Hierodiction Software

EVOTE Internet Voting System

What is EVOTE?

EVOTE offers remote, Internet-based electronic voting that protects General Voting Principles. EVOTE is customizable and in contrast to conventional e-voting systems, puts the election committee in the centre of all activities. It is the election committee who has full control over the election data, who jointly releases the election and ascertains the result via a user-friendly interface that does not require programming skills or in-depth computing knowledge.

EVOTE is based on published cryptographic research results and follows the EML (election markup language) model as referred to in the Council of Europe Recommendation 2004(11).

EVOTE consists of the following modules:

Common Administration Space (CAS): Customizing functions for election administrators and election committees, which enables one to enter all parameters necessary to conduct an election or referendum via a user-friendly, graphical interface. The Administration Space enables even dislocated election committees to virtually meet and to jointly define and release the election as well as to monitor the election and to open the ballot box once voting has stopped.

The Common Administration Space enforces strict access management on the level of system administration, election administration and the election committee functions for an individual constituency; some functions may only be accessed by a pre-defined quorum of committee members or administrators.

Voter Roll Loading Tool (VRL): This enables one to load voters, to merge voter rolls from several sources, to define consistency rules in the loading operation, and to update and to check the voter roll.

E-Voting Server (EVS): This encompasses a start page that launches the Java-based voting client and a set of Web services to communicate with the voting client. The start page is delivered as source code and can easily be integrated in a custom-made Web page of the election authority.

The Web services respond to the voting client's requests, check their validity and drive the voting client by providing the necessary data for the voter.

The E-Voting Server keeps track of all launched Voting Client Sessions and performs consistency checks on each request by the Voting Client.

The Voting Client (EVC): This is the interface to the voter enabling the voter to register for an election and to cast a vote (for scenarios, see below). The Voting Client is Java-based and hence platform independent. Communications between the Voting Client and the Voting Web service are fully encrypted and authenticated.

The Secure Key Management Server (SKM): All cryptographic election keys are managed by the SKM, which enables cryptography-based majority decisions in committees (eg., when a majority in an election committee decides to open and count the ballot).

The Verifier (VFY): An extension to the SKM, which provides a second digital signature on voting rights in addition to the election server. An independent watchdog authority providing additional safeguards in the election process would typically run the Verifier (available 2008).

Logging and Auditing (LGG): EVOTE offers a large number of potential logging points covering the activities of the system administration, election committee and voters. Except for the most crucial events (e.g., election was released) the logging point may be selected/deselected via a simple user-friendly interface depending on the specific auditing needs.

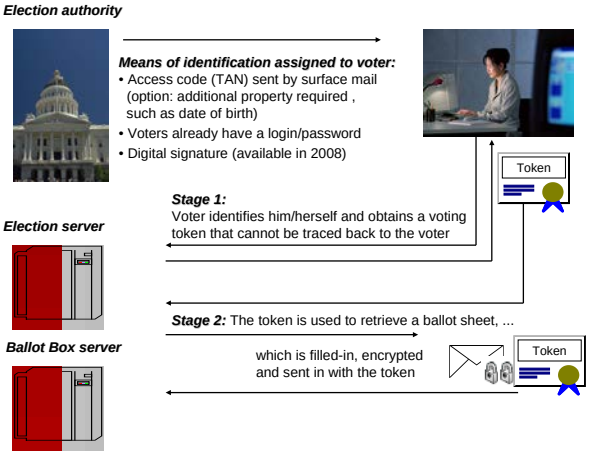
A large number of reports are offered on all administration levels, which enables election committee members (and not just system administration) to monitor an ongoing election. The logging is encrypted and tamper-resistent.

Intrusion Detection Cockpit (IDC): CAS, EVS, SKM and VFY constantly monitor themselves and their incoming data traffic. All suspicious activities are logged, classified and cause alerts that show in the IDC component.

