großer Vorteil für die Transparenz bei der Verwendung der OpenID, aber andererseits kennt jeder OpenID-Provider alle Systeme und Zeitpunkte, bei denen die OpenID verwendet wurde. Dadurch ist ein OpenID-Provider in der Lage ein Nutzungsprofil für seine Benutzerkonten zu erstellen. Er kann somit nicht nur die beschriebene

Online-Identität erkennen, sondern auch den Benutzer durch das Nutzungsverhalten noch ein bisschen gläserner machen. Deshalb sollte sich jeder vor der Registrierung über den Umgang des Providers mit Benutzerinformationen informieren.

Bis jetzt gibt es keine technische Lösung, die das mögliche Anlegen eines Nutzerprofils verhindert, doch würde ein OpenID-Provider beim Profiling ertappt, dann würde er schlagartig seine Kunden verlieren. Daher gibt es neben den in vielen Ländern geltenden rechtlichen Bestimmungen auch einen moralischen Schutz vor dem Profiling des OpenID-Providers.

Das Streuen verschiedener OpenIDs, welche zu verschiedenen Providern gehören, verhindert die Anhäufung von Nutzerprofilen.

Die Möglichkeit des Profilings ist auch E-Mail-Providern oder Internet-Service-Providern in anderer Form möglich.

Der potenziellen Gefahr kann nur durch die Verwendung von mehreren OpenID-Providern begegnet werden. Dabei werden die für das Profiling interessanten Informationen auf mehrere unabhängige Dienste verteilt.

6.3 Folgerung

Ein Online-Wahlsystem, das die in Abschnitt 2.2 beschriebenen Anforderungen an Wahlen und die in diesem Kapitel beschriebenen *Schutzziele* erfüllt, muss an einem speziell gesichertem Ort betrieben werden. Es muss sichergestellt sein, dass keine Unberechtigten physikalischen Zugriff auf die für das Wahlsystem wichtigen Bestandteile erhalten können. Dies beinhaltet auch die Stromversorgung und Netzwerkverbindung. Gleichzeitig muss der bestmögliche Schutz gegen physikalische Störungen des Systems ohne menschlichen Einfluss, wie beispielsweise einem Hardware-Ausfall, erbracht werden. Daher sollten die Server des Systems entsprechende Redundanz besitzen und sich in speziell gesicherten Rechenzentren befinden.

Die Betreuung des Wahlsystems darf nur von vertrauenswürdigen und kompetenten Personen mit entsprechendem Hintergrundwissen und Sorgfalt übernommen werden. Sie müssen den nötigen Schutz der Software mit speziellen Programmen gegen Schadprogramme und Angriffe aufrechterhalten. Neben einer sauberen Dokumentation des normalen Betriebes müssen Notfallpläne für die unterschiedlichen möglichen Probleme existieren, so dass im Ernstfall ein schnelles und korrektes Vorgehen möglich ist.

Die Software des Online-Wahlsystems muss korrekt, sicher und zuverlässig arbeiten. Dieses kann durch eine Überprüfung von Experten sichergestellt werden. Eine Zertifizierung, die auch den Außenstehenden bekannt ist, erhöht dabei das Vertrauen der Wahlberechtigten gegenüber dem Wahlsystem.

Für die zur Wahl zugelassenen OpenID-Provider gelten prinzipiell dieselben Auflagen wie für das Online-Wahlsystem. Zusätzlich stehen die möglichen Arten der Authentifizierung und Identifizierung im Vordergrund. Eine detaillierte Beschreibung enthält Kapitel 5.

Dieselben Auflagen sind unmöglich von den Wahlberechtigten zu fordern, jedoch sollten auch sie ihre Hard- und Software sorgfältig auswählen. Die Rechner der Wahlberechtigten sollten frei von Schadsoftware sein und aktuelle Versionen ihres Betriebssystems enthalten. Zusätzlich sollten eine Anti-Virensoftware und eine Firewall zum Schutz vorhanden sein.

In den letzten Jahren ist das Sicherheitsbewusstsein der Privatanwender stark gestiegen, so dass die meisten Systeme der Wahlberechtigten diesen Anforderungen ohnehin entsprechen. Nicht zuletzt durch die Verbreitung von *Home-Banking* haben die Anwender ein gestärktes Interesse an einer sicheren Umgebung mit Online-Zugang. Da die Auswahl eines OpenID-Providers der Auswahl eines E-Mail-Providers in vielen Punkten gleicht, ist auch dies keine große Hürde für einen Wahlberechtigten. Die Verbreitung von OpenID nimmt stark zu, so dass einige Wahlberechtigte diese Technologie vielleicht schon nutzen.

7 Zusätzlich einsetzbare Authentifizierungsmerkmale

Bei einer Wahl mit OpenID muss dem OpenID-Provider starkes Vertrauen bezüglich der Authentifizierung der Wahlberechtigten entgegengebracht werden. Der Wahlveranstalter kann daher, wie in Abschnitt 5.3 beschrieben, nur bestimmte OpenID-Provider zulassen. Falls er sich nicht alleine auf die sorgfältige und korrekte Arbeitsweise der zugelassenen OpenID-Provider verlassen will, kann er ein zusätzliches Wählerpasswort für den Wahlvorgang fordern. Dadurch entsteht neben der möglichen Multi-Faktor-Authentifizierung beim OpenID-Provider ein weiterer unabhängiger Faktor für die Authentifizierung beim Wahlvorgang. Der Wähler muss sich in diesem Fall an zwei unterschiedlichen Stellen mit jeweils eigenen Authentifizierungsmerkmalen ausweisen.

Jedoch entsteht bei der Verwendung von Wählerpasswörtern ein schon bekanntes Verteilungsproblem. Im Gegensatz zur herkömmlichen Verteilungsvariante der bei der Erstellung des Wählerverzeichnisses generierten Passwörter sind dem Wählerverzeichnis nicht die Namen der Wahlberechtigten sondern nur deren OpenID-Identifier bekannt. Würde das Wählerverzeichnis mehr als die OpenID-Identifier von den Wahlberechtigten kennen, würden viele Vorteile der vorgestellten Lösung verloren gehen. Im Folgenden wird eine Verteilungsmethode beschrieben, bei der die Kontaktdaten einzig dem Verteilungsdienst bekannt sind.

Neben der Authentifizierung beim OpenID-Provider spielt auch die Zugehörigkeit des OpenID-Identifiers zum Wahlberechtigten eine entscheidende Rolle. Diese Verbindung wird automatisch bei der Registrierung der OpenID-Identifier geprüft. Bei einer maschinell gestützten Prüfung kann ein weiteres Sicherheitsmerkmal verwendet werden. Dieses *VerifyTAN* genannte Merkmal kann ebenfalls über einen weiteren unabhängigen Kanal verbreitet werden, so dass auch die Zugehörigkeitsprüfung bei der Registrierung verbessert werden kann. Im letzten Abschnitt dieses Kapitels wird dieses Merkmal und deren Verwendung beschrieben.

7.1 Optionales Wählerpasswort

Das Sicherheitsniveau der Wählerauthentifizierung kann durch ein zusätzliches Geheimnis in Form eines Wählerpassworts gesteigert werden. Jeder Wahlberechtigte erhält in diesem Anwendungsfall vor dem Start der Wahldurchführungsphase ein Wählerpasswort. Diese Passwörter sind eindeutig, werden nicht mehrfach vergeben und werden, fest verbunden mit der Wählerkennung, ins Wählerverzeichnis eingetragen. Bei der Wahl authentifiziert sich der Wähler erst bei seinem angegebenen OpenID-Provider und danach beim Wählerverzeichnis mit seinem Wählerpasswort. Somit wird die Authentifizierung der Wahl um einen weiteren Faktor erweitert, so dass unabhängig vom Provider eine Multi-Faktor-Authentifizierung stattfindet. Da das Wählerpasswort über einen anderen Kanal verteilt wird, ist es für Angreifer deutlich schwieriger an alle nötigen Zugangsdaten für die Wahl zu gelangen.

Der Nachteil bei diesem Ansatz ist die zusätzliche Verteilung der Wählerpasswörter. Wenn diese Verteilung nicht über einen sicheren elektronischen Weg erfolgen kann, dann entstehen weitere Kosten.

7.2 Verteilung der optionalen Wählerpasswörter

Soll neben der Wählerkennung auch ein Wählerpasswort zur Wahl verwendet werden, muss dieses während der Wahlvorbereitung an die Wahlberechtigten verteilt werden. Da die Wählerpasswörter vor Dritten geschützt werden müssen, darf die Verteilung nur über sichere Kanäle erfolgen.

Die Generierung der Wählerpasswörter erfolgt automatisch bei der Erstellung des Wählerverzeichnisses. Jeder Wählerkennung wird dabei ein zugehöriges Wählerpasswort zugewiesen, welches nach der Erstellung an den zugehörigen Wahlberechtigten verteilt werden muss. Für diese Verteilung werden die Kontaktdaten von den Wahlberechtigten benötigt, die allerdings bei der Erstellung nicht bekannt sein dürfen. Würden die Kontaktdaten bei diesem Schritt lesbar sein, dann wäre die Verbindung zwischen dem Wahlberechtigten und seinem OpenID-Identifier, der als Wählerkennung dient, dem Wahlsystem bekannt. Daher wird die Verteilung der Wählerpasswörter einem unabhängigen Dienst übergeben, der keine Kenntnis von den Wählerkennnungen hat.

Dem Verteilerdienst werden nur die Kontaktdaten und das zugehörige Wählerpasswort übermittelt. Er erhält keine weiteren Informationen. Seine Aufgabe ist einzig die Verteilung der Wählerpasswörter an die Wahlberechtigten mit Hilfe ihrer Kontaktdaten. Je nach nutzbarer Infrastruktur können die Wählerpasswörter elektronisch, beispielsweise mit verschlüsselten E-Mails, oder papierbasiert mittels PIN-Briefen

versandt werden. Es ist auch möglich, mehrere Verteilerdienste mit unterschiedlichen Verteilungsarten zu verwenden, so dass die Wahlberechtigten, denen ihr Passwort nicht elektronisch übermittelt werden kann, ihres papierbasiert erhalten.

Die für die Verteilung der Wählerpasswörter nötigen Kontaktdaten sind dem Wahlveranstalter bekannt. Sie werden von ihm so verschlüsselt, dass nur der Verteilungsdienst sie entschlüsseln kann. Dafür kann ein asymmetrisches Verschlüsselungsverfahren wie RSA [RSA] [Buc01] [Sch06] verwendet werden. Der Wahlveranstalter verschlüsselt einzeln die Kontaktdaten mit dem öffentlichen Schlüssel des Verteilers, so dass nur der Verteiler die Daten mit seinem privaten Schlüssel entschlüsseln kann. Dritten ist es nicht möglich ohne den geheimen privaten Schlüssel Informationen aus den verschlüsselten Daten zu gewinnen, daher dürfen die verschlüsselten Kontaktdaten bei der Erstellung des Wählerverzeichnisses bekannt sein.

Für die Verteilung der Passwörter ist die Zuordnung zu den richtigen Kontaktdaten entscheidend. Wie in Abbildung 7.1 dargestellt finden mehrere Prozesse zwischen der Ver- und Entschlüsselung der Kontaktdaten statt. Die Informationen der Wahlberechtigten werden jeweils als Tupel weitergegeben und die enthaltenen Daten sind dabei so verschlüsselt, dass nur der Dienst, der sie benötigt, sie entschlüsseln kann. Es entsteht eine Informationskette vom Wahlveranstalter, der die Namen der Wahlberechtigten und deren Kontaktdaten für die Verteilung kennt, bis zu den Wahlberechtigten, die ihre Wählerpasswörter vom Verteilungsdienst erhalten.

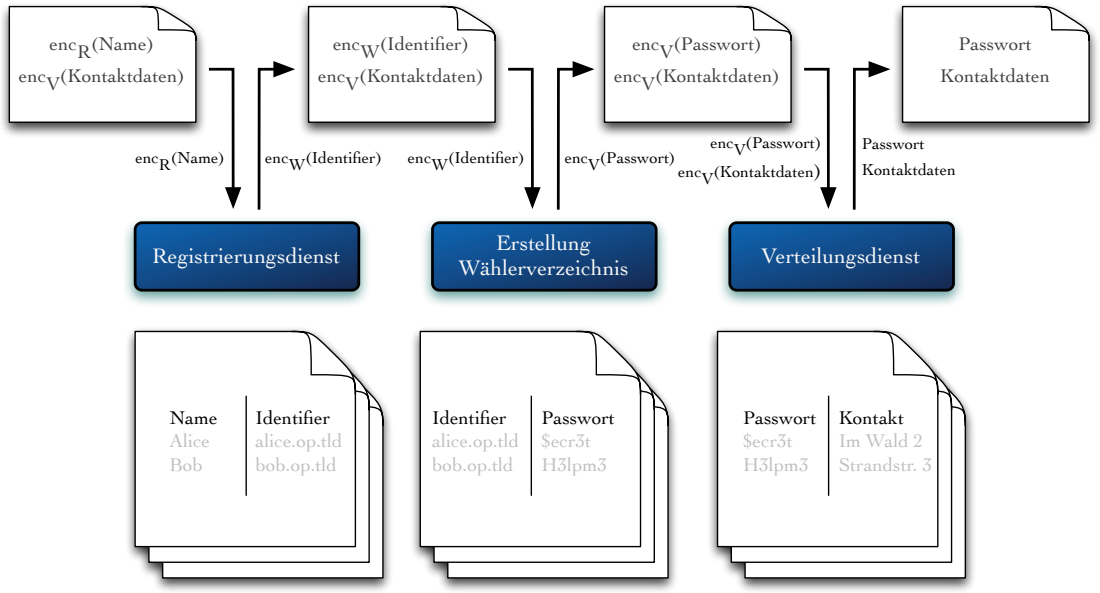

Abbildung 7.1: Informationsfluss des Online-Wahlsystems mit Wählerpasswörtern

Bei der Registrierung der Wählerkennungen werden aus den erhaltenen Datentupeln

die Einträge mit den Namen der Wahlberechtigten entschlüsselt, um sie für die Wahlberechtigungsprüfungen verwenden zu können. Die erfassten OpenID-Identifier werden den Namen zugeordnet und nach dem Ende der Registrierungsphase werden die verschlüsselten Namen in den erhaltenen Datentupeln durch die verschlüsselten Identifier ersetzt und die Datensätze für die Erstellung des Wählerverzeichnisses weitergegeben.

Während der Erstellung des Wählerverzeichnisses werden aus den erhaltenen Datentupeln die Einträge mit den OpenID-Identifiern entschlüsselt und jedem Identifier wird ein Wählerpasswort zugewiesen. Anschließend werden die Wählerpasswörter verschlüsselt und anstelle der verschlüsselten Identifier in die Datentupeln geschrieben. Der neue Datensatz wird an den Verteilungsdienst übergeben.

