Hierodiction Software

EVOTE Internet Voting System

Was ist EVOTE?

EVOTE bietet Internet-basierte elektronische Stimmabgabe unter strikter Einhaltung der Wahlrechtsgrundsätze. EVOTE ist customisierbar und stellt – im Gegensatz zu konventionellen e-Voting Systemen die Wahlkommission ins Zentrum aller Aktivitäten. Die Wahlkommission hat die volle Kontrolle über die Wahldaten, gibt in einem gemeinsamen Akt die Wahl frei und ermittelt das Ergebnis mit Hilfe einer benutzerfreundlichen, graphischen Oberfläche, die vom Benutzer keinerlei Programmier- oder vertiefte IT-Kenntnisse verlangt.

EVOTE basiert auf wissenschaftlichen Forschungsresultaten, die publiziert sind und folgt EML (Election Mark-up Language), die in Europaratsempfehlung 2004(11) referenziert wird.

EVOTE besteht aus den folgenden Modulen:

Common Administration Space (CAS):
Der CAS bietet Customisingfunktionen für Wahladministratoren und Wahlkommissionen und ermöglicht es über eine benutzerfreundliche Oberfläche, alle Parameter einzugeben, die für die Abhaltung einer Wahl oder einer Abstimmung nötig sind. Der CAS ermöglicht auch dezentrale Wahlkommissionen, die virtuell zusammentreten und gemeinsam die Wahldaten eingeben, prüfen und freigeben. Die Wahlkommissionen können über den CAS die Wahl auch life überwachen und die Urne öffnen.

Der CAS setzt dabei ein striktes Zugriffs- und Rechtekonzept durch mit den Rollen, Systemadministrator, Wahladministrator und Wahlkommissionsmitglied. Einige Funktionen können nur von einem vordefinierten und nicht änderbaren Quorum an Kommissionsmitgliedern benutzt werden.

Voter Roll Loading Tool (VRL): Mit diesem Beladewerkzeug können Wählerstammdaten und Wahlrechte in das System geladen werden. VRL bietet umfangreiche Funktionen für das Zusammenführen und die Prüfung von dezentral gehaltenen Wähler(teil-)verzeichnissen.

E-Voting Server (EVS): Dies umfasst eine Start (Web) Page, die den Java-basierten Wahlclient startet und ein Set an Web Services, die mit dem Wahlclient kommunizieren. Der E-Voting Server verfolgt alle Sitzungen, die er gestartet hat und prüft alle Anfragen auf Gültigkeit. Die Start Page kann in die allgemeine Wahlseite des Wahlveranstalters integriert werden.

Der Wahlclient (EVC): er stellt die Schnittstelle zum Wählenden dar und ermöglicht es, sich für Wahlen zu registrieren und eine Stimme abzugeben. Er ist Java-basiert und damit plattformunabhängig. Die Kommunikation mit dem EVC ist vollständig verschlüsselt und authentisiert.

Secure Key Management Server (SKM): Alle kryptographischen Schlüssel für die Wahl warden vom SKM gemanagt, er ermöglicht kryptographisch abgesicherte Quorumsentscheidungen (z.B. zum Öffnen der Urne und Zählen der Stimmen).

Verifikator (VFY): Diese Erweiterung des SKM stellt eine zweite digitale Signatur auf die elektronischen Wahlkarten zusätzlich zum EVS bereit. Er wird sinnvollerweise von einer unabhängigen Kontrollinstanz betrieben (verfügbar 2008).

Logging und Audit (LGG): EVOTE bietet eine große Zahl potentieller Protokollierungspunkte über die Aktivitäten der Administratoren, Wahlkommissionen und Wählenden. Außer bei extrem kritischen Vorgängen können Protokollierungspunkte je nach Auditierungserfordernissen ein- und ausgeschaltet werden.

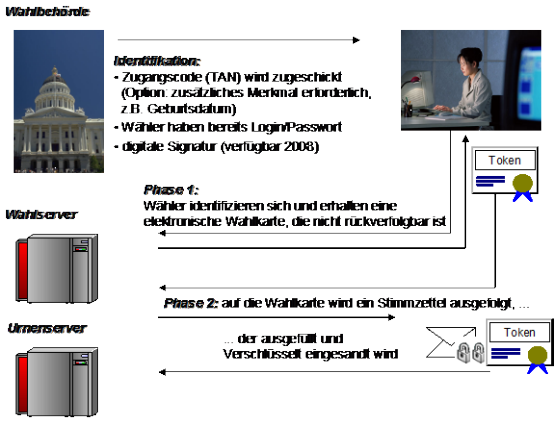
LGG bietet eine große Zahl von Berichten für alle administrativen Bereiche, die es Wahlkommissionsmitgliedern (und nicht nur Systemadministratoren) ermöglichen, die Wahl zu verfolgen. Die Protokollierungen sind verschlüsselt und gegen Manipulation geschützt.

Intrusion Detection Cockpit (IDC): CAS, EVS, SKM und VFY überwachen sich laufend selbst sowie den eingehenden Datenverkehr. Verdächtige Aktivitäten werden protokolliert und erzeugen einen sofortigen Alarm in der IDC.

Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

Organisatorische Szenarios

Aufgrund seiner Flexibilität unterstützt EVOTE mehrere Wahlszenarien:



Die Phasen 1 und 2 können in einer Transaktion kombiniert oder zeitlich getrennt in zwei Transaktionen durchgeführt werden. Der letztere Fall entspricht im Procedere der Briefwahl. Er hat den Vorteil, dass die Registrierung für e-Voting einige Tage vor der Wahl enden und die Liste der nicht für e-Voting (oder die konventionelle Briefwahl) Registrierten als Papierwählerverzeichnisse für die Wahllokale gedruckt werden kann. Damit wird eine on-line Anbindung der Wahllokale überflüssig, was zu enormen Kostensenkungen führt.

In beiden Fällen wird das Stimmgeheimnis durch die elektronische Wahlkarte geschützt, die auf den Wählenden nicht rückverfolgt werden kann, deren Authentizität und Einmaligkeit aber sehr wohl durch kryptographische Verfahren sichergestellt ist. Optional kann auch eine zweite digitale Signatur einer Kontrollinstanz auf der elektronischen Wahlkarte aufgebracht werden (Verifikatormodul).

Wahlbetrug – und hier ist die Serveradministration des Wahlsystems der gefährlichste Gegner – wird u.a. durch eine Verschlüsselung der Stimmen mit den öffentlichen Schlüsseln der Wahlkommissionsmitglieder noch beim Wählenden erreicht. Der Stimminhalt ist damit für die Serveradministration unerreichbar und nur die Wahlkommission oder ein vordefiniertes gültiges Quorum davon kann die Stimmen öffnen und zählen. Die vom Wahlserver und einem optionalen Verifikator authentisierte elektronische Wahlkarte wird untrennbar mit der Stimme gespeichert. Eine Verbindung, die nur von der Wahlkommission eingesehen und verifiziert werden kann.

Vorteile

Stimmgeheimnis: Sobald die Stimme abgegeben wurde, wird das Stimmgeheimnis durch das Protokoll in [1] sichergestellt.

Sicherung gegen "Malware": Der Wahlclient ist keine Webseite, sondern ein Java Applet. Im Gegensatz zu einfachen Webseiten kann das Applet seine Kommunikation mit dem Server, Inputs und seine interne Konsistenz selbst prüfen. [2]

Sicherungen gegen Angriffe Dritter: Die gesamte Kommunikation zwischen Wahlclient und Server ist verschlüsselt und authentisiert.

Sicherung gegen Wahlbetrug: Nur die Wahlkommission hat Zugriff auf die verschlüsselten Stimmzettel. Das Öffnen der Stimmzettel kann von einer einstimmigen oder einer Mehrheitsentscheidung abhängig gemacht werden (vgl. [3]), wobei das Mehrheitsquorum nachträglich nicht mehr manipulierbar ist.

Auditierbarkeit: Der Systemadministration und den Wahlkommissionen stehen umfangreiche Protokollierungen zur Verfügung. Die Protokolle sind verschlüsselt und gegen Manipulation gesichert.

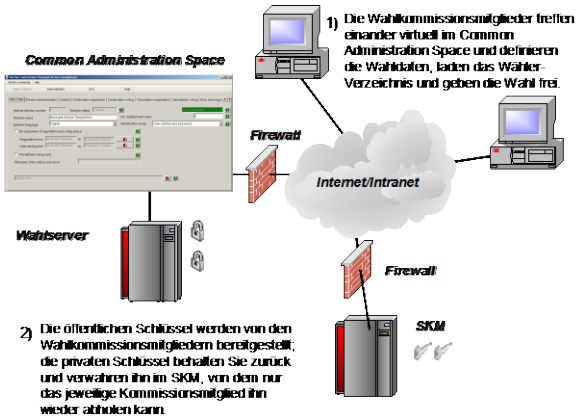
Flexibilität: EVOTE unterstützt Haupt- und Präferenzoptionen, mehrere Wahlkreise pro Wahl, die Vergabe mehrerer Stimmen durch den Wähler, Kumulation und Panagieren, Streichen, verschiedene Stimmzetteldesigns und Identifizierungsmethoden für den Wählenden. Texte, die dem Wähler angezeigt werden, können in einem einfach zu bedienenden Editor definiert werden.

Wahlkommissionen: EVOTE stellt den Common Administration Space (CAS) zur Verfügung, mit dem die Wahlkommissionsmitglieder gemeinsam die Wahl administrieren; der CAS kann simultan von allen Kommissionsmitgliedern verwendet werden, auch wenn diese sich nicht am selben Ort befinden. Die Wahlkommission legt die Stammdaten in den Wahlkreisen an, legt den Stimmzettel und die Möglichkeiten zur Vergabe von Stimmen und Streichungen fest und gibt gemeinschaftlich die Wahl frei. Sie beobachtet laufend die Wahl und öffnet gemeinsam die Urne.

