

# i-voting

Genial einfaches Verfahren zum Wählen über das Internet vom eigenen Computer aus

## Beschreibung des Verfahrens

### Zusammenfassung

Das **i-voting**© Verfahren arbeitet mit Stimmzetteln in Form von **Intergrammen**, die mit einer **anonymen** digitalen Signatur unterzeichnet werden. Die Signatur wird mit einer **Signierdiskette** oder einer **Signierchipkarte** erzeugt. **i-voting** ist wählerfreundlich, transparent, sicher und preiswert.

Ein **Intergramm**© ⊗ ist eine vom Verfasser am Computer in Form einer "dreiteiligen digitalen Signatur©" unterschriebene und verschlüsselt über das Internet gesendete Mitteilung, die nur vom Empfänger selbst entschlüsselt werden kann. Die Echtheit der Signatur und die Unversehrtheit der Mitteilung werden durch einen Klick geprüft. Intergramme ermöglichen eine einfache und sichere Stimmabgabe über das Internet vom eigenen Computer aus.

Eine solche Internetwahl wird als **i-voting**© bezeichnet. Das Verfahren ermöglicht die Überprüfung des Wahlergebnisses durch den Wähler. Es läuft folgendermaßen ab:

- Vor der Wahl beantragt der Wähler, seine Stimmabgabe über das Internet zu tätigen. Die Gemeinde als Wahlbehörde prüft, ob der Antragsteller im Wählerverzeichnis aufgeführt ist und vermerkt dies.
- Der Internetwähler erhält von der Gemeinde eine nur für die Wahl bestimmte spezielle Signierdiskette oder Signierchipkarte, die zunächst noch nicht verwendbar ist. Außerdem erhält er einen Code, mit dem er seine Signier-Diskette/Chipkarte am heimischen Computer aktivieren kann, um Intergramme mit **anonymer** Signatur zu erzeugen.
- Diese **Wahldiskette** bzw. **Wahlchipkarte** und den Code kann er sich persönlich bei der Gemeinde an einem dort aufgestellten Kunden-Computer erzeugen. Eine Wahldiskette kann sich der Wähler auch am eigenen Computer herstellen, wenn er an einem von der Gemeinde betriebenen Intergramm-Dienst teilnimmt. Hierzu beantragt er die Zustellung per Intergramm von Datensatz und Code zum Anfertigen seiner Wahldiskette.
- Am Wahltag lädt sich der Internetwähler den elektronischen Stimmzettel auf seinen Computer, füllt am Bildschirm den Stimmzettel aus, authentisiert sich mit seiner Wahl-Diskette/Chipkarte, versieht den Stimmzettel durch einen Klick mit einer anonymen Signatur (Abbildung 1) und sendet ihn durch einen weiteren Klick verschlüsselt über das Internet an eine elektronische Wahlurne, in der alle eingehenden Internetstimmzettel gesammelt werden.
- Nach Wahlende authentisiert sich der Wahlleiter mit einer speziell für ihn angefertigten Signier-Diskette/Chipkarte am Computer des Wahllokals und

lädt durch einen Klick die elektronischen Stimmzettel aus der Wahlurne auf diesen Computer, wobei sie automatisch entschlüsselt werden.

- Die anonyme Signatur jedes Stimmzettels wird durch einen Klick verifiziert.
- Ungültig unterzeichnete Stimmzettel und solche mit Signaturen, die von demselben anonymen Unterzeichner stammen, werden vor der Auszählung der Stimmen ausgesondert.
- Die verifizierten Stimmzettel werden in eine elektronische Stimmzettelbox eingegeben (Abbildung 2) und ausgewertet. Dort kann jeder Interessierte ihre Echtheit anhand der anonymen Signatur und das Wahlergebnis anhand des zur Auswertung verwendeten Algorithmus prüfen.
- Außerdem können die elektronischen Stimmzettel ausgedruckt, zusammen mit den auf Papier ausgefüllten Stimmzetteln ausgewertet und für Kontrollzwecke aufbewahrt werden.