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

Organisational Scenarios

Due to its flexibility, EVOTE supports several election scenarios:



Stage 1 and 2 may be combined in one transaction or they may be two separate transactions following the principle of postal voting, where voters register and obtain a voting card (here an electronic voting token) and later cast their vote. This procedure offers the advantage that if registration for e-voting ends some time before general voting starts, voters, who have not registered for e-voting (or postal voting) are printed on the paper rolls distributed to the polling stations. Hence, polling stations need not be equipped with online access to the voter roll which makes e-voting considerably more cost-effective.

In either case voter secrecy is protected by the voting token which due to the cryptographic algorithms used, cannot be traced back to the voter, but nevertheless cannot be forged by a third party. Optionally, a second digital signature by an independent authority may be added using the Verifier module.

Election fraud – and the most dangerous adversary here is the election server administration themselves – is among other measures prevented by the public keys provided by the election committee. The vote is encrypted in the Voting Client inaccessible to the server administration. Only the election committee in its entirety or in a pre-defined quorum decision may open the ballot and count it. The token authenticated by the election server and an optional Verifier is inextricably linked to the vote – a link, which again can only be viewed and verified by the election committee.

Benefits

Voting Secrecy: Once, the vote has been cast, anonymity is technically guaranteed by the cryptographic protocol in [1].

Safeguards against Malware: The voting client is not a Web page, but a Java Applet. In contrast to simple Web pages, the Applet may validate all communications with the election server, check inputs, and run internal consistency checks. [2]

Safeguards against Third-Party Attacks: All communication between the election server and the voting client is encrypted and authenticated.

Safeguards against Election Fraud: Only the election committee may access the ballot, which is cryptographically protected from all unauthorized access. Opening of the ballot may depend on a unanimous committee decision or an ex-ante defined, unalterable majority quorum (for the cryptographic procedure, see [3]).

Auditable: Extensive logging facilities are provided for the election committee and administration.

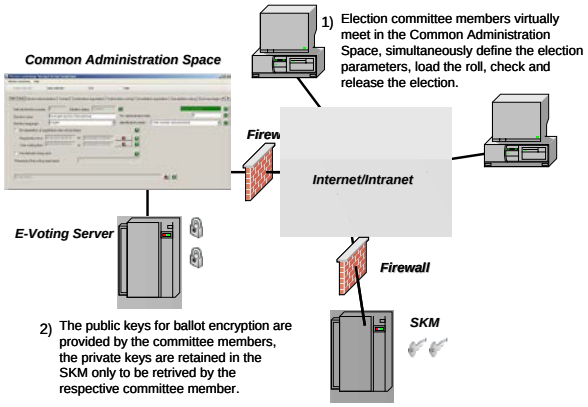
Flexible: EVOTE supports main and preferential options, multiple constituencies per election, multiple votes, cumulating votes, splitting the ticket, several ballot sheet designs and voter identification modes. Confirmation and error texts displayed to the voter may be defined in a comfortable text editor.

Election Committee: EVOTE provides a Common Administration Space for the committee members to jointly administrate an election that may be used simultaneously, even though the committee members work from different locations. Via the administration tool, the election committee creates election and the ballot sheet, defines voting rights, jointly releases and monitors the election and finally opens the electronic ballot box.

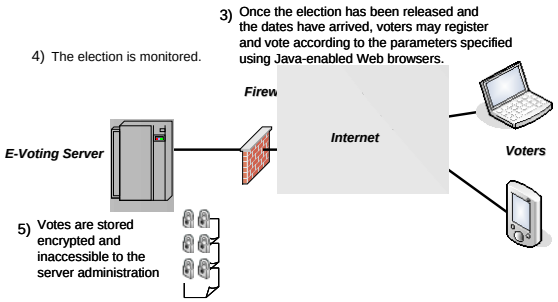
[1] Prosser, A., Müller-Török, R.: E-Democracy – eine neue Qualität im demokratischen Entscheidungsprozess, Wirtschaftsinformatik 44(2002), pp. 545-556
[2] Prosser, A., Schiessl, K.: Elections via the Internet; Int. Journal of Public Admin. in Central and Eastern Europe 1/2007, pp. 28-38
[3] Prosser,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

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

Election Administration