Der Verteilungsdient entschlüsselt aus den erhaltenen Datentupeln die Wählerpasswörter und Kontaktdaten, so dass er die Wählerpasswörter mittels ihrer Kontaktdaten an die Wahlberechtigten verteilen kann. Da bei jedem Schritt nur gezielt Einträge in den Datentupeln ersetzt werden, ist die Zuordnung zwischen den Wählerpasswörtern und den Kontaktdaten korrekt. Durch die Verschlüsselung der einzelnen Einträge in den Datentupeln, derart, dass nur der entsprechende Dienst diese Einträge entschlüsseln kann, bleibt das *Need-To-Know-Prinzip* erhalten.

7.3 VerifyTAN

Die Zugehörigkeit eines OpenID-Identifiers zu einem Wahlberechtigten wird bei der Registrierung der Wählerkennung geprüft. Diese Aufgabe übernimmt der Registrierungsdienst, dessen Prüfung um einen zusätzlichen Faktor erweitert werden kann. Über einen weiteren vom Online-Wahlsystem unabhängigen Kanal kann eine *VerifyTAN* an den Wahlberechtigten übermittelt werden. Eine *VerifyTAN* besteht aus einer sicheren zufällig erzeugten Zeichenkette ähnlich wie ein Wählerpasswort, ist aber nur während der Prüfung einmalig gültig, so dass bei jeder Erfassung einer Wählerkennung eine neue generiert wird. Die Gültigkeitsdauer einer *VerifyTAN* sollte auf wenige Minuten oder eine Browsersession begrenzt werden.

Für die Zustellung der *VerifyTANs* sind schnelle Transportwege empfehlenswert, da so die Gültigkeitsdauer der *VerifyTANs* kurz gehalten werden kann. Beispielsweise eignen sich Dienste wie E-Mail, Jabber und SMS dafür. Die nötigen Kontaktinformationen können entweder von dem Wahlberechtigten selber angegeben oder falls diese bekannt sind, direkt verwendet werden. Wenn der Wahlberechtigte die Kontaktinformationen nicht beeinflussen kann, dann wird ein Missbrauchsversuch bei der Registrierung

zusätzlich erschwert. Viele Wahlveranstalter einer Online-Wahl kennen die E-Mail-Adressen der Wahlberechtigten, so dass eine direkte Verwendung für die Übertragung der *VerifyTANs* bei der Registrierung der Wählerkennungen möglich ist.

Durch eine zusätzliche *VerifyTAN* wird der Stimmenkauf (mit Hilfe eines fremden OpenID-Identifiers) erschwert, da bei der Erfassung des OpenID-Identifiers neben den Zugangsdaten für das Erfassungssystem und den Anmeldedaten beim zugehörigen OpenID-Provider auch noch der Zugriff auf den zusätzlichen Kanal, über den die *VerifyTAN* übertragen wird, gebraucht wird. Wenn eine Infrastruktur zur elektronischen Verteilung der *VerifyTANs* vorhanden ist, dann sollte der geringe Mehraufwand für den Gewinn an Sicherheit in Kauf genommen werden.

8 Verlauf der Online-Wahl

In diesem Kapitel wird der Ablauf einer Wahl mit allen nötigen Voraussetzungen und allen möglichen Varianten beschrieben. Dabei wird nicht auf einen speziellen Fall eingegangen, sondern jeder Abschnitt so weit wie möglich allgemein gehalten. Die verwendeten Begriffe und Definitionen sind in den vorangegangenen Kapiteln beschrieben.

Der Wahlprozess kann in mehrere aufeinanderfolgende Phasen gegliedert werden. Nach jeder Phase können alle erfassbaren Ereignisse versiegelt werden, so dass danach noch jeder Schritt überprüfbar und nachvollziehbar ist.

8.1 Voraussetzung

Bevor eine Online-Wahl durchgeführt werden kann, muss sichergestellt werden, dass eine solche Form der Wahl mit den bestehenden Satzungen vereinbar ist. Wenn die rechtlichen Voraussetzungen erfüllt sind, werden die organisatorischen Angelegenheiten festgelegt. Dabei wird unter anderem eine Liste der wahlberechtigten Personen und der wählbaren Kandidaten erstellt. Weiterhin werden das Design der Stimmzettel und Webseiten sowie die auswählbaren Sprachen festgelegt.

Es wird geklärt in welcher Weise die Teilnehmer der Wahl identifiziert werden. Ob dabei bekannte Merkmale zur Authentifizierung genutzt werden können, hängt von der vorhandenen Infrastruktur ab.

Auch muss festgelegt werden, welche OpenID-Provider für die Online-Wahl erlaubt werden. Außerdem wird bestimmt ob *VerifyTANs* bei der Erfassung der Wählerkennungen und ob Wählerpasswörter für den Wahlvorgang verwendet werden sollen. Wenn eine Verwendung angeordnet wird, dann muss die Verteilungsart der *VerifyTANs* bzw. Wählerpasswörter entschieden werden.

Es muss die Betreuung der einzelnen Systeme und Dienste geregelt und ein Notfallplan erstellt werden. Hierbei werden auch die Art der Verschlüsselung und Zugriffsmöglichkeiten für den Wahlvorstand bestimmt.

Nach jeder Entscheidung muss immer wieder geprüft werden, ob die Vereinbarungen den Wahlrechtsgrundsätzen entsprechen.

8.2 Vorbereitung

Während der Vorbereitungsphase werden alle besprochenen Systeme und Dienste installiert und getestet. Dabei werden die Zugangs- und Kommunikationsschlüssel sowie die zu verwendenden Zertifikate festgelegt und verteilt.

Neben den technischen Vorbereitungen werden die Wahlberechtigten über die Start- und Endtermine der Registrierungs- und Wahldurchführungsphasen informiert. Dabei erhalten sie auch die URLs zu den einzelnen für sie wahlrelevanten Diensten und Auflagen wie die Erstellung einer OpenID bei einem zugelassenen OpenID-Provider, falls noch nicht vorhanden.

8.3 Registrierung der Wählerkennungen

Zu einem vorher festgelegten und bekannt gemachten Termin startet die Registrierungsphase der Wählerkennungen. Während dieses Zeitraums müssen die Wahlberechtigten in vereinbarter Weise ihre OpenID-Identifier, die als Wählerkennung dienen, erfassen lassen. Dieser Vorgang durchläuft mehrere Schritte.

Schritt 1

Im ersten Schritt muss die Person identifiziert und deren Wahlberechtigung geprüft werden. Dazu werden die vorher festgelegten Merkmale zur Identifizierung der Person verwendet. Diese Merkmale können wie in Anschnitt 3.1 beschrieben in Wissen, Besitz oder Biometrie kategorisiert werden. Welche Kategorie, oder ob eine oder mehrere Kategorien verwendet werden dürfen oder müssen, wurde in der Vorbereitungsphase festgelegt. Die Prüfungsbedingungen müssen so gewählt sein, dass jeder Wahlberechtigte zweifelsfrei identifiziert werden kann.

Sollte der Wahlveranstalter ein Zugangssystem besitzen, das diese Aufgabe übernehmen kann, vertrauenswürdig und mit den Wahlrechtsgrundsätzen aus Abschnitt 2.2 vereinbar ist, kann dieses genutzt werden. Ein Beispiel für solch ein System könnte ein eigenes Mitgliederportal sein, in dem alle Wahlberechtigten registriert sind. Wenn eine solche Infrastruktur zur Verfügung steht, kann sich der Wahlberechtigte dort anmelden und nach der erfolgreichen Authentifizierung kann seine Wahlberechtigung geprüft werden. Dies kann beispielsweise mit Hilfe einer Liste aller Wahlberechtigten erfolgen.

Sollte der Wahlveranstalter kein geeignetes Zugangssystem besitzen, dann kann er die Wahlberechtigten persönlich überprüfen. Eine persönliche Überprüfung aller Wahlberechtigten sollte aber, falls nicht anders möglich, nur einmal erfolgen, da es gegen den Gedanken einer Online-Lösung spricht. Nach einer erfolgreichen persönlichen Prüfung kann mit jedem Identifizierten ein oder mehrere Merkmale für die nächste Authentifizierung festgelegt werden, damit bei einer erneuten Wahl keine persönliche Prüfung mehr benötigt wird. Eine persönliche Prüfung ist sehr sicher, kostet aber viel Zeit und Geld, wodurch die Gesamtkosten für eine Wahl steigen.

Schritt 2

Wenn eine Person zweifelsfrei entsprechend den Wahlrechtsgrundsätzen als Wahlberechtigter identifiziert wurde, wird im nächsten Schritt ihre Wählerkennung festgelegt.

Für die Wählerkennung wird der offene Standard OpenID eingesetzt. Ein großer Vorteil dieser neuen Technologie ist die benutzerzentralisierte Authentifizierung. Jeder Wahlberechtigte benötigt für die Wahl eine eigene OpenID bei einem für die Online-Wahl zugelassenen OpenID-Provider.

Bei vielen OpenID-Providern ist es möglich, mehrere OpenID-Identifier an einen Account zu binden. Wenn der Wahlberechtigte einen solchen OpenID-Provider, der selbstverständlich für die Wahl zugelassen sein muss, benutzt, dann empfiehlt sich die Erstellung einer zusätzlichen OpenID nur für die Wahl. Dadurch können keine Rückschlüsse von Dritten, die den OpenID-Identifier schon kennen, gezogen werden. Sollte die OpenID beispielsweise schon bei einem Fotoportal mit persönlichen Bildern und eindeutiger Beschriftung genutzt werden, dann wäre ein Rückschluss auf den Besitzer leicht möglich.

Ein Vorteil der Benutzerzentralisierung von OpenID ist, dass der Besitzer die Verwendung seiner OpenID gezielt steuern kann. Der Wahlberechtigte kann daher entsprechend seinem persönlichen Sicherheitsempfinden mit seinen OpenIDs agieren.

Da von einer OpenID zum Schutz der persönlichen Daten des Besitzers nicht auf diese geschlossen werden kann, muss die Zugehörigkeit der OpenID zum Wahlberechtigten geprüft werden. Durch diese Prüfung wird sichergestellt, dass der Wahlberechtigte sich bei der Angabe seines OpenID-Identifiers als Wählerkennung nicht vertippt hat und diese auch wirklich nutzen kann. Weiterhin wird sichergestellt, dass es sich dabei auch um seine OpenID handelt und er nicht die fremde OpenID eines Stimmenkäufers angibt.

Für die Erfassung und Prüfung der OpenIDs wird ein Online-System verwendet. Direkt nachdem der Wahlberechtigte seinen OpenID-Identifier angegeben hat, wird dieser geprüft.

Zuerst wird geprüft, ob der zugehörige OpenID-Provider für die Wahl zugelassen ist und ob es keine *Delegierte OpenID* ist. Eine *OpenID Delegation* ermöglicht eine Art Alias für den OpenID-Identifier. Hierfür kann eine beliebige Webseite verwendet werden, die den Verweis auf den zugehörigen OpenID-Provider und den dortigen OpenID-Identifier enthält. Da so der OpenID-Provider getauscht werden kann, ohne den OpenID-Identifier zu ändern, ist die Verwendung von solchen Delegationen bei einer Online-Wahl nicht erlaubt. Wenn die OpenID den Wahlbestimmungen entspricht, dann wird deren Zugehörigkeit zum Wahlberechtigten geprüft. Dazu muss der Wahlberechtigte sich auf der Folgeseite mit dieser OpenID anmelden. Wenn er sich mit dieser OpenID anmelden kann, dann ist er im Besitz der Authentifizierungsdaten.

Die Qualität dieser Zugangsdaten hat einen direkten Einfluss auf die Sicherheit der Online-Wahl, daher sollte wie eingangs erwähnt sorgfältig ausgewählt werden, welche OpenID-Provider zugelassen werden. Werden nur OpenID-Provider zugelassen, die ihre Benutzer mit starken Identifizierungsverfahren wie Postident bei der Registrierung überprüfen, und nur aufwendige Authentifizierungsmerkmale wie Biometrie oder Smartcards zum Anmelden akzeptieren, dann ist deren Weitergabe der OpenID samt benötigter Zugangsdaten zwecks Stimmenkauf sehr unwahrscheinlich.

Wenn zur Überprüfung der OpenID-Zugehörigkeit auch *VerifyTANs* verwendet werden, dann erhält der Wahlberechtigte direkt nach der Eingabe seines OpenID-Identifiers eine *VerifyTAN* über einen vorher festgelegten Kanal. Für die Zustellung der *VerifyTAN* kann beispielsweise eine E-Mail verwendet werden. Weitere Möglichkeiten sind im Abschnitt 7.3 beschrieben. Nachdem der Wahlberechtigte sich erfolgreich mit seiner OpenID angemeldet hat, muss er auf der Folgeseite die erhaltene *VerifyTAN* eingeben. Die *VerifyTAN* ist nur für einen kurzen Zeitraum gültig und ist an die Sitzung des Browsers (Session-ID) gebunden. Daher kann die *VerifyTAN* nur direkt nach der erfolgreichen Authentifizierung mittels OpenID eingegeben werden. Nur wenn die korrekte *VerifyTAN* eingegeben wurde, wird der OpenID-Identifier als Wählerkennung zugelassen. Der Einsatz von *VerifyTANs* wird vor dem Beginn der Registrierungsphase festgelegt.

Je nach Wahlbestimmung kann das Ersetzen von schon angegebenen OpenID-Identifiern als Wählerkennung während der Registrierungsphase erlaubt oder verweigert werden. Sollte das Ersetzen erlaubt sein, dann wird der schon erfasste OpenID-Identifier nach dem erfolgreichen Durchlaufen aller Prüfungen, wie bei der ersten Erfassung mit dem neuen Identifier, überschrieben. Sollte jedoch das Ersetzen nicht erlaubt sein, dann erhält der Wahlberechtigte erst nach der erfolgreichen Anmeldung mit seiner OpenID die Hinweismeldung, dass das Ändern nicht erlaubt ist. Dadurch

ist es Angreifern nicht möglich durch einfaches Angeben von OpenID-Identifiern deren mögliche Wahlverbindung zu erkennen.

Wenn ein Wahlberechtigter eine OpenID angegeben hat, die alle Prüfungen überstanden hat, dann wird der OpenID-Identifier für ihn als Wählerkennung mit dem Vermerk der erfolgreichen Prüfung verschlüsselt in eine Datenbank geschrieben. Dabei wird eine asymmetrische Verschlüsselung verwendet, so dass nur bei der Erstellung des Wählerverzeichnisses die Einträge entschlüsselt werden können.

In Abbildung 8.1 ist der Ablauf der Registrierung dargestellt. Die Schritte, die beim Einsatz einer *VerifyTAN* hinzukommen, sind grau hinterlegt.