## Einleitung

Zu den Schwierigkeiten von Wahlen über das Internet gehören unter anderem:

- Authentisierung des Wählers
- Geheimhaltung der Stimmabgabe
- Integrität des Stimmzettels
- verlässliche Übermittlung und Aufbewahrung der Stimmzettel
- Ausschluss mehrfacher Stimmabgabe durch einen Wähler
- Absicherung gegen Angriffe auf die Hardware der Internetwahl

Die bisherigen Projekte einer Internetwahl versuchen, diesen Schwierigkeiten mehr oder weniger gut zu begegnen. Das deutsche Projekt “**i-vote**“ ⊗ ist beispielsweise einer Briefwahl nachempfundenen und basiert auf der konventionellen **asymmetrischen** digitalen Signatur. Es läuft etwa wie folgt ab: Zunächst verschlüsselt der Wähler seinen elektronischen Stimmzettel mit dem öffentlichen Schlüssel des Wahlleiters, signiert den verschlüsselten Stimmzettel mit seinem auf einer Chipkarte befindlichen privaten Schlüssel und schickt das Ergebnis an ein elektronisches Wahlamt. Dort wird die Signatur mit dem öffentlichen Schlüssel des Wählers und dessen Wahlberechtigung anhand der Wählerliste geprüft. Das Wahlamt entfernt die Originalsignatur und ersetzt sie durch seine eigene Signatur mit Hilfe seines eigenen privaten Schlüssels und übermitteln den so neuverschlüsselten Stimmzettel an eine elektronische Wahlurne. Deren Software prüft die Signatur des Wahlamts mit dem öffentlichen Wahlamtsschlüssel und speichert bei positiven Ergebnis den eingegangenen verschlüsselten Stimmzettel. Nach Ende der Wahl entschlüsselt der Wahlleiter alle in der Urne eingegangenen elektronischen Stimmzettel mit seinem privaten Schlüssel und macht das Ergebnis bekannt. Tatsächlich ist das i-vote-Protokoll noch etwas verwickelter.

Die wesentliche Schlussfolgerung aus dem Projekt i-vote besagt, dies Verfahren kann voraussichtlich nur von **öffentlichen Internetwahllokalen** aus durchgeführt werden. Dabei sollte wegen des technischen Ausfallrisikos

insgesamt etwa die doppelte Anzahl von Internetwahllokalen wie bisher bei konventionellen Wahlen mit Papier, Stift und Urne bereitgestellt werden. Das **i-vote**-Verfahren käme nur dann für eine Stimmabgabe vom eigenen Computer aus in Betracht, wenn die Sicherheitsanforderungen wesentlich herabgeschraubt werden. Der Hauptgrund hierfür ist die Rückverfolgbarkeit der Wähleridentität über den Internetanschluss des Computers.

Andere Ansätze für Internetwahlen mit Stimmabgabe vom eigenen Computer her setzen auf die Identifizierung des Wählers durch eine Geheimzahl, die ihm per Post oder verschlüsselt über das Internet zugestellt wird. Diese Methode entspricht weitgehend dem Telebanking oder anderen E-Business-Transaktionen, mit dem Unterschied, dass bei der Internetwahl das Ergebnis der Transaktion nicht direkt sichtbar wird und deshalb auch nicht geprüft werden kann. Erste Erfahrungen mit einem solchen System wurden im Januar 2003 in der Schweiz bei einer Volksabstimmung in der Gemeinde Anières im Kanton Genf gemacht. Bei dieser Abstimmung musste der Wähler neben seinem Votum zur Identifizierung eine 16-stellige Geheimzahl, einen weiteren Code und einige persönliche Daten in den elektronischen Stimmzettel eingeben, die mit den im Wahlserver gespeicherten Daten der Wählerliste verglichen wurden. In die elektronische Wahlurne gelangten nur die verschlüsselten Stimmzettel ohne Geheimzahl, Zusatzcode und persönlichen Daten.

Die technischen Probleme dieses Projekts gehen aus einem Bericht [⊗](#) der Projektleitung vom September 2002 hervor. Hauptschwachpunkte des Verfahrens sind - wie beim Projekt i-vote - die Sicherheitsrisiken und die fehlende demokratische Kontrolle infolge mangelnder Transparenz, die sich insbesondere dadurch ausdrückt, dass der Wähler die Transaktionen von der Abgabe seines Stimmzettels bis zur Auswertung nicht unmittelbar verfolgen kann.