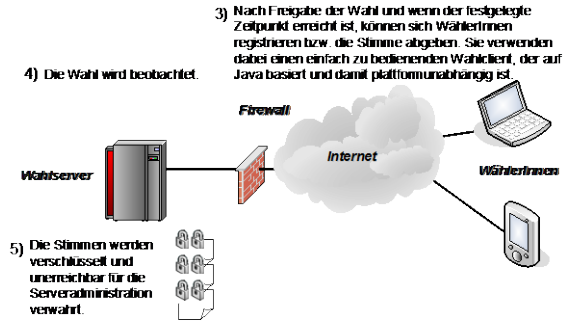
[1] Prosser, A., Müller-Török, R.: E-Democracy – eine neue Qualität im demokratischen Entscheidungsprozess, Wirtschaftsinformatik 44(2002), S. 545-556
[2] Prosser, A., Schiessl, K.: Elections via the Internet; Int. Journal of Public Admin. in Central and Eastern Europe 1/2007, S. 28-38
[3] Prosser, A., Kofler, R., Krimmer, R., Unger, M.-K.: Implementation of quorum-based decisions in an election committee; LNCS 3183(2004), S. 122-127

Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

Wahladministration

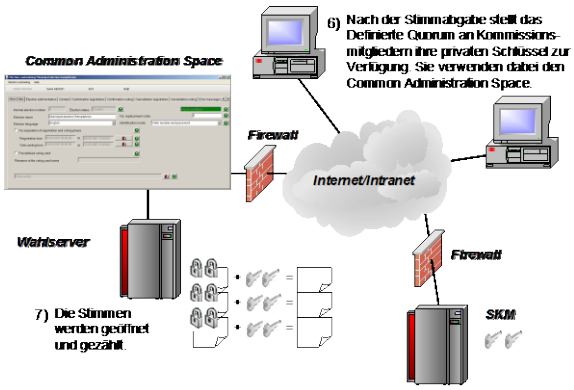


Der Common Administration Space ermöglicht es der Wahlkommission alle relevanten Parameter der Wahl selbst einzugeben und zu prüfen. Umfangreiche Prüfroutinen stellen die Integrität der Daten sicher. Nach Freigabe der Wahl können die relevanten Daten nicht mehr geändert werden (Schritt 1).



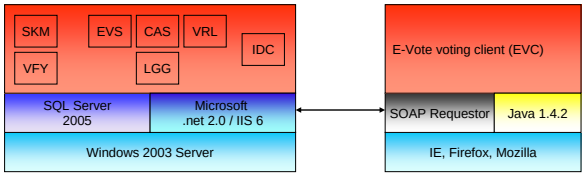
Bei der Freigabe legt die Wahlkommission das Quorum zum Öffnen der elektronischen Urne fest und jedes Mitglied generiert ein privates/öffentliches Schlüsselpaar, wobei der öffentliche Schlüssel für die Verschlüsselung des Stimmzettels beim Wählenden bereitgestellt und der private Schlüssel im SKM verwahrt bleibt. Nur das jew. Kommissionsmitglied kann diesen privaten Schlüssel freigeben. Daher kann weder ein Systemadministrator des Wahlsystems noch ein einzelnes Kommissionsmitglied die Wahl manipulieren (Schritte 2 - 5).

EVOTE offeriert extensive Überwachungswerkzeuge für Systemadministration und Wahlkommissionen ohne aber dabei das Stimmgeheimnis zu gefährden. Verdächtige Aktivitäten werden sofort gemeldet.



Nach Ende der Stimmabgabe stellen die Wahlkommissionsmitglieder ihre privaten Schlüssel zur Verfügung und öffnen gemeinsam die elektronische Urne; die Stimmen werden geprüft und ausgezählt (Schritte 6 und 7).

Systemarchitektur



Die Serverkomponenten von EVOTE basieren auf allgemein anerkannten Industriestandards, der Wahlclient ist Java-basiert und damit plattformunabhängig. Die Kommunikation basiert auf standardisierten Web Services (SOAP) und benutzen Nachrichtenformate der Election Markup Language (EML).

Diese Architektur ermöglicht es, die Produktivität und allgemeine Unterstützung von Industriestandards mit offenen Systemplattformen im Wahlclient zu verbinden.

Es ermöglicht es auch, Komponenten von Drittanbietern flexibel in EVOTE zu integrieren, sofern diese SOAP Web Services und EML unterstützen, wie etwa externe Software zur Verwaltung der Wählerevidenz, Auszählungssoftware oder externe Identifikation der Wählenden. An kritischen Punkten bietet EVOTE “Program Exits”, die den Anschluss externer Komponenten ermöglichen.

EVOTE inkorporiert den Stand der Forschung im Bereich e-Voting und die Software wird laufend an die neuesten Entwicklungen angepasst. EVOTE bietet einen Wartungsvertrag mit Second/Third Level Support, Training und Beratungsdienstleistungen über das System.

Service Provider, die EVOTE einsetzen, können die Basis-Softwarebibliotheken von EVOTE, die Protokollierungskomponente und das IDC sowie den SKM Server für eigene Entwicklungen in anderen Bereichen als e-Voting einsetzen. Dies wird durch umfangreiche Softwaredokumentationen erleichtert.

Kontakt: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at