Schritt 3

Die Datenbank enthält am Ende der Registrierungsphase alle erfolgreich geprüften OpenID-Identifier der Wahlberechtigten, die sich registriert haben. Aus dieser Datenbank werden alle mit dem Merkmal für erfolgreiche Prüfung versehenen verschlüsselten OpenID-Identifier entnommen. Wenn beim Wahlvorgang Wählerpasswörter verwendet werden sollen, dann müssen die nötigen Kontaktdaten der Wahlberechtigten dem Verteilerdienst zur Verfügung stehen. Daher werden die Kontaktdaten asymmetrisch verschlüsselt, so dass nur der Verteilerdienst sie entschlüsseln kann, und als Tupel zusammen mit den verschlüsselten OpenID-Identifier für die Erstellung des Wählerverzeichnisses weitergereicht. Dabei darf die Zugehörigkeit der verschlüsselten Kontaktdaten zu den verschlüsselten OpenID-Identifiern nicht gestört werden, da sie von keinem anderen wiederhergestellt werden kann.

Da nur verschlüsselte Daten weitergegeben werden, kann kein Dritter bei einem erfolgreichen Angriff auf die Übertragung eine relevante Information gewinnen. Trotzdem sollte für die Übertragung ein sicherer Kanal gewählt werden, damit die Integrität der Daten nicht gefährdet wird.

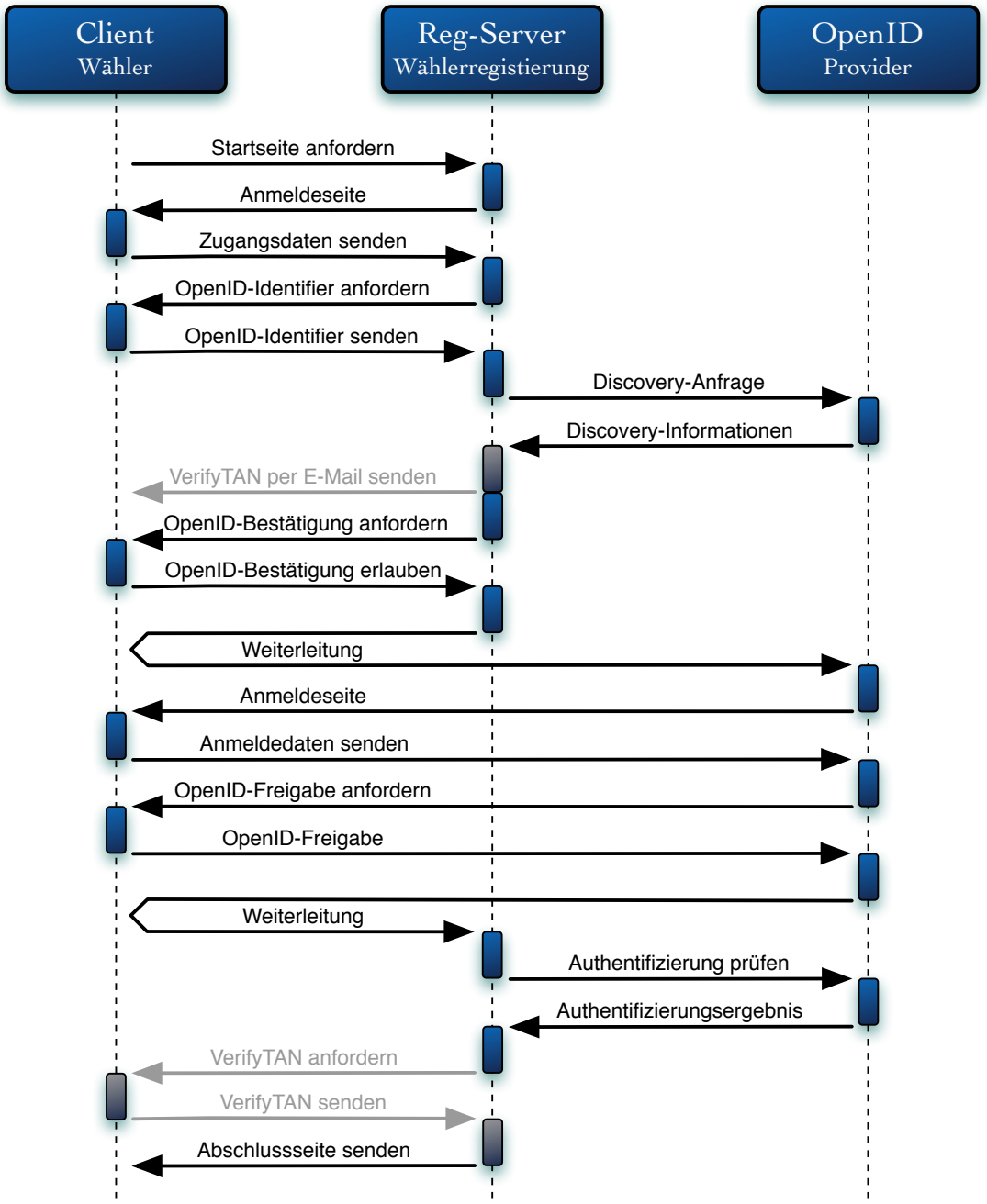

Abbildung 8.1: Registrierungsvorgang mit optionaler *VerifyTAN* (hellgrau)

8.4 Erstellung des Wählerverzeichnisses

Für die Erstellung des Wählerverzeichnisses werden die vom Registrierungsdienst erhaltenen Daten verwendet. Dazu werden zuerst die verschlüsselten OpenID-Identifier entschlüsselt.

Ein OpenID-Identifier kann mit unterschiedlichen Zeichenketten beschrieben werden. Da es bei solchen Identifiern um URLs handelt, können sie beispielsweise mit oder ohne führende Protokoll-Kennzeichnung (*http://* oder *https://*) angegeben werden. Trotz der unterschiedlichen Schreibweise ist ihre Verbindung zur OpenID eindeutig. Als Wählerkennung wird daher der Identifier in eine eindeutige, normalisierte Form gebracht, so dass jede mögliche in der Spezifikation von OpenID beschriebene Darstellungsform eines OpenID-Identifiers zu derselben normalisierten Zeichenkette führt. Anschließend werden im Wählerverzeichnis die normalisierten Identifier als Wählerkennungen für die Wahlberechtigten gespeichert.

Wenn beim Wahlvorgang auch Wählerpasswörter verwendet werden sollen, dann werden diese bei der Generierung des Wählerverzeichnisses automatisch mit erstellt. Die Wählerpasswörter sind wie in Abschnitt 7.1 beschrieben zufällig erzeugte Zeichenketten, die den Wählerkennungen fest zugeordnet sind. Der Wähler muss in diesem Szenario nach der erfolgreichen Authentifizierung mittels OpenID das zugehörige Wählerpasswort angeben, um sich beim Wahlsystem anzumelden. Bei der Erzeugung der Wählerpasswörter werden diese automatisch mittels asymmetrischer Verschlüsselung mit dem öffentlichen Schlüssel des Verteilerdienstes verschlüsselt.

Für die Verteilung der Wählerpasswörter werden die Kontaktdaten der Wahlberechtigten benötigt. Diese wurden bei der Registrierung der Wähler mit dem öffentlichen Schlüssel des Verteilerdienstes verschlüsselt und den verschlüsselten OpenID-Identifiern zugeordnet. Mit dieser Zuordnung werden die verschlüsselten Wählerpasswörter den verschlüsselten Kontaktdaten zugewiesen, indem einfach die Einträge der verschlüsselten OpenID-Identifier mit denen der verschlüsselten Wählerpasswörter ersetzt werden. Anschließend werden die Wählerpasswörter über einen sicheren Kanal an den Verteilerdienst übergeben.

8.5 Optionale Verteilung der Wählerpasswörter

Wenn bei der Wahl Wählerpasswörter eingesetzt werden, dann verteilt dieser Dienst sie vor dem Wahlstart. Der Verteilungsdienst für Wählerpasswörter entschlüsselt die erhaltenen Kontaktdaten und Wählerpasswörter. Danach versendet er die Wählerpasswörter an die zugehörigen Wahlberechtigten mittels der Kontaktdaten.

Dabei verlässt er sich auf die Integrität der erhaltenen Daten und Zuordnungen zwischen den Kontaktdaten und den Wählerpasswörtern. Da ihm die zugehörigen Wählerkennungen nicht bekannt sind, kann er keine Rückschlüsse von den Kontaktdaten auf das Wahlverhalten der Wahlberechtigten ziehen.

8.6 Die Wahldurchführungsphase

Nachdem alle organisatorischen und technischen Vorbereitungen abgeschlossen sind und die Wahlberechtigten ihre nötigen Zugangsdaten für den Wahlvorgang kennen, kann die Wahldurchführungsphase gestartet werden. Der genaue Zeitpunkt für den Start sowie für das Ende wurde während der Vorbereitungsphase festgelegt und dem Wahlberechtigten mit der URL für das Wahlsystem mitgeteilt.

Während der Wahldurchführungsphase kann sich der Wahlberechtigte am Wahlsystem anmelden. Dazu gibt er seinen vorher registrierten OpenID-Identifier ein und wird zur Authentifizierung zum OpenID-Provider weitergeleitet. Wenn er sich dort korrekt authentifiziert hat, wird vom Wahlsystem die erfolgreiche Authentifizierung validiert und im Erfolgsfall gelangt er zur Folgeseite.

Bei einer Wahl mit Wählerpassworten wird er nun aufgefordert sein Wählerpasswort einzugeben, welches danach mit Hilfe seines Eintrags im Wählerverzeichnis geprüft wird. Nach einer erfolgreichen Prüfung gelangt er zu derselben Folgeseite, zu der auch ein Wähler bei einer Wahl ohne Wählerpasswörter ohne diesen Zwischenschritt gelangen würde.

Sobald der Wähler sich erfolgreich am Wahlsystem angemeldet hat, wird seine Wahlberechtigung geprüft. Dabei wird geschaut, ob er schon eine Stimme verbindlich abgegeben hat. Wenn er dies getan hat, dann ist dieses im Wählerverzeichnis vermerkt und er bekommt einen Hinweis, dass für ihn die Wahl beendet ist, weil er schon gewählt hat. Sollte er schon gewählt haben ohne seine Stimme verbindlich abgegeben zu haben oder noch keinen Stimmzettel ausgefüllt haben, dann wird er zum Stimmzettel weitergeführt. Bei dieser Weiterleitung wird die Verbindung zu seiner Person gelöst, so dass er geheim wählen kann.

Jetzt kann er seinen Stimmzettel ausfüllen und bei Bedarf korrigieren bevor er ihn verbindlich abgibt. Erst nach der verbindlichen Abgabe des Stimmzettels, wird dieser der Urne zugeführt.

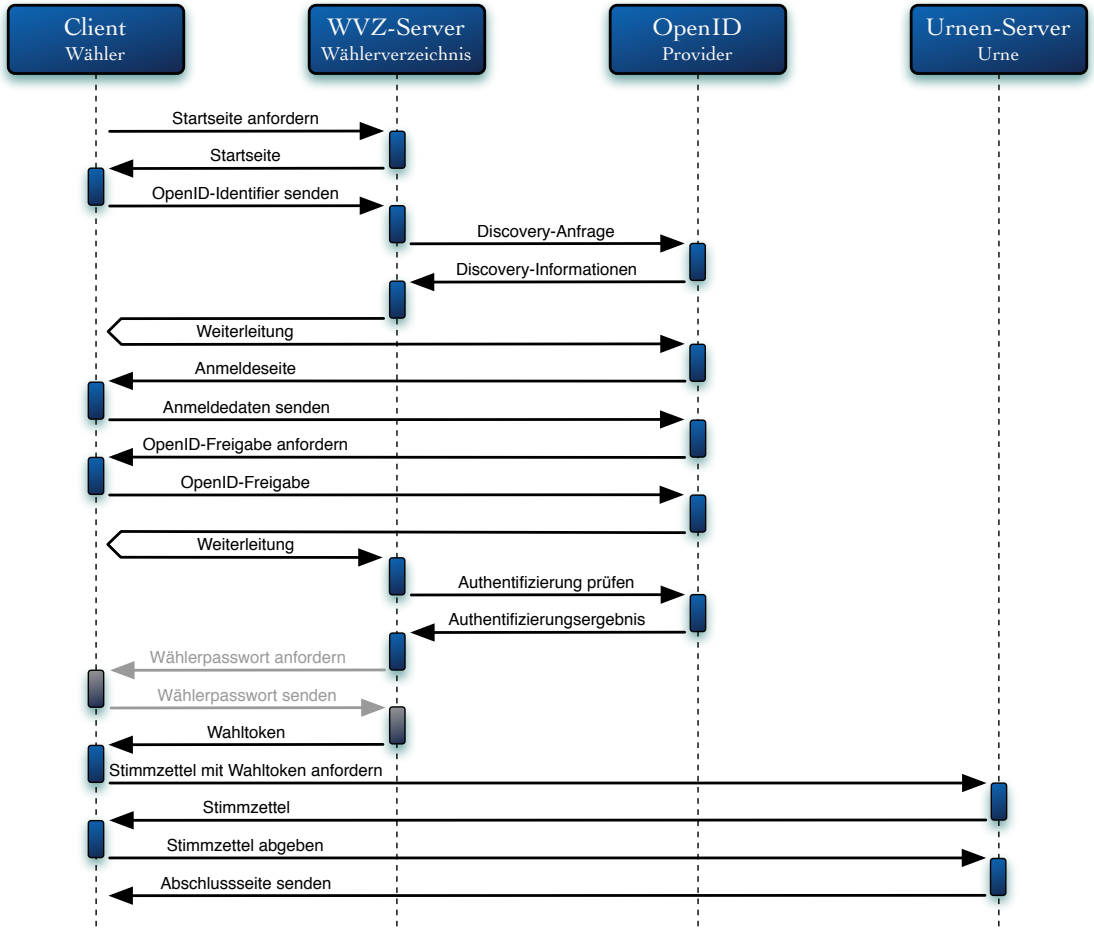

Abbildung 8.2: Wahlvorgang mit optionalem Wählerpasswort (hellgrau)

8.7 Auszählung und Dokumentation

Am Ende der Wahldurchführungsphase werden die Wahlsysteme für die Wahlberechtigten gestoppt, so dass sich der Inhalt der Urne nicht mehr verändern lässt. Danach kann mit der Auszählung der Stimmzettel begonnen werden. Im Gegensatz zu einer Papierwahl können die Stimmzettel nicht mit zusätzlichen Markierungen, wie beispielsweise dem Namen des Wählers, einem Satz über die Kandidaten, kleinen Zeichnungen oder gewollten Beschädigungen des Papiers versehen werden. Somit können die Stimmzettel vom Wähler nur durch falsche Stimmabgabe ungültig gemacht werden. Dies kann entweder, falls beim Stimmzettel vorgesehen, durch ein Kreuz bei „ungültig Wählen“, durch eine unzulässige Anzahl an Kreuzen oder gleichzeitiges Auswählen von „Ja“ & „Nein“ bei Einzelentscheidungen geschehen. Ein Vorteil bei der Auszählung von Online-Wahlen ist, dass das undeutliche Ankreuzen von Kandidaten wegfällt. Folglich kann jedes Kreuz unmissverständlich als Wählerwille erkannt und ausgezählt werden.