Die bisherigen Projekte sind also noch nicht ausgereift. Vor allem sind sie aber nicht so einfach und transparent wie konventionelle Wahlen in der Wahlkabine. Berücksichtigt man die nicht unerheblichen Kosten für die Schaffung einer flächendeckenden Infrastruktur für Internetwahlen, so überrascht nicht, dass Bundestags- oder Europawahlen über das Internet nach den bisherigen Konzepten noch in weiter Ferne stehen.

### **i-voting**

Ein neues, **i-voting**© genanntes Verfahren, bei dem per **Intergramm**© [⊗](#) gewählt und die Identität des Wählers mit einer **anonymen** digitalen Signatur des Stimmzettels verifiziert wird, ist den bisher vorgeschlagenen Internet-Wahlmethoden, aber auch dem herkömmlichen Wahlverfahren, in Transparenz und Wählerfreundlichkeit überlegen.

Ein **Intergramm** ist eine vom Verfasser mit Hilfe einer Signier-Diskette/Chipkarte in Form einer "dreiteiligen digitalen Signatur©" unterschriebene und verschlüsselt über das Internet gesendete Mitteilung, die nur vom Empfänger selbst entschlüsselt werden kann. Die Echtheit der Signatur und die Unversehrtheit der Mitteilung werden durch einen Klick geprüft.

Die dreiteilige digitale Signatur eines Intergramms besteht aus drei Zahlen, beispielsweise:

72085 33172  
04381 80478  
42866 39105

Sie ist, im Gegensatz zur herkömmlichen asymmetrischen digitalen Signatur, leicht wahrnehmbar, so dass man sie zweckmäßigerweise zusammen mit dem Text auf dem Bildschirm zeigt und auf Papier ausdruckt. Die Bedeutung der drei Zahlen ist leicht zu verstehen:

- **die erste Zahl (Unterzeichnerkennung K) beantwortet die Frage: wer hat den Text erzeugt?** Sie kennzeichnet die Identität des Unterzeichners und ist für verschiedene Personen immer unterschiedlich. Sie berechnet sich aus den persönlichen Daten des Unterzeichners wie Name, Geburtstag, Geburtsort, oder wird als Zufallszahl erzeugt.
- **die zweite Zahl (Textsiegel S) beantwortet die Frage: um welchen Text handelt es sich?** Sie kennzeichnet die Identität eines Textes und ist für verschiedene Texte immer unterschiedlich. Sie berechnet sich mit einem öffentlichen Einwegalgorithmus als Hashwert aus allen Schriftzeichen des Textes und ihrer Anordnung.
- **die letzte Zahl (Unterschriftsbeweis U) beantwortet die Frage: wurde der Text tatsächlich vom Unterzeichner genehmigt?** Sie kennzeichnet die Tatsache, dass der Unterzeichner den Text aktiv gebilligt hat und ist für verschiedene Texte und für verschiedene Unterzeichner auch bei gleichem Text immer unterschiedlich. Sie berechnet sich als Transformation aus dem Textsiegel S mit einem geheimen (privaten) Einwegalgorithmus, der vorzugsweise durch eine **Geheimzahl G** definiert ist, unter alleiniger Kontrolle des Unterzeichners.

Durch ihre erste Zahl K definiert die normale dreiteilige digitale Signatur eine ganz bestimmte, den Empfängern von Intergrammen bekannte oder zumindest identifizierbare Person. Diese gewollte Kennzeichnung des Unterzeichners eines Intergramms entspricht vollkommen der Identitätsfunktion einer eigenhändigen Unterschrift. Der Unterzeichner erzeugt die dreiteilige digitale Signatur auf seinem Computer durch einen Klick, nachdem er sich mit einer eigens für ihn angefertigten Signier-Diskette/Chipkarte an seinem Computer authentisiert hat.

Für einen elektronischen Stimmzettel kommt diese normale dreiteilige digitale Signatur natürlich nicht infrage, denn spätestens beim Verifizieren der Signatur werden die Personalien des Unterzeichners offen gelegt, damit klar ist, wer unterzeichnet hat. Mit einer kleinen, jedoch entscheidenden Änderung, lässt sich das übliche Intergramm-Verfahren mit normaler Unterzeichnerkennung K an die Belange einer geheimen Internetwahl anpassen. Dies wird aus folgender Überlegung klar:

Die Daten zum Erzeugen der Signierdiskette jedes neuen Teilnehmers am üblichen Intergramm-Verfahren werden unter der Aufsicht einer diesem Verfahren eigenen vertrauenswürdigen Instanz vom System hergestellt, nachdem die Instanz sich von der Identität des neuen Teilnehmers überzeugt

hat. Nach dem Startbefehl erzeugt das System automatisch und von außen her nicht wahrnehmbar für den neuen Teilnehmer K- und G-Werte, die als Wertepaar K-G verschlüsselt in die Datenbank eines gegen äußere Einflüsse und Wahrnehmungen abgeschirmten autonomen Moduls (Internetserver) gelangen. Im gleichen Zug stellt das System eine zunächst noch nicht aktivierbare personalisierte Datei her, welche ebenfalls die K- und G-Werte enthält. Außerdem wird vom System ein Code zum Aktivieren dieser Datei erzeugt.

Wenn der neue Teilnehmer sich persönlich bei der vertrauenswürdigen Instanz vorstellt, kann er dort unmittelbar vom System den Code und die noch nicht aktivierbare personalisierte Datei auf einer Diskette oder Chipkarte erhalten. Falls sich die vertrauenswürdige Instanz ohne die persönliche Anwesenheit des Teilnehmers durch Zusendung beweiskräftiger Unterlagen von dessen Identität überzeugt, erhält der Teilnehmer den Code und die noch nicht aktivierbare personalisierte Datei auf getrennten Wegen, worauf er sich die Datei auf eine Diskette kopiert. Nach Eingabe des Codes verfügt der Teilnehmer über eine individuelle Signierdiskette zum Unterschreiben seiner Intergramme.

Die entscheidende Änderung dieses normalen Intergramm-Verfahrens in Hinsicht auf seine Nutzung für Internetwahlen (**i-voting**) liegt darin, die Unterzeichnerkennung K der dreiteiligen digitale Signatur nicht für jeden sichtbar mit der Person des Unterzeichners zu verknüpfen, sondern K als Zufallszahl zu erzeugen und vor jedermann geheim zu halten, abgesehen natürlich vom Eigentümer der Signier-Diskette/Chipkarte selbst. Die Authentizität von Intergrammen, deren Unterschrift einen solchermaßen **anonymen** K-Wert enthält, lässt sich durch Verifizieren genau so wie die eines Intergramms mit **normaler** Unterzeichnerkennung K sicher nachweisen.

Das i-voting-Verfahren kann vom heimischen Computer aus einfach, transparent, kostengünstig, zeitsparend und sicher organisiert werden. Als vertrauenswürdige Instanz, unter deren Aufsicht das System die Daten zur Herstellung der Signier-Disketten/Chipkarten erzeugt, fungiert die für den Stimmbezirk zuständige Wahlbehörde bzw. Gemeinde. Das autonome Modul in Form des gegen äußere Einflüsse und Wahrnehmungen abgeschirmten Internetserver kann dabei für viele Stimmbezirke gemeinschaftlich eingerichtet werden.

Internetwahlen auf Basis von i-voting laufen folgendermaßen ab: Rechtzeitig vor der Wahl lädt sich der zukünftige Internetwähler die Intergramm-Software aus dem Internet auf seinen Computer und besorgt sich bei seiner Gemeinde, die einen Intergramm-Server betreibt, nach Verifizierung der Identität des potenziellen Internetwählers, persönlich eine noch nicht aktivierbare normale Signierdiskette bzw. Signierchipkarte und einen Aktivierungscode, mit dem er daheim die Signier-Diskette/Chipkarte aktiviert. Gegebenenfalls kann der Wähler die Datei zum Herstellen einer noch nicht aktivierbaren Signierdiskette über das Internet erhalten, und den Code auf separatem Weg. Der Wähler kopiert dann die Datei auf eine Diskette und aktiviert diese anschließend mit dem Code. Hiermit ist eine normale, jederzeit in beiden Richtungen nutzbare Intergramm-Verbindung zwischen dem Wähler und seiner Gemeindeverwaltung hergestellt.