Entsprechend der Wahlverordnung werden die Stimmzettel ausgezählt und die Anzahl der entsprechenden Möglichkeiten erfasst.

Die Anzahl der verbindlichen Stimmabgaben aus dem Wählerverzeichnis muss selbstverständlich mit der Anzahl der Stimmzettel aus der Urne übereinstimmen.

Das Ergebnis der Stimmzettel sowie eine elektronische Kopie der Stimmzettel (falls möglich) wird zusammen mit der *Dokumentation vom Wählerverzeichnis* an den Wahlveranstalter übergeben. Darin ist aufgeführt mit welcher Wählerkennung eine verbindliche Stimme abgegeben wurde. Des Weiteren werden die Dokumentation über den Wahlablauf mit allen aufgetretenen Ergebnissen, die eingesetzten Prüfsummen und vieles mehr an den Wahlveranstalter übergeben.

Wenn der Wahlveranstalter die *Dokumentation vom Wählerverzeichnis* den Wahlberechtigten zugänglich macht, dann können diese überprüfen, ob mit ihrer Wählerkennung eine verbindliche Wahlhandlung ausgeführt wurde. Dieses Vorgehen ist im Zusammenhang mit der *Überprüfbarkeit der Wahl* [BVe] empfehlenswert. Da als Wählerkennung nur OpenID-Identifier zu sehen sind, kann kein Rückschluss auf die zugehörigen Personen gezogen werden. Somit kann leicht jeder registrierte Wahlberechtigte seinen Eintrag im Wählerverzeichnis finden und verifizieren.

9 Implementierung

In diesem Kapitel wird die als *Proof-of-Concept* erstellte Referenzimplementierung beschrieben. Neben der Arbeit wurde die hier entwickelte und vorgestellte Lösung mit allen Varianten als Software-Produkt erstellt und getestet. Dazu wurde ein Online-System für die Registrierung der Wählerkennungen und ein Portal zur beispielhaften Personenprüfung neu entwickelt und das schon vorhandene Online-Wahlsystem *Polyas* [Pol] angepasst und verwendet.

9.1 Das Online-Wahlsystem Polyas

Den Ausschlag für die Verwendung des Online-Wahlsystem *Polyas* [Pol] der *Micromata GmbH* für die Referenzimplementierung brachte der langjährige produktive Einsatz dieses Online-Wahlsystems. Im Gegensatz zu vielen anderen Online-Wahlsystemen hat *Polyas* schon in mehr als einem Jahrzehnt seine Praxistauglichkeit bewiesen. *Polyas* wurde erstmals 1996 bei der finnischen *Youth Elections* [Fin] eingesetzt, bei der 64.000 finnische Jugendliche ihre Stimme elektronisch abgaben. In Deutschland wird seit 2002 jede *Juniorwahl* [Kum] mit diesem Online-Wahlsystem durchgeführt. Im Jahr 2003 wurde es für die erste rechtsgültig Online-Wahl in Deutschland, bei der Wahl des Vorstandes der *Initiative D21* [D21], verwendet. Neben der *Gesellschaft für Informatik* [GI] und der *Deutschen Forschungsgesellschaft* [DFG] wählten auch Versicherungen, Genossenschaftsbanken und andere Unternehmen, Organisationen und Vereine mit *Polyas*, so dass bis heute über 750.000 verbindliche Stimmen mit diesem Online-Wahlsystem abgegeben wurden. Neben der nachgewiesen Praxistauglichkeit soll auch die Sicherheit von *Polyas* durch eine gerade laufende Zertifizierung nach *Common Criteria* [CC] bestätigt werden.

Die in dieser Arbeit vorgestellte Lösung ist für jedes Online-Wahlsystem mit vorgelagerter Wählerauthentifizierung geeignet und nicht nur in Verbindung mit *Polyas* einsetzbar.

9.1.1 Konzept von Polyas

Der Aufbau von *Polyas* orientiert sich an einer Urnenwahl in einem Wahllokal und nicht an einer Briefwahl. Ähnlich dem klassischen Aufbau einer papierbasierten Präsenzwahl gibt es auch bei *Polyas* ein Wählerverzeichnis und eine Wahlurne. Daher wird die Verbindung zwischen dem Wähler und seinem Stimmzettel schon beim Einwurf in die Wahlurne dauerhaft gelöst und nicht, wie bei einer Briefwahl, erst bei der Auszählung der Stimmen.

9.1.2 Komponenten von Polyas

Das Wahlsystem besteht aus vier eigenständigen Teilsystemen, die alle auf verschiedenen Rechnern in unterschiedlichen Rechenzentren betrieben werden können. Alle Teilsysteme kommunizieren verschlüsselt durch das Internet miteinander. Für den Wahlvorgang benötigt der Wähler nur einen Browser, einen Internetzugang und seine Zugangsdaten. Die Abbildung 9.1 zeigt die Komponenten von *Polyas* und deren Verbindung durch das Internet.

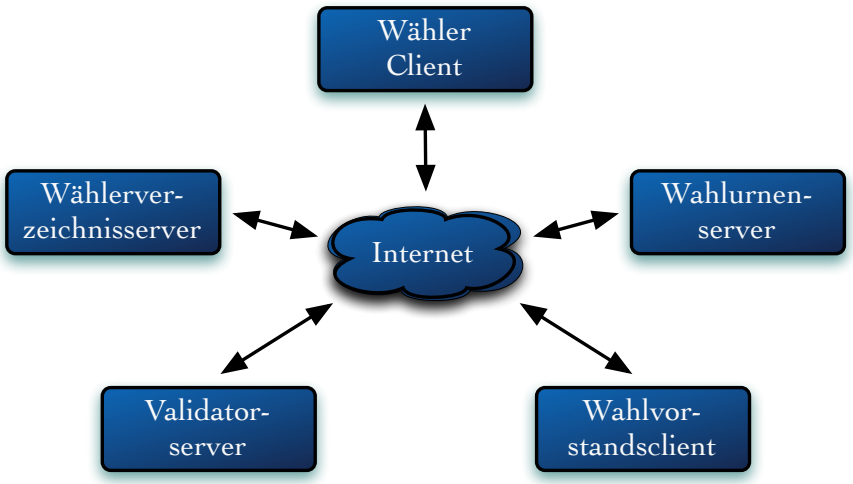

Abbildung 9.1: Komponenten von *Polyas*

Wählerverzeichnis

Die Überprüfung der Wahlberechtigung übernimmt in der ursprünglichen Version von *Polyas* alleine das Wählerverzeichnis. Ihm gegenüber muss der Wähler sich identifizieren und seine Identität nachweisen. Dazu wurden bei den meisten Wahlen

Wählerkennungen und Wählerpasswörter verwendet, die mit PIN-Briefen verteilt wurden. Nach der Authentifizierung beim Wählerverzeichnis wird die Wahlberechtigung des Teilnehmers geprüft. Falls die Identität der Person zweifelsfrei nachgewiesen wurde und eine Wahlberechtigung vorlag, hat der Wähler ein *Wahltoken* erhalten. Ein *Wahltoken* besteht aus einer langen zufällig erzeugten Zeichenkette und wird für den Zugang zur Urne verwendet.

Wahlurne

Die Wahlurne enthält die Stimmzettel und kennt keine Daten von den Wahlberechtigten. Einen Stimmzettel erhält der Wähler nur, wenn er der Wahlurne ein gültiges *Wahltoken* übergibt. Nachdem der Wähler seinen Stimmzettel ausgefüllt und seine Wahl verbindlich bestätigt hat, wird sein Stimmzettel in der Urne dauerhaft gespeichert. Sein *Wahltoken* wird dabei für ungültig erklärt und sein Wahlvorgang im Wählerverzeichnis vermerkt. Sollte sich der Wähler erneut beim Wählerverzeichnis anmelden, dann erhält er kein *Wahltoken* mehr, da seine Wahlberechtigung durch die verbindliche Abgabe erloschen ist. Eine erneute Anmeldung an der Urne mit seinem erhaltenen *Wahltoken* ist ebenfalls nicht möglich, da diese inzwischen ungültig ist. Nach dem Ende der Wahldurchführungsphase werden die Stimmzettel der Wahlurne ausgezählt.

Validator

Der Validator dient als Kontrollinstanz für das Wählerverzeichnis und die Wahlurne. Durch ihn wird verhindert, dass Einträge nach der Erstellung des Wählerverzeichnisses verändert oder hinzugefügt werden können. Er besitzt zu jedem Eintrag im Wählerverzeichnis einen Kontrollwert, der bei der Anmeldung am Wählerverzeichnis geprüft wird. Wenn die Authentifizierung des Wählers beim Wählerverzeichnis erfolgreich war, seine Wahlberechtigung festgestellt wurde und der Kontrollwert vom Validator geprüft wurde, dann erzeugt der Validator ein *Wahltoken*. Dieses ist zufällig und vom Validator keiner Person zuordbar. Der Validator kann aus dem Kontrollwert nicht erkennen, welcher Eintrag aus dem Wählerverzeichnis dazugehört. Nach der Erzeugung des *Wahltokens* wird es der Wahlurne und dem Wählerverzeichnis übermittelt. Das Wählerverzeichnis reicht das *Wahltoken* an den Wähler weiter.

Wahlvorstandsinterface

Das Wahlvorstandsinterface bietet den Berechtigten des Wahlvorstandes die Steuerung der anderen drei Komponenten und ermöglicht das Freischalten des Wahlsystems,

die Durchführung von Selbsttests, das Starten und Stoppen der Wahl, sowie das Auszählen und Archivieren. Nachdem das Wahlsystem für eine Wahl installiert, konfiguriert und das Wählerverzeichnis erstellt wurde, können alle weiteren Schritte über das Interface durchgeführt werden, so dass keine direkten Zugriffe auf die zur Wahl beteiligten Server mehr nötig sind. Das Online-Wahlsystem kann direkt über einen Browser gesteuert werden.

9.2 Erweiterung des Online-Wahlsystems

Das Online-Wahlsystem *Polyas* wurde für die vorgestellte Lösung mit der Anbindung an externe Authentifizierungsdienste erweitert und angepasst. Hierfür wurden das Wählerverzeichnis und der zugehörige Dienst erweitert, so dass eine Anmeldung mit OpenID möglich ist. Das Tool zur Erstellung des Wählerverzeichnisses wurde mit neuen Funktionen versehen, so dass OpenID-Identifier als Wählerkennung verwendet werden können. Weiterhin wurde ein Wählerregistrierungsdienst mit Server neu entwickelt, um die OpenID-Identifier der Benutzer erfassen zu können.

Das ursprüngliche Online-Wahlsystem wurde so erweitert, dass die Verwendung von Wählerpasswörtern nicht mehr nötig ist und diese nur noch auf Wunsch des Wahlveranstalters als zusätzliches Authentifizierungsmerkmal verwendet werden können. Daher ist eine kostenintensive Verteilung von Zugangsdaten mittels PIN-Briefen nicht mehr erforderlich.

Der Wahlberechtigte kann seinen Authentifizierungsdienst in Form eines OpenID-Providers selbst auswählen. Dabei kann er den Provider auswählen, dem er das meiste Vertrauen schenkt. Als Hilfe bei dieser Auswahl kann der Wahlveranstalter selbstverständlich Empfehlungen geben oder wie in Abschnitt 5.3 beschrieben nur bestimmte Provider für die Verwendung bei der Online-Wahl zulassen. Aus den bei den Providern verwendbaren Authentifizierungsmerkmalen kann der Wahlberechtigte ebenfalls frei wählen, so dass er für sich persönlich entscheiden kann, wie sicher seine Authentifizierung bei der Wahl sein soll. Somit ist es nicht zwingend nötig, dass jeder Wahlberechtigte eine Multi-Faktor-Authentifizierung mit kryptographisch extrem sicheren Geräten bei seinem Provider vornehmen muss, aber falls jemand dies wünscht, kann er dies tun. Jeder Wahlberechtigte kann direkten Einfluss auf die Qualität seiner Authentifizierung nehmen.

Das erweiterte Online-Wahlsystem mit allen Komponenten ist in Abbildung 9.2 dargestellt. Im Folgenden werden erst der neu erstellte Wählerregistrierungsserver und danach die Änderungen am Tool zur Erstellung des Wählerverzeichnisses sowie die Änderungen am Wählerverzeichnisdienst beschrieben. Anschließend wird deren Verwendung aus der Sicht der Wahlteilnehmer gezeigt.

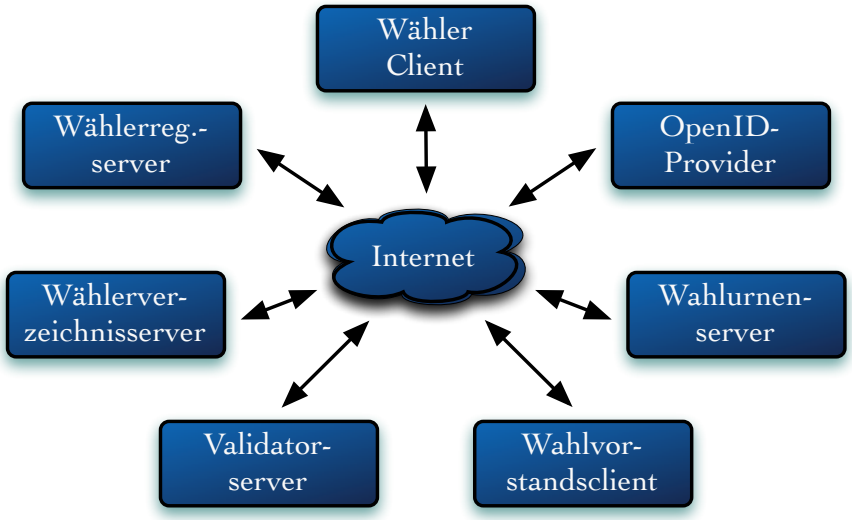

Abbildung 9.2: Komponenten des erweiterten Wahlsystems

9.3 Wählerregistrierungsserver

9.3.1 Beschreibung

Der Wählerregistrierungsserver ist ein neu entwickeltes, eigenständiges System, das die Prüfung der Teilnahmeberechtigungen für die Wahl übernimmt und die Wählerkennungen nach einer gründlichen Prüfung erfasst. Jeder Wahlberechtigte benötigt vor dem Start der Wahldurchführungsphase seine Zugangsdaten. Im Gegensatz zur ursprünglichen Variante, werden den Wahlberechtigten diese Zugangsdaten nicht zugesandt, sondern sie legen diese selber fest. Als Wählerkennung werden OpenID-Identifier verwendet, die die Wahlberechtigten selber angeben, da sie nur ihnen bekannt sind. Die Authentifizierungsmerkmale für die Nutzung der Identifier werden ebenfalls von den Wahlberechtigten bei den zugehörigen OpenID-Providern festgelegt. Daher hat der Wahlberechtigte einen direkten Einfluss auf die Qualität seiner Authentifizierung. Falls der Wahlveranstalter nur bestimmte OpenID-Provider für die Online-Wahl zulassen möchte, kann er diese mit einer *Whitelist* angeben. Sollte ein Wahlberechtigter einen nichtzugelassenen OpenID-Provider für die Authentifizierung bei der Wahl verwenden wollen, dann wird dies schon bei der Registrierung seines OpenID-Identifiers bemerkt, so dass sichergestellt ist, dass alle erfassten OpenID-Identifier auch für die Wahl zugelassen sind. Weiterhin wird sichergestellt, dass bei der Angabe des OpenID-Identifiers keine Tippfehler gemacht wurden und der Wahlberechtigte die Authentifizierungsmerkmale für seinen OpenID-Account benutzen kann. Alle erfassten OpenID-Identifier durchlaufen schon bei der Registrierung dieselben Sicher-

heitsprüfungen, die später bei der OpenID-Anmeldung am Wählerverzeichnisserver erfolgen. Folglich ist sichergestellt, dass die erfassten OpenID-Identifier auch beim Wahlvorgang genutzt werden können.