Der zweite Schritt umfasst die Vorbereitung und Durchführung der Internetwahl. Zunächst beantragt der zukünftige Internetwähler durch persönliches Vorsprechen oder per Intergramm bei seiner Gemeinde seine Teilnahme an der Internetwahl. Er versichert dabei an Eides statt, dass er seine Stimme persönlich und unbeeinflusst abgeben wird. Nachdem ein Beauftragter der Gemeinde geprüft hat, ob der Wähler im Wählerverzeichnis aufgeführt ist, wird mittels der **Wahlserver-Software** für den Wähler eine noch nicht aktivierbare **Wahldiskette** oder **Wahlchipkarte** und ein zugehöriger Aktivierungscode erzeugt.

Falls der Wähler persönlich bei der Gemeinde vorspricht, empfängt er dort direkt seine noch nicht aktivierte Wahl-Diskette/Chipkarte und seinen Code. Bei einem Antrag auf Teilnahme an der Internetwahl per Intergramm erhält der Wähler, ebenfalls per Intergramm, eine Datei zur Erzeugung einer Wahldiskette und gesondert den Code zu ihrer Aktivierung. Die Datei kopiert er sich auf eine Diskette und aktiviert diese mit dem Code. Damit verfügt er über eine einsatzbereite Wahldiskette zum anonymen Unterzeichnen eines elektronischen Stimmzettels.

Vor seiner Stimmabgabe lädt sich der Internetwähler einen **elektronischen Stimmzettel** herunter, füllt diesen am Computer-Bildschirm aus, authentisiert sich mit seiner Wahl-Diskette/Chipkarte, unterzeichnet den Stimmzettel mit einer anonymen digitalen Signatur (Abbildung 1) durch einen Klick und sendet ihn als Intergramm durch einen weiteren Klick verschlüsselt an das autonome Modul mit der **elektronischen Wahlurne**.

Nach Wahlende authentisiert sich der Wahlleiter an einem im Wahllokal aufgestellten Computer mit einer für ihn angefertigten **Prüfdiskette** (entspricht einer normalen Signierdiskette) und öffnet hierdurch die elektronische Wahlurne, in der alle eingegangenen Internetstimmzettel in verschlüsselter Form gesammelt sind. Durch einen Klick werden die Stimmzettel von der elektronischen Wahlurne über das Internet zum Computer des Wahllokals gesendet und dort automatisch entschlüsselt. Durch je einen Klick wird die digitale Signatur aller Stimmzettel verifiziert.

Stimmzettel mit ungültiger Signatur oder solche mit gleichem K-Wert werden ausgesondert. Hiermit wird sichergestellt, dass jeder Internetwähler nur einen Stimmzettel einreichen kann. Auch ist ausgeschlossen, dass ein Internetwähler noch zusätzlich persönlich im Wahllokal seine Stimme abgibt, denn sein Antrag auf Teilnahme an der Internetwahl wurde in der Wählerliste vermerkt.

Die verifizierten Stimmzettel werden in eine **elektronische Stimmzettelbox** eingegeben (Abbildung 2) und ausgewertet. Dort kann jeder Interessierte ihre Echtheit anhand der anonymen Signatur und das Wahlergebnis anhand des zur Auswertung verwendeten Algorithmus prüfen.

Außerdem können die elektronischen Stimmzettel ausgedruckt, zusammen mit den persönlich im Wahllokal ausgefüllten oder per Brief eingereichten und auf Papier ausgefüllten Stimmzetteln ausgewertet und für Kontrollzwecke aufbewahrt werden.