Die Registrierung erfolgt in den im Abschnitt 8.3 beschriebenen Schritten. Die erste Prüfung bei Registrierung einer Wählerkennung ist die Teilnahmeberechtigung an der folgenden Wahl. Dazu muss als Erstes die Identität der Person geprüft werden. Dies kann entweder durch eine menschliche oder eine maschinenunterstützte Methode passieren.

In vielen Fällen sind die Personen, die an der Wahl teilnehmen dürfen, schon elektronisch beim Wahlveranstalter erfasst. Wenn die Teilnehmer schon Zugangsdaten von einem anderen System oder Dienst des Wahlveranstalters haben und sie sich mit diesen Zugangsdaten authentifizieren können, dann können diese für die Personenprüfung beim Registrierungsserver genutzt werden. Hierfür könnte beispielsweise ein Portal mit dem Registrierungsserver verbunden werden. Sollte keine passende Infrastruktur vorhanden sein, ist eine persönliche Prüfung notwendig.

Damit die Implementierung keine persönliche Personenprüfung benötigt, wurde auch hierfür eine Online-Lösung entwickelt. Die Teilnehmer melden sich zuerst mit ihren Authentifizierungsmerkmalen am Wählerregistrierungsserver an. Wie üblich erhalten die Benutzer ihre Authentifizierungsdaten nach einer Personenprüfung, so dass der Registrierungsdienst keine weiteren Personenprüfungen mehr vornehmen muss.

Für die Referenzimplementierung wurde eine Anmeldung mit Benutzername und Passwort erstellt, da dies die weitverbreitetsten Merkmale sind und keine zusätzliche Hard- oder Software benötigen. Diese Anmeldung kann selbstverständlich leicht für einen speziellen Anwendungsfall mit anderen Authentifizierungsmerkmalen angepasst werden.

9.3.2 Konfiguration

Entsprechend den jeweiligen Wahlbestimmungen kann als weiterer Faktor für die Personenprüfung eine in Abschnitt 7.3 beschriebene *VerifyTAN* verwendet werden. Die Entscheidung darüber kann in der Konfigurationsdatei des Dienstes eingestellt werden. Weiterhin kann eine *Whitelist* mit den für die Wahl zugelassenen OpenID-Providern angegeben werden. Hierbei ist eine Zulassungsentscheidung auf Grund des verwendeten Transfer-Protokolls möglich, so dass bei Providern, die sowohl verschlüsselte als auch unverschlüsselte Kommunikation mit dem OpenID-Endpoint erlauben, nur die sichere Variante erlaubt wird. Das Listing 9.1 zeigt die entsprechenden Konfigurationseinträge mit beispielhaften Werten.

Listing 9.1: Konfiguration des Wählerregistrierungsservers

```
<!-- useVerifyTan: "yes" or "no"
    (default: send VerifyTAN via Email) -->
<Environment
    name="useVerifyTan"
    type="java.lang.String"
    override="false"
    value="yes"
 />


<!-- List of allowed OpenID-Providers -
    Some Providers have different Endpoints
    for http and https -->
<Environment
    name="OPEndpointsAllowed"
    type="java.lang.String"
    override="false"
    value="http://pip.verisignlabs.com/server,
           https://pip.verisignlabs.com/server,
           http://www.myopenid.com/server,
           https://www.myopenid.com/server,
           https://open.login.yahooapis.com/openid/op/auth,
           http://meinguter.name/index.php/serve,
           https://my.xlogon.net/server/"
 />
```

9.4 Tool zum Erstellen des Wählerverzeichnisses

9.4.1 Beschreibung

Das Online-Wahlsystem *Polyas* enthält ein Tool zur Erstellung eines Wählerverzeichnisses. Dieses Tool wurde erweitert, so dass es die vom Wählerregistrierungsdienst erfassten OpenID-Identifier verwenden und zusätzlich optionale Wählerpasswörter beliebiger Länge erstellen kann.

Die vom Wählerregistrierungsdienst verschlüsselten OpenID-Identifier werden entschlüsselt und als Wählerkennungen in das Wählerverzeichnis eingetragen. Sollen zusätzlich Wählerpasswörter für die Wahl verwendet werden, dann werden diese automatisch erstellt und einer Einwegfunktion übergeben, deren Ergebnis zur Wählerkennung mit ins Wählerverzeichnis eingetragen wird. Gleichzeitig werden die Passwörter dabei so verschlüsselt, dass nur der Verteilungsdienst sie entschlüsseln kann und zusammen mit den vom Registrierungsserver erhaltenen verschlüsselten

Kontaktdaten an den Verteilungsdienst weitergegeben. Diese Informationsweitergabe ist in Abbildung 7.1 dargestellt.

Sollen keine Wählerpasswörter verwendet werden, werden für jede Wählerkennung interne Prüfwerte erstellt, die zusammen mit den Wählerkennungen anstelle eines Passwortes mit in das Wählerverzeichnis eingetragen werden. Durch dieses Vorgehen können alle Prüffunktionen des Validators erhalten bleiben.

Zum Schutz vor Angriffen auf die verwendete Einwegfunktion werden die Wählerpasswörter bzw. internen Prüfwerte mit einer zufällig erzeugten Zeichenkette expandiert, so dass eine Vorberechnung mit Zeichenketten entsprechend der zu erwartenden Passwortlänge nicht möglich ist. Weiterhin wird zur stärkeren Bindung des Wählerpasswortes bzw. Prüfwertes an die Wählerkennung, ein Teil des OpenID-Identifiers mit an die Funktion übergeben.

Sollte ein Angreifer Zugriff auf die Zeichenkette mit dem Ergebnis der Einwegfunktion in der Datenbank erhalten, dann würde der Austausch dieser Zeichenkette gegen eine, deren Eingabepasswort ihm bekannt ist, ihm keine Anmeldung ermöglichen. Er würde zusätzlich die geheime Zeichenkette zur Expandierung und die Zugangsdaten für den OpenID-Identifier kennen müssen. Ein Austausch des OpenID-Identifiers würde nicht unbemerkt bleiben, da alle OpenID-Identifier auch dem Registrierungsdienst bekannt sind. Zusätzlich müsste ein Angreifer auch Zugriff auf den Validator haben, da dieser unabhängig jede Anmeldung überprüft.

9.4.2 Konfiguration

Sollen für die Wahl zusätzliche Wählerpasswörter genutzt werden, dann wird deren Länge bei der Erstellung des Wählerverzeichnisses festgelegt. Wenn keine Wählerpasswörter verwendet werden sollen, dann wird eine weitere zufällige Zeichenkette angegeben. Das Listing 9.2 zeigt die Eingabeaufforderung bei der Erstellung des Wählerverzeichnisses.

Listing 9.2: Konfiguration zur Erstellung des Wählerverzeichnisses

```
1 if arg -t 0
2   create tan for internal use only
3   tan = sha256(tanExpand + sha256(pin + salt))
4 else
5   create tan with random printTan-part for voter-auth
6   tan = sha256(tanExpand + printTan + sha256(pin))
7
8 Please insert length of passwords and if necessary a saltstring
9 Usage: -t <n>
10        -t 0 -s <salt>
11 Input:
```

Neben den Daten für die Datenbanken des Wählerregistrierungs- und Validatorservers werden Konfigurationsinhalte für den Wählerverzeichnisserver ausgegeben. Diese enthalten die Entscheidung über die Verwendung von Wählerpasswörtern und die Zeichenketten zur Expandierung für die Einwegfunktion. Ein Beispiel für solche Konfigurationsinhalte für den Wählerverzeichnisserver zeigt das Listing 9.3. Bei der Verwendung von Wählerpasswörtern wird zusätzlich eine verschlüsselte Datei mit den Daten für den Verteilerdienst erzeugt.

Listing 9.3: Konfigurationseinträge für den Wählerverzeichnisservers

```
1 Add the following lines into context.xml:
2 <Environment
3     name="useTan"
4     type="java.lang.String"
5     override="false"
6     value="yes"
7  />
8 <Environment
9     name="tanExpand"
10    type="java.lang.String"
11    override="false"
12    value="R28xd28zaHBEYURVVldVZUtUUjBsQUx5aWw0ckFWNkY="
13 />
```

9.5 Wählerverzeichnisserver

9.5.1 Beschreibung

In der ursprünglichen Version wurden die Wähler vom Wählerverzeichnisserver authentifiziert. Mit Hilfe des Wählerverzeichnisses wurde geprüft, ob die Authentifizierung gültig ist und ob für den Geprüften eine Wahlberechtigung vorliegt. Diese Authentifizierungsmechanismen wurden erweitert, so dass auch eine Authentifizierung mit OpenID möglich ist. Die Erweiterung wurde so eingebettet, dass auch die ursprüngliche Variante noch verwendbar ist. Daher kann auch ein Spezialfall, bei dem einige Wähler statt mit OpenID weiterhin mit vergebener Wählerkennung und PIN wählen, ermöglicht werden. Die gleichzeitige Verwendung beider Varianten ist unzulässig.

9.5.2 Konfiguration

Wie beim Wählerregistrierungsserver kann auch beim Wählerverzeichnisserver eine *Whitelist* mit den für die Wahl zugelassenen OpenID-Providern angegeben werden.

Dies sollte die gleiche Liste wie in der Konfigurationsdatei des Wählerregistrierungsserver (siehe Listing 9.1) sein. Sie darf mehr, aber auf keinen Fall andere Einträge als die Konfigurationsdatei des Wählerregistrierungsserver enthalten, da sonst zugelassene OpenID-Identifier abgewiesen werden könnten.

Entsprechend den jeweiligen Wahlbestimmungen können Wählerpasswörter als weiterer Faktor für die Wählerauthentifizierung verwendet werden. Diese Entscheidung wird in der Konfiguration des Wählerverzeichnisses, wie in Listing 9.4 beispielhaft dargestellt, angegeben. Die Daten dafür werden bei der Erstellung des Wählerverzeichnisses automatisch mit erzeugt (vergleiche Listing 9.3).

Listing 9.4: Konfiguration des Wählerverzeichnisservers

```
<!-- List of allowed OpenID-Providers -
    Some Providers have different Endpoints
    for http and https -->
<Environment
    name="OPEndpointsAllowed"
    type="java.lang.String"
    override="false"
    value="http://pip.verisignlabs.com/server,
           https://pip.verisignlabs.com/server,
           http://www.myopenid.com/server,
           https://www.myopenid.com/server,
           https://open.login.yahooapis.com/openid/op/auth,
           http://meinguter.name/index.php/serve,
           https://my.xlogon.net/server/"
 />
<!-- useTan:    "yes" or "no" -->
<!-- tanSalt:   needed if useTan is set to "no" -->
<!-- tanExpand: Random value created with Registry -->
<Environment
    name="useTan"
    type="java.lang.String"
    override="false"
    value="no"
 />
<Environment
    name="tanSalt"
    type="java.lang.String"
    override="false"
    value="Pepper4Polyas"
 />
<Environment
    name="tanExpand"
    type="java.lang.String"
    override="false"
    value="R28xd28zaHBEYURVVldVZUtUUjBsQUx5aWw0ckFWNkY="
 />
```

9.6 Registrierung der Wählerkennung

In diesem Abschnitt wird die Registrierung der Wählerkennung aus der Sicht der Wahlberechtigten beschrieben. Jeder Wahlberechtigte benötigt für den Wahlvorgang eine Wählerkennung. Da als Wählerkennung OpenID-Identifier verwendet werden, können die Wählerkennungen nicht an die Wahlberechtigten verteilt werden. Dies spart gleichzeitig die Kosten für die Verteilung.

Bei dem folgenden Ablauf wird, falls nicht explizit anderes beschrieben, davon ausgegangen, dass jeder Schritt erfolgreich durchlaufen wird. Kommt es durch eine falsche Eingabe eines Benutzers, fehlender Teilnahmeberechtigung an der Wahl oder aus anderen Gründen zu einem Fehler, dann wird der Benutzer auf eine Fehlerseite geführt. Es ist aus Sicherheitsgründen nicht möglich einen Schritt zurück zu gehen, so dass im Fehlerfall der Benutzer die Registrierung von Anfang an erneut durchlaufen muss. Die Komponenten des Registrierungssystems und deren Kommunikationsverbindungen sind in Abbildung 9.3 dargestellt.

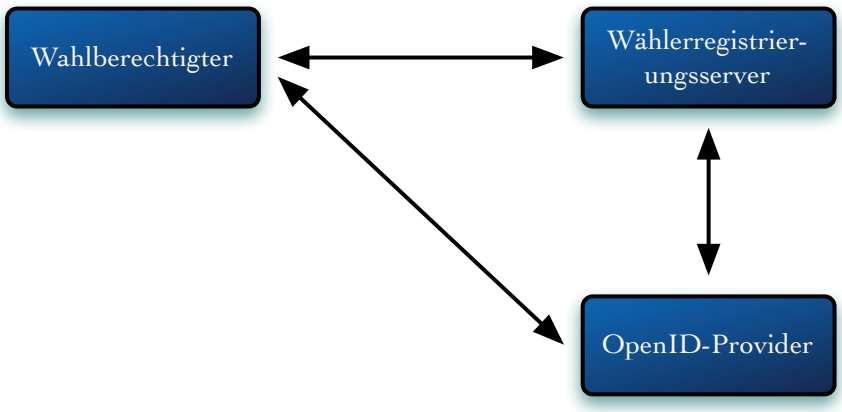

Abbildung 9.3: Kommunikation der Komponenten des Registrierungssystems

9.6.1 Anmeldung am Wählerregistrierungsserver

Im ersten Schnitt meldet sich der Teilnehmer mit seinen Zugangsdaten am Registrierungsserver an. Dabei werden seine Zugangsdaten und seine Wahlberechtigung geprüft. Die Abbildung 9.4 zeigt eine solche Anmeldung mit Benutzername und Passwort.

Abbildung 9.4: Anmeldung am Wählerregistrierungsserver

9.6.2 Eingabe der Wählerkennung

Im nächsten Schritt gibt der Wahlberechtigte seine Wählerkennung in Form eines OpenID-Identifiers ein. Der Identifier ist fest mit einer OpenID bei einem OpenID-Provider verbunden.

Es ist nicht erlaubt eine *OpenID-Delegation* zu verwenden, da sie eine Art Alias für den OpenID-Identifier ist und das Wechseln des zugehörigen OpenID-Providers zum Identifier ermöglichen würde. In einem solchen Fall ist es möglich, einen Identifier mit einem zur Wahl zugelassenen Provider zur Registrierung und später mit einem anderen zu Verknüpfen. Dies würde allerdings beim Wahlvorgang auffallen, da dort erneut die Zulassung des OpenID-Providers geprüft wird. Sollte der Wahlberechtigte den Identifier einer delegierten OpenID eingeben, dann würde er zur Fehlerseite mit dem entsprechenden Hinweis wie in Abbildung 9.12 dargestellt weitergeleitet.

Der eingegebene OpenID-Identifier wird als Wählerkennung für den Wahlberechtigten vorgemerkt. Die Abbildung 9.5 zeigt ein Eingabeformular mit dem spezifizierten Symbol für einen OpenID-Identifier.

Nachdem der Wahlberechtigte seinen Identifier eingeben hat, wird geprüft, ob dieser gültig ist und zu einem für die Wahl zugelassenem OpenID-Provider gehört.

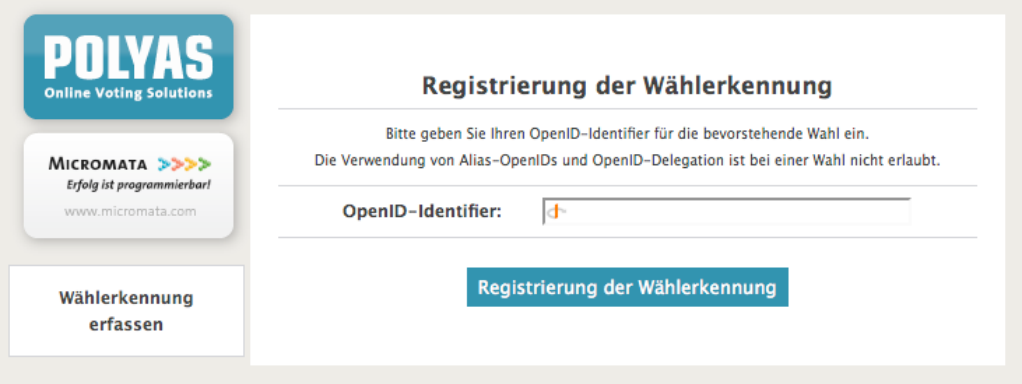

Abbildung 9.5: Registrierung der Wählerkennung (OpenID-Identifier)

9.6.3 Bestätigung der OpenID-Zugehörigkeit

Als nächstes muss der Wahlberechtigte nachweisen, dass der Identifier seiner OpenID ihm gehört. Dazu wird er aufgefordert, sich mit seiner OpenID zu authentifizieren.

Für den Nachweis kann als weiterer Faktor eine *VerifyTAN* verwendet werden. Diese Entscheidung wurde vor dem Start der Registrierungsphase festgelegt.

Ohne VerifyTAN

Ohne *VerifyTAN* wird dem Wahlberechtigten der Dialog, wie in Abbildung 9.6 dargestellt, angezeigt. Mit einem Klick auf „OpenID verifizieren“ wird er automatisch zu seinem OpenID-Provider weitergeleitet. Hierfür wird der von ihm angegebene OpenID-Identifier verwendet.

Abbildung 9.6: Bestätigung der OpenID ohne *VerifyTAN*

Mit VerifyTAN

Bei einer Registrierung mit *VerifyTANs* wurde nach der erfolgreichen Prüfung des OpenID-Identifiers dem Wahlberechtigten seine *VerifyTAN* auf einen anderen Kanal übermittelt. In diesem Beispiel wurde sie per E-Mail an den Wahlberechtigten versendet. Die E-Mail-Adresse wurde vom Wahlveranstalter beim Registrierungsdienst vor dem Start der Registrierungsphase hinterlegt, so dass bei der Registrierung diese zur Verhinderung von Missbrauch nicht geändert werden kann.

Der Wahlberechtigte wird wie in Abbildung 9.7 dargestellt darüber informiert, dass ihm eine *VerifyTAN* per E-Mail übermittelt wurde und dass er diese zur Verifizierung seiner OpenID nach der Authentifizierung mittels OpenID angeben muss.

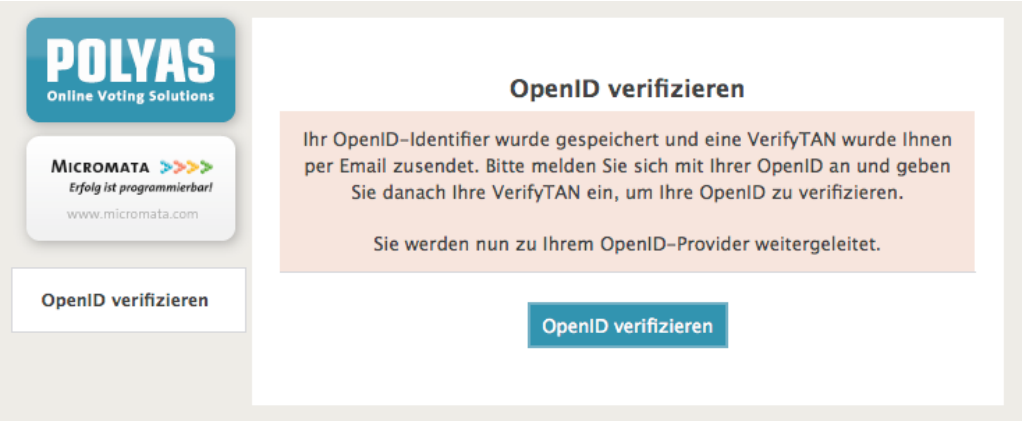

Abbildung 9.7: Bestätigung der OpenID mit *VerifyTAN*

9.6.4 Anmeldung beim OpenID-Provider

Der Wahlberechtigte wird automatisch zur Anmeldeseite von seinem OpenID-Provider geleitet, falls er sich nicht schon vorher dort angemeldet hat und die Anmeldung noch gültig ist. In diesem Fall würde der Anmeldeschritt ausgelassen und er sofort zur Freigabeseite von seinem OpenID-Provider geleitet. In Abbildung 9.8 wird eine Anmeldung mit Passwort gezeigt.

9.6.5 Freigabe beim OpenID-Provider

Nach der Anmeldung beim OpenID-Provider wird der Wahlberechtigte von seinem OpenID-Provider gefragt, ob er seine OpenID mit dem angegebenen OpenID-Identifier

Abbildung 9.8: Anmeldung beim OpenID-Provider mit Passwort

für die Authentifizierung beim Wählerregistrierungsserver freigeben möchte. Diese Freigabe kann erlaubt, verweigert oder dauerhaft erlaubt werden. Wenn eine dauerhafte Erlaubnis vorliegt, dann wird dieser Dialog wie in Abbildung 9.9 dem OpenID-Besitzer nicht gezeigt und er wird automatisch zum nächsten Schritt weitergeleitet. Eine dauerhafte Erlaubnis kann jederzeit vom Benutzer beim OpenID-Provider zurückgenommen werden.

Abbildung 9.9: Freigabe der OpenID-Authentifizierung zur Bestätigung

Nach der Anmeldung und Freigabe bei seinem OpenID-Provider wird der Wahlberechtigte automatisch zum Wählerregistrierungsserver weitergeleitet.

9.6.6 Eingabe der VerifyTAN

Wenn bei der Wählerregistrierung eine *VerifyTAN* verlangt wird, dann wurde dem Wahlberechtigten, wie in Abbildung 9.7 gezeigt, diese über einen unabhängigen Kanal zugestellt. Diese muss er nun in ein Formular, wie in Abbildung 9.10 dargestellt, eingeben. Zur Sicherheit wird ihm dabei sein von ihm angegebener OpenID-Identifier angezeigt.

Falls keine *VerifyTANs* genutzt werden, wird dieser Schritt ausgelassen.

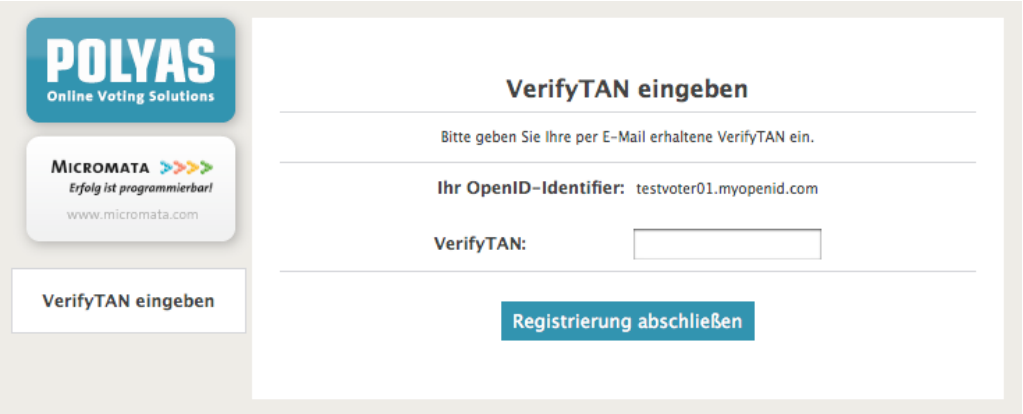

Abbildung 9.10: Eingabeseite für *VerifyTAN*

9.6.7 Abschluss der Registrierung der Wählerkennung

Im letzten Schritt, nachdem alle Prüfungen erfolgreich abgeschlossen wurden, wird der OpenID-Identifier des Wahlberechtigten so verschlüsselt, dass nur das Tool zur Erstellung des Wählerverzeichnisses diesen entschlüsseln kann. Dem Wahlberechtigten wird die erfolgreiche Registrierung seiner Wählerkennung mit einer Abschlussseite, wie in Abbildung 9.11 dargestellt, mitgeteilt. Für ihn ist die Registrierungsphase abgeschlossen und er kennt seine Wählerkennung für die Wahl, ohne dass diese ihm übermittelt werden musste.

Der Wahlveranstalter kann festlegen ob eine bereits erfasste Wählerkennung durch eine neuerfasste ersetzt werden darf. Seine Entscheidung wird den Wahlberechtigten mit allen weiteren für die Wahl wichtigen Informationen vor dem Start der Wählerregistrierungsphase mitgeteilt. Ist es den Wahlberechtigten erlaubt, ihre Wählerkennung während der Registrierungsphase zu ändern, dann müssen sie alle Schritte wie beim ersten Mal durchlaufen. Sollte ein Wahlberechtigter versuchen seine Wählerkennung zu ändern, obwohl es ihm untersagt ist, dann erhält er eine Fehlermeldung erst nach der Bestätigung der neuen OpenID-Zugehörigkeit. Dies

dient als Schutz, damit es in diesem Szenario keinem Teilnehmer möglich ist durch Angeben von OpenID-Identifiern, deren Wahlzugehörigkeit zu prüfen.

Abbildung 9.11: Abschlussseite der Wählerregistrierung

9.6.8 Bei Fehlern

Sollte in einem der Schritte ein Fehler beispielsweise durch fehlende Anmeldung beim OpenID-Provider oder Verwendung eines *delegierten OpenID-Identifiers* auftreten, dann wird dieser dem Benutzer mit einer Fehlerseite, wie in Abbildung 9.12 dargestellt, mitgeteilt. Er muss dann seine Registrierung vom ersten Schritt an erneut beginnen. Eine vergebene *VerifyTAN* ist aus Sicherheitsgründen auch immer nur für einen Versuch gültig.

Abbildung 9.12: Fehlerseite bei der Wählerregistrierung

9.7 Wahlvorgang mit OpenID

In diesem Abschnitt wird der Wahlvorgang mit OpenID aus der Sicht des Wählers beschrieben. Der Wähler nutzt dabei seine OpenID mit dem zugehörigen OpenID-Identifier, den er während der Registrierungsphase als seine Wählerkennung angegeben hat, um sich gegenüber dem Wahlsystem zu authentifizieren. Die Komponenten des Online-Wahlsystems mit deren Kommunikationsverbindungen, die während der Wahl verwendet werden, sind in Abbildung 9.13 dargestellt.

Wie bei der Registrierung der Wählerkennungen, wird auch beim folgenden Ablauf, falls nicht explizit anderes beschrieben, davon ausgegangen, dass jeder Schritt erfolgreich durchlaufen wird. Bei einer falschen Eingabe des Benutzers, fehlender Wahlberechtigung oder einem anderen Problem, wird dem Wähler eine Fehlerseite mit einer entsprechenden Fehlermeldung angezeigt. Aus Sicherheitsgründen ist es nicht möglich, einen Schritt zurück zu gehen, so dass im Fehlerfall der Wähler seinen Wahlvorgang beginnend mit Anmeldung erneut durchlaufen muss. Selbstverständlich ist es dem Wähler möglich, während eines korrekten Wahlvorgangs seine Stimmabgabe zu korrigieren, solange er seinen Stimmzettel nicht verbindlich abgegeben hat.

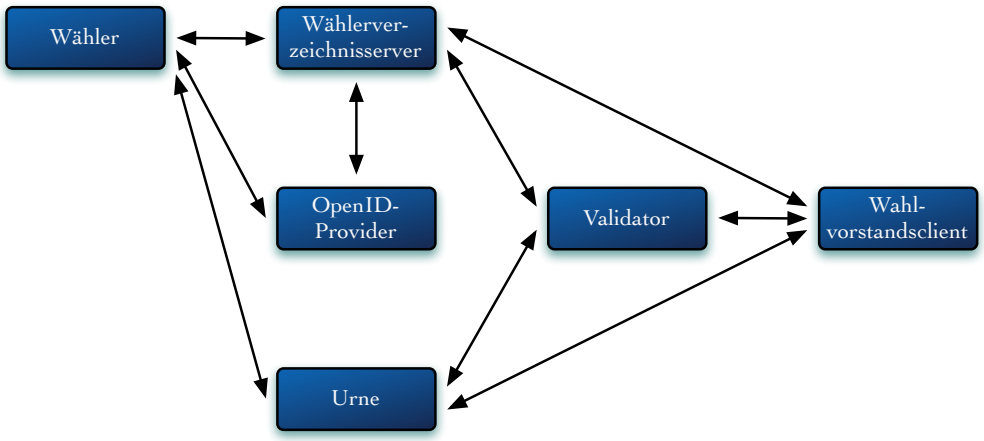

Abbildung 9.13: Kommunikation der Komponenten des Online-Wahlsystems

9.7.1 Anmeldung mit OpenID

Nach dem Aufrufen der Startseite des Wahlsystems sieht der Wähler das in Abbildung 9.14 dargestellte Eingabeformular für seine OpenID-Anmeldung. Dort gibt er seinen bereits für den Wahl registrierten OpenID-Identifier an, um sich am Wahlsystem anzumelden.