Zur Sicherheit können Duplikate der elektronischen Wahlurne und anderer wesentlicher Komponenten des Systems vorgesehen werden. Bei Ausfall der

originalen Einheit können beispielsweise die verschlüsselten Stimmzettel aus dem Duplikat der Wahlurne herunter geladen werden.

### **Die Problematik des Stimmenkaufs**

Einen möglichen gesetzeswidrigen Kauf von Stimmrechten hat der Gesetzgeber bei der Briefwahl bewusst in Kauf genommen, um einer großen Wählerzahl die bequeme Teilnahme an einer Wahl zu ermöglichen. Ein gleiches Risiko besteht bei einer elektronischen Wahl vom eigenen Computer aus.

Ein betrügerischer Stimmenkauf lässt sich beim **i-voting**-Verfahren in folgender Weise ausschließen: Jeder Internetwähler benennt seiner Gemeinde eine vertrauenswürdige Person, an welche sein Aktivierungscode per Intergramm geschickt wird. Diese Person fungiert als Wahlzeuge. Vor der Wahl versichert der Zeuge an Eides statt per Intergramm, dass er dem Wähler zum Zeitpunkt der Wahl persönlich den Code aushändigen wird. Weiterhin verpflichtet sich der Wahlzeuge, darauf zu achten, dass der Wähler in seiner Gegenwart, jedoch ohne die Möglichkeit für den Zeugen, Einzelheiten zu erkennen, die Wahldiskette aktiviert, den elektronischen Stimmzettel ausfüllt, anonym unterschreibt und an die elektronische Wahlurne abschickt. Nachdem die für die Organisation der Wahl zuständige Gemeinde die eidesstattliche Erklärung des Wahlzeugen erhalten hat, übermittelt sie diesem den Code.

### **Vorzüge von i-voting**

Das i-voting-Verfahren ist wählerfreundlich, transparent, sicher und preiswert, denn:

- Der Internetwähler muss, wenn er mit Signierdisketten arbeitet, zur Vorbereitung der Wahl nicht persönlich bei seiner Gemeinde vorsprechen, sondern kann die Wahlunterlagen per Intergramm einreichen und erhalten.
- Der Wähler gibt seine Stimme am eigenen Computer ab.
- Die Hardware-Ausstattung zur Organisation der Internetwahl ist bei der Wahlbehörde und beim Wähler denkbar gering, besonders wenn statt Chipkarten mit Disketten gearbeitet wird.
- Der Wahlvorgang ist für den Wähler und die Wahlbehörde einfach und bequem.
- Auch die Wahlauswertung ist einfach und bequem.
- Jeder Internetwähler und sonstig Interessierte kann das Wahlergebnis zur Information und Kontrolle von seinem Computer aus einsehen.
- Die anonyme Signatur eines Stimmzettels kann nur der Wähler selbst mit dem Unterzeichner in Verbindung bringen, denn die Internetspuren lassen sich höchstens bis zum autonomen Modul zurückverfolgen.
- Bei Ausdruck auf Papier können die elektronisch übermittelten Stimmzettel wie die übrigen Stimmzettel verwaltet werden.
- Ein Stimmenkauf lässt sich ausschließen.

### **Abbildungen 1 und 2**

**Abbildung 1:  
Anonym signierter Stimmzettel  
für i-voting**

<b>ABRAHAM Max</b>	<input type="radio"/>
<b>BECKER Günter</b>	<input type="radio"/>
<b>CAESAR Heinz</b>	<input type="radio"/>
<b>DREIER Helmut</b>	<input type="radio"/>
<b>EBERHARD Oskar</b>	<input type="radio"/>
<b>FOCKER Adalbert</b>	<input type="radio"/>
<b>GREINER Bernhard</b>	<input type="radio"/>
<b>HOLZHAUER Daniel</b>	<input checked="" type="radio"/>
<b>ISENACKER Quirin</b>	<input type="radio"/>
<b>JELAFFKE Ulrich</b>	<input type="radio"/>
<b>KOLBENHAUER Kurt</b>	<input type="radio"/>
<b>LEIMENER Bartel</b>	<input type="radio"/>

72085 33172  
04381 80478  
42866 39105

**Abbildung 2:  
Schema von i-voting**