Abbildung 9.14: Anmeldung am Wählerverzeichnisserver mit OpenID

9.7.2 Anmeldung beim OpenID-Provider

Nachdem er seinen OpenID-Identifier übertragen hat, wird er automatisch für die Authentifizierung zu seinem OpenID-Provider weitergeleitet. Dort gibt er dann die Zugangsdaten für seine OpenID an. In Abbildung 9.15 ist beispielhaft eine Anmeldung mit einem Browser-Zertifikat gezeigt.

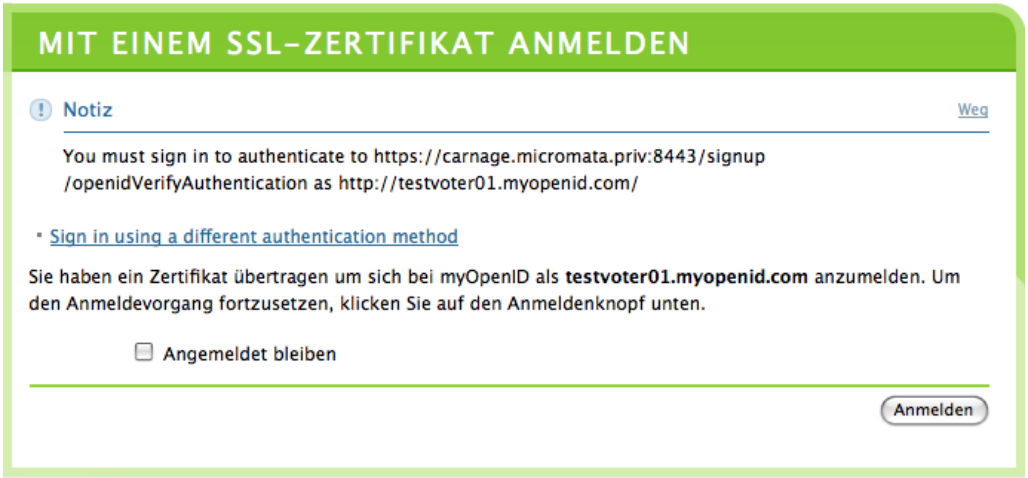

Abbildung 9.15: Anmeldung beim OpenID-Provider mit SSL-Zertifikat

9.7.3 Freigabe beim OpenID-Provider

Folgend erlaubt der OpenID-Besitzer die Verwendung seiner OpenID für die Authentifizierung beim Wählerverzeichnisserver. Die Abbildung 9.16 zeigt die Freigabeseite

des OpenID-Providers *myOpenID*.

Abbildung 9.16: Freigabe der OpenID-Authentifizierung am Wählerverzeichnisserver

9.7.4 Eingabe Wählerpasswort

Nachdem seine Authentifizierung vom Wählerverzeichnis erfolgreich verifiziert wurde, gelangt er, je nachdem, ob bei der Wahl Wählerpasswörter eingesetzt werden oder nicht, zur Eingabeseite für sein Wählerpasswort oder direkt zur nachfolgenden Hinweisseite. Diese Seiten zeigen in den Abbildungen 9.17 und 9.18.

Abbildung 9.17: Eingabeseite für Wählerpasswort

9.7.5 Anmeldung erfolgreich

Zu diesem Zeitpunkt hat sich der Wähler erfolgreich am Wählerverzeichnisserver angemeldet. Es wurde die Zulassung seines OpenID-Providers und seine Authentifizierung beim OpenID-Provider sowie, falls vergeben, sein Wählerpasswort geprüft. Weiterhin wurde anhand seines Eintrags im Wählerverzeichnis geprüft, dass er noch nicht verbindlich gewählt hat.

Ihm wurde automatisch ein Wahltoken übermittelt, mit dem er sich bei der Urne zum Erhalt eines Stimmzettels anmelden kann. Weiterhin wurden alle Session-Informationen inklusive der Session gelöscht. Jetzt hat der Wähler nur noch ein Wahltoken, so dass von dem Wahltoken nicht auf ihn über seine vorher eingegebenen Informationen geschlossen werden kann. Wenn er auf den Button „Weiter zur Wahl“ klickt, wird sein Wahltoken an den Urnenserver übermittelt und er dorthin weitergeleitet. Das Wahltoken dient als Authentifizierungsmerkmal am Urnenserver und ist mit keinen anderen Informationen verbunden.

Die Abbildung 9.18 zeigt die Webseite mit dem Hinweis der erfolgreichen Anmeldung und dem Button zum Urnenserver.

Abbildung 9.18: Anmeldung erfolgreich - Link zum Stimmzettel

9.7.6 Stimmzettel ausfüllen

Der Urnenserver überprüft das mitgesendete Wahltoken. Ist dieses gültig, erhält der Wähler einen Stimmzettel und kann mit der Stimmabgabe beginnen. In Abbildung 9.19 ist beispielhaft ein leerer Stimmzettel dargestellt. Nach dem Ausfüllen wird er zur nächsten Seite weitergeleitet.

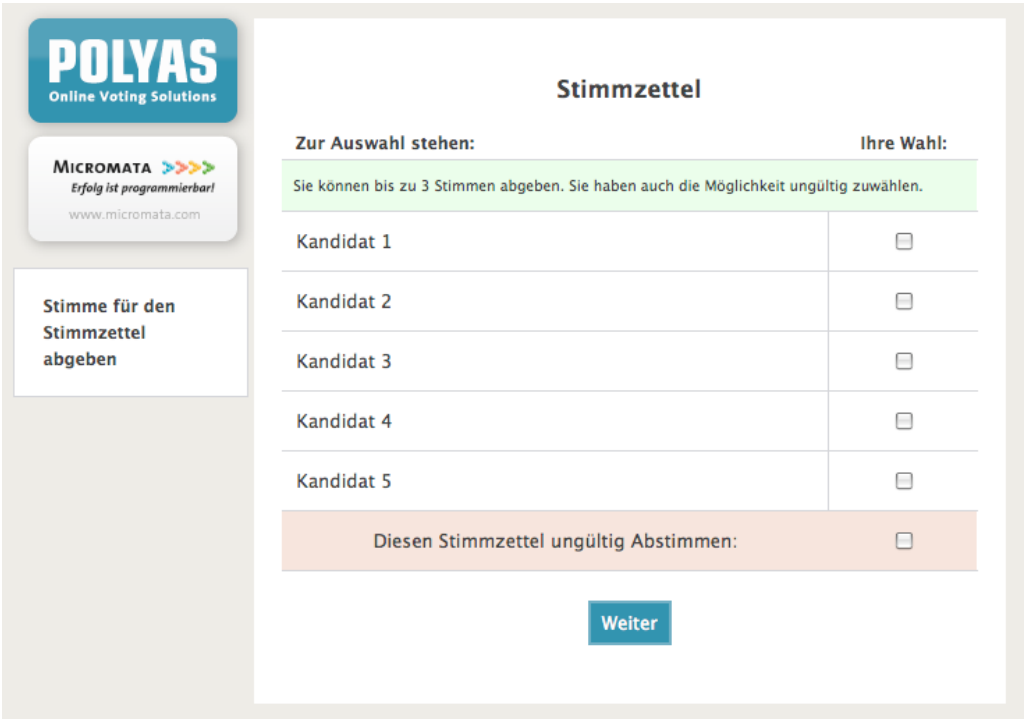

Abbildung 9.19: Stimmzettel

9.7.7 Verbindliche Stimmabgabe

Nachdem der Wähler seine Wahl getroffen hat, wird ihm sein ausgefüllter Stimmzettel angezeigt. Dies dient als *Übereilungsschutz*, so dass der Wähler nicht aus Versehen eine falsche Auswahl getroffen hat und diese abgibt.

Er kann seinen Stimmzettel korrigieren, verbindlich abgeben oder seinen Wahlvorgang unterbrechen. Nach einer Unterbrechung muss er sich jedoch erneut am Wählerverzeichnis, wie beim ersten Mal, anmelden. Er kann seinen Stimmzettel solange korrigieren, bis er ihn verbindlich abgibt. Durch eine verbindliche Stimmabgabe gelangt er zur Folgeseite.

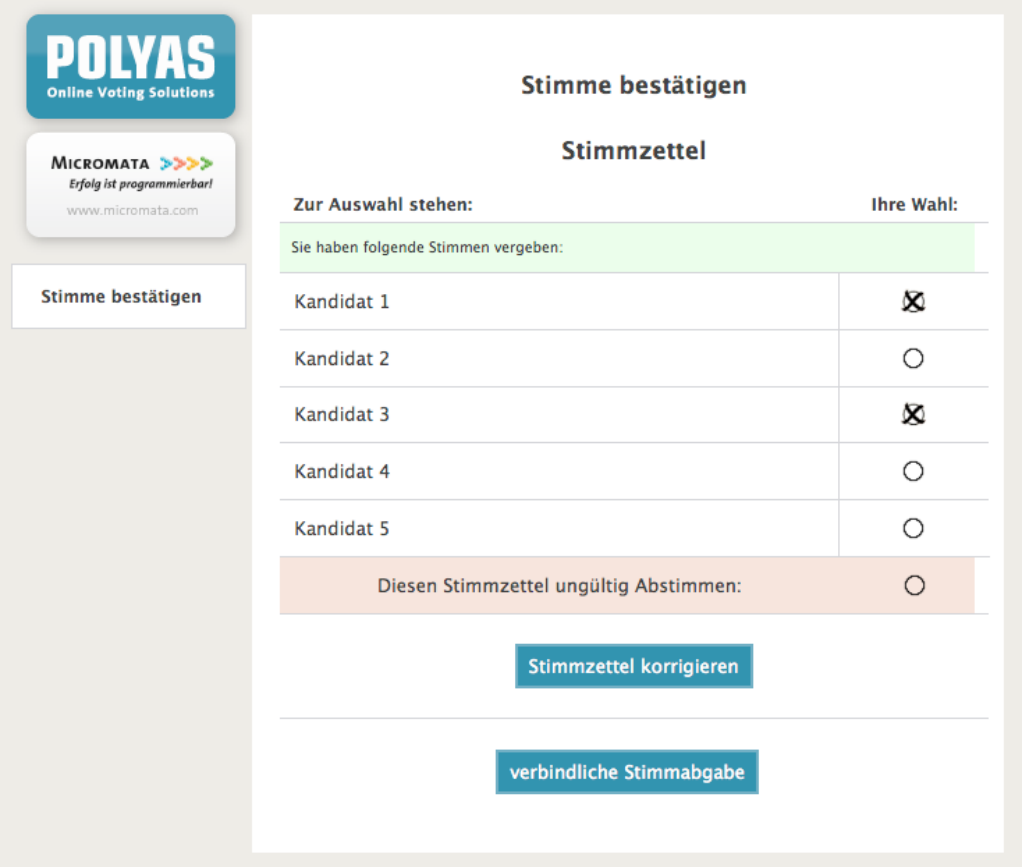

Abbildung 9.20: Stimmzettel verbindlich abgeben

9.7.8 Wahlvorgang beendet

Wenn der Wähler seine Stimme verbindlich abgegeben hat, ist für ihn der Wahlvorgang beendet und er verliert automatisch seine Wahlberechtigung. Eine erneute Stimmabgabe ist damit ausgeschlossen ist. Er bekommt eine wie in Abbildung 9.21 dargestellt Abschlussseite angezeigt.

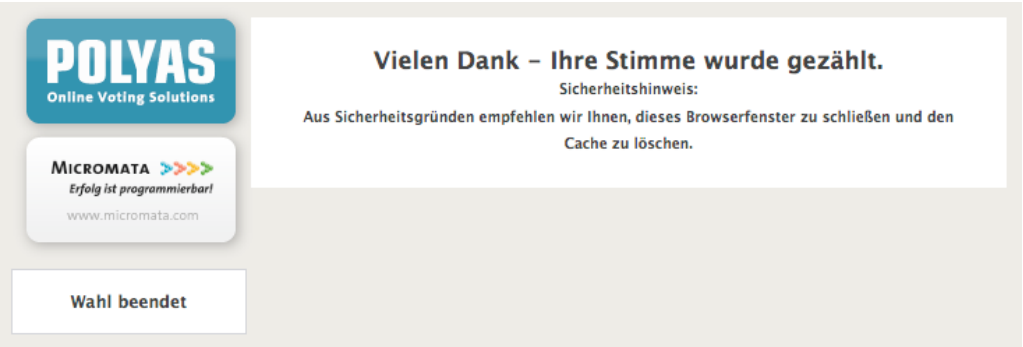

Abbildung 9.21: Wahlvorgang abgeschlossen

9.7.9 Bei Fehlern

Wenn in einem der Schritte ein Fehler, beispielsweise durch fehlende Anmeldung bei OpenID-Provider oder Verwendung eines *delegierten OpenID-Identifiers* auftritt, dann wird dieser dem Benutzer durch eine Fehlerseite mitgeteilt. Er muss dann seinen Wahlvorgang vom ersten Schritt an erneut beginnen. Die Abbildung 9.22 zeigt eine solche Fehlerseite.

Abbildung 9.22: Fehlerseite bei dem Wahlvorgang

10 Fazit & Ausblick

10.1 Fazit

In dieser Arbeit wurde gezeigt, wie externe Authentifizierungsdienste die Identitätsprüfungen der Wahlberechtigten übernehmen können. Durch den Einsatz des offenen Standards OpenID kann die Sicherheit bei der Authentifizierung auf ein hohes Niveau gebracht werden. Es kann jeder Wahlberechtigte selbst oberhalb des vom Wahlveranstalter vorgegeben Levels an Sicherheit, die eigene Sicherheit bei der Authentifizierung noch weiter erhöhen. Beispielsweise kann ein Wahlberechtigter eine Multi-Faktor-Authentifizierung für seine Anmeldung beim Wahlvorgang festlegen, auch für den Fall, dass der Wahlveranstalter nur ein Authentifizierungsmerkmal vorschreibt. Auch die Verwendung von SSL-Client-Zertifikaten, Smardcards, Biometrie oder Ähnlichem ist erlaubt. Ein Wahlberechtigter kann für die Authentifizierung bei seinem OpenID-Provider seine biometrischen Merkmale als ersten Faktor und sein Telefon samt einer geheimen PIN zur Bestätigung als weitere Faktoren verwenden. Somit sind für die Authentifizierung beim OpenID-Provider biometrische, besitz- und wissensbasierte Merkmale nötig. Dies führt zu einer extrem sicheren Authentifizierung, die in dieser Qualität nicht nur für ein Online-Wahlsystem sehr selten ist. Der Wahlberechtigte kann selbst Einfluss auf die Qualität seiner Authentifizierung nehmen, wird aber nicht gezwungen, sich bestimmte Hard- oder Software zu beschaffen. Die Minimalanforderung für den Wahlvorgang ist nur ein Browser mit Internetzugang.

Durch die benutzerzentralisierte Technologie OpenID ist der Wahlberechtigte in den Authentifizierungsvorgang bei der Wahl direkt eingebunden. Er selbst authentifiziert sich an einer von ihm gewählten Stelle mit den von ihm gewählten Authentifizierungsmerkmalen. Dies erhöht das Vertrauen in die Authentifizierung und schafft mehr Transparenz beim Vorgang.

Weiterhin wurde gezeigt, wie sehr der einzelne Wahlberechtigte auf die Geheimhaltung seines Wahlverhaltes Einfluss nehmen kann. Durch eine sorgfältige Auswahl seines OpenID-Identifiers kann der Wahlberechtigte seine Wählerkennung so wählen, dass sie keinen Rückschluss auf seine Person ermöglicht. Somit ist seine Wahlbeteiligung auf jeden Fall geheim. Im Gegensatz zu einer Brief- oder Präsenzwahl erhält niemand einen Umschlag mit seinem Namen oder kann den Wähler auf dem Weg zur Urne

beobachten. Da das Wahlsystem von ihm nur den OpenID-Identifier kennt, könnte selbst im Fall einer Manipulation sein Stimmzettel nicht seiner Person zugeordnet werden. Für den Wahlberechtigten ist die Trennung zwischen der Authentifizierung und der Stimmabgabe klar sichtbar.

Die Überprüfbarkeit einer Wahl ist bei einer Distanzwahl generell und schon alleine aufgrund des verteilten Vorgangs zwischen Stimmabgabe und Auszählung der Stimme schlechter als bei einer klassischen papierbasierten Urnenwahl. Die hier vorgestellte Lösung stellt aber im Vergleich zu einer papierbasierten Briefwahl eine Verbesserung dar. Der Wähler kann zwar nicht direkt den Weg seines Stimmzettels verfolgen, aber im Gegensatz zum Postweg erhält er eine Fehlermeldung, falls bei der Übermittlung ein Problem aufgetreten ist. Auch kann der Wähler bei dieser Lösung erkennen, ob seine Stimme gezählt wurde. Dabei ist es durch den Einsatz von OpenID nur ihm möglich, diese Information zu gewinnen. Er kann auch erfahren, wie viele Stimmen verbindlich abgegeben wurden, da er bei einem Einblick in das Wählerverzeichnis sehen kann, mit welchem OpenID-Identifier gewählt wurde. Dies ist selbst bei einer klassischen Urnenwahl in einem Wahllokal nicht möglich, da dort aus Datenschutzgründen der Einblick in das Wählerverzeichnis verweigert wird. Somit kann jeder, der Einblick in die Dokumentation der Wahl haben darf, erkennen, wie viele Stimmen abgeben wurden und ob diese Anzahl den ausgezählten Stimmen entspricht. Der Wähler muss sich nicht blind auf die Zuverlässigkeit der Übermittlung bei der papierbasierten Stimme verlassen.

Für die Erfassung der Wählerkennungen wurde ein Online-System neu entwickelt. Mit Hilfe dieses Systems können die Wahlberechtigten ihre OpenID-Identifier angeben, die als Wählerkennung verwendet werden sollen. Daher ist die Verbindung zwischen ihrer Person und ihrer Wählerkennung nur ihnen und dem Wählerregistrierungsserver bekannt. Das System stellt bei der Erfassung sicher, dass die Identität des Teilnehmers stimmt, prüft automatisch dessen Wahlberechtigung und dessen OpenID-Identifier und OpenID-Provider. Weiterhin wird die Bindung zwischen dem Wahlberechtigten und seinem OpenID-Identifier geprüft, um sicher zu stellen, dass es auch seiner ist. Durch den Wählerregistrierungsserver brauchen keine Zugangsdaten mehr versendet zu werden, wodurch die Kosten für PIN-Briefe eingespart werden. Daher können auch keine Zugangsdaten auf dem Weg zum Wahlberechtigten abgefangen, manipuliert oder kopiert werden. Die Authentifizierungsmerkmale legt der Wahlberechtigte mit seinem OpenID-Provider fest, so dass sie das Wahlsystem nie erfährt. Desweiteren wird durch die Online-Erfassung der OpenID-Identifier sichergestellt, dass keine Tippfehler unbemerkt bleiben und dass der Wahlberechtigte seine OpenID auch verwenden kann. Zusätzlich ist nach dem Abschluss der Registrierungsphase die genaue Anzahl der Wahlberechtigten für die Online-Wahl bekannt.

Da alle Komponenten des Online-Wahlsystems genauso wie die OpenID-Provider nur einen Browser mit Internetzugang voraussetzen, erhöht sich die Barrierefreiheit.

Die OpenID-Provider haben einen direkten Einfluss auf die Sicherheit der Wahl. Daher wurde eine Möglichkeit entwickelt, nur bestimmte OpenID-Provider für die Online-Wahl zuzulassen. Diese Einschränkung ist optional, so dass der Wahlveranstalter entscheiden kann, ob er die Auswahl der OpenID-Provider alleine seinen Wahlberechtigten überlassen möchte, oder ob er eine Vorauswahl festlegt. Für die Entscheidung, welche OpenID-Provider zugelassen werden sollten, wurden Auswahlkriterien beschrieben. Durch den Wählerregistrierungsserver wird sichergestellt, dass nur OpenID-Identifier von OpenID-Providern erfasst werden, die auch beim späteren Wahlvorgang verwendet werden dürfen. Sollte ein Wahlberechtigter einen nichtzugelassenen OpenID-Provider verwenden wollen, dann wird es ihm automatisch bei der Erfassung seines Identifiers mitgeteilt, so dass er in Ruhe einen anderen OpenID-Provider auswählen kann.

Für den Fall, dass bei einer Wahl die Authentifizierung nicht alleine den OpenID-Providern überlassen werden soll, können zusätzliche Wählerpasswörter verwendet werden. Es wurde eine Verfahren beschrieben, wie die Wählerpasswörter erstellt und an die Kontaktdaten der Wahlberechtigten zugestellt werden können, ohne dass das Wahlsystem die Kontaktdaten erfährt. Daher ist es auch beim Einsatz von zusätzlichen Wählerpasswörtern dem Wahlsystem nicht möglich, Rückschlüsse von den Wählerkennungen auf die zugehörigen Wahlberechtigten zu ziehen.

Da die OpenID-Provider von dem Wahlsystem unabhängig arbeiten, ist deren Sicherheit und Funktion nicht vom Wahlsystem beeinflusst. Würde ein Angreifer mit den OpenIDs der Wahlberechtigten wählen wollen, dann müsste er jeden bei der Wahl benutzten OpenID-Provider angreifen. Allein durch die Anzahl der unabhängigen OpenID-Provider erscheint ein solcher Angriff als sehr unwahrscheinlich.

Neben der Beschreibung eines Verlaufs einer solchen Online-Wahl wurde deren Realisierbarkeit mit einer Referenzimplementierung nachgewiesen. Dazu wurde ein Wählerregistrierungsserver neu implementiert und ein bestehendes Online-Wahlsystem erweitert. Somit wurde nachgewiesen, dass die Anbindung externer Authentifizierungsdienste an ein Online-Wahlsystem möglich ist und die beschriebenen Vorteile bringt.

10.2 Ausblick

Die Nachfrage nach Online-Wahlen wächst. Immer mehr Unternehmen, Gesellschaften und Vereine entdecken die Vorteile von Online-Wahlen. Während in der Politik die Verwendung von Online-Wahlen stark umstritten ist, kommen Interessierte verstärkt aus der Wirtschaft. In naher Zukunft sollen Stimmabgaben bei Hauptversammlungen auch online möglich sein. Gerade bei Wahlen mit sehr vielen Wahlberechtigten, die

sich an unterschiedlichen Orten aufhalten, bietet eine Online-Wahl eine komfortable Möglichkeit zur Wahlteilnahme. Ein sicheres Online-Wahlsystem, das dem Benutzer eine Überprüfbarkeit seiner Wahlteilnahme ermöglicht und gleichzeitig dessen Identität geheim hält, ist sicher ein Schritt in die richtige Richtung.

Die Verbreitung von OpenID nimmt ständig zu. Immer mehr Webdienste ermöglichen eine Authentifizierung mittels OpenID und auch die Anzahl der OpenID-Provider steigt kontinuierlich. Besonders der Anschluss großer Unternehmen wie *Microsoft*, *Sun Microsystems* und *Google* mit starker Webpräsenz führte in den letzten Monaten zur schnellen Verbreitung von OpenID. Der offene Standard von OpenID wird ständig weiterentwickelt, so dass immer mehr Anwendungsbereiche hinzugenommen werden. Vielleicht werden bald viele Internetnutzer statt unzähligen Benutzernamen und Passwörtern eine OpenID haben. Einige haben sicher jetzt schon eine, ohne dies bemerkt zu haben. Die Webseite der *OpenID Foundation* [Ope] überrascht den OpenID-Suchenden mit dem Satz: „*Surprise! You may already have an OpenID.*“

Literaturverzeichnis

[AE07] Ammar Alkassar and Melanie Volkamer (Eds.). *E-Voting and Identity*. Springer, 2007.

[Ath] Massachusetts Institute of Technology. *Athena at MIT*. `http://ist.mit.edu/services/athena`.

[Ber02] Andreas Bertsch. *Digitale Signaturen*. Springer, 2002.

[Buc01] Johannes Buchmann. *Einführung in die Kryptographie*. Springer, 2001.

[Bun08] Bundesamt für Sicherheit in der Informationstechnik. *Common Criteria Schutzprofil - Basisansatz von Sicherheitsanforderungen an Online-Wahlprodukte*. Number BSI-PP-0037. Februar 2008.

[Bun09] Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2009*. `https://www.bsi.bund.de/cae/servlet/contentblob/476182/publicationFile/30725/Lagebericht2009_pdf.pdf`, 2009.

[BVe] *Urteil des Zweiten Senats vom 3. März 2009, 2 BvC 3/07, 2 BvC 4/07*. `http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html`.

[CC] Common Criteria for Information Technology Security Evaluation. `http://www.commoncriteriaportal.org`.

[Cor07] Corporate Trust, Claudia Tödtmann, Bärber Bongartz. *Studie: Industriespionage - Die Schäden durch Spionage in der deutschen Wirtschaft*, 2007.

[D21] Initiative D21. `http://www.initiatived21.de/`.

[DFG] Deutsche Forschungsgemeinschaft DFG. `http://www.dfg.de/`.

[dot] dotVote GbR. *dotVote - Digitales Wahlstift-System*. `http://www.dotvote.de`.

[Eck05] Claudia Eckert. *IT-Sicherheit Studienausgabe. Konzepte - Verfahren - Protokolle*. Oldenbourg, 2005.

[Fin] Finnish Youth Cooperation Allianssi. *YOUTH Election*. `http://www.alli.fi/`.

[Gar03] Jason Garman. *Kerberos. The Definitive Guide*. 2003.

[GG] *Grundgesetz für die Bundesrepublik Deutschland*. `https://www.btg-bestellservice.de/pdf/10060000.pdf`.

[GI] Gesellschaft für Informatik e.V. `http://www.gi-ev.de/`.

[Gri03] Dimitris A. Grizalis. *Secure Electronic Voting*. Kluwer Academic Publishers, 2003.

[GwG] *Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG)*. `http://bundesrecht.juris.de/bundesrecht/gwg_2008/gesamt.pdf`.

[Hag03] Axel Hagedorn. *Distributed Denial of Service - Angriffswerkzeuge und Abwehrmöglichkeiten*. TU Darmstadt, 2002/2003.

[Her08] Hanmer Herrnson, Niemi. *Voting Technology*. Brookings, 2008.

[HK05] J. K. Hodge and R. E. Klima. *The Mathematics of Voting and Elections: A Hands-On Approach*. American Mathematical Society, 2005.

[Jan] JanRain - OpenID. `http://www.janrain.com/openid`.

[Joa06] Joaquin Miller, editor. *Yadis Specification - Version 1.0*. 2006.

[Ker] Massachusetts Institute of Technology. *Kerberos: The Network Authentication Protocol*. `http://web.mit.edu/kerberos/`.

[Kum] Kumulus e.V. *Juniorwahl*. `http://www.juniorwahl.de/`.

[Men08] Niels Menke. *Sicherheit elektronischer Wahlsysteme am Beispiel des Online-Wahlsystems Polyas*. Universität Kassel, 2008.

[Mic07] Micromata GmbH. *Polyas Sicherheitskonzept mit technischer Dokumentation*. Internes Dokument, 2007.

[myO] JanRain, Inc. *myOpenID*. `https://www.myopenid.com`.

[Ned] Nedap Election Systems. *Nedap*. http://www.election-systems.eu.

[OA1] OpenID Foundation. *OpenID Authentication 1.1*. http://openid.net/specs/openid-authentication-1_1.html.

[OA2] OpenID Foundation. *OpenID Authentication 2.0*. http://openid.net/specs/openid-authentication-2_0.html.

[Ope] OpenID Foundation. http://openid.net/.

[Pho] PhoneFactor, Inc. *PhoneFactor*. http://www.phonefactor.com.

[Pol] Micromata GmbH. *Polyas*. http://www.polyas.de.

[Pos] Deutsche Post AG. http://www.deutschepost.de.

[Pre] Premier Election Solutions, Incorporated. *AccuVote*. http://www.premierelections.com.

[Reh08] Rafeeq Ur Rehman. *The OpenID Book - A comprehensive guide to OpenID protocol and running OpenID enabled web sites*. Conformix Technologies Inc., 2008.

[RSA] R.L. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. http://people.csail.mit.edu/rivest/Rsapaper.pdf.

[Sch06] Bruce Schneier. *Angewandte Kryptographie*. Pearson Studium, 2006.

[Sec08] Secunia. *Secunia Monthly Report, October 2008*. https://secunia.com/, 2008.

[Sid06] Sid Stamm, Zulfikar Ramzan, Markus Jakobsson. *Drive-By Pharming*. Indiana University, Bloomington and Symantec, Inc., 2006.

[Sig01] Bundesministeriums der Justiz and juris GmbH. *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)*. http://bundesrecht.juris.de/bundesrecht/sigg_2001/gesamt.pdf, 2001.

[Tru] TrustBearer Labs. *TrustBearer OpenID - OpenID with Strong Authentication.* `http://openid.trustbearer.com`.

[VK05] Melanie Volkamer and Robert Krimmer. *Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In:* EGOV (Workshops and Posters). 2005.

[VK06] Melanie Volkamer and Robert Krimmer. *Die Online-Wahl auf dem Weg zum Durchbruch. Informatik Spektrum*, 29(2):98–113, 2006.

[Vol09] Melanie Volkamer. *Evaluation of Electronic Voting.* Springer, 2009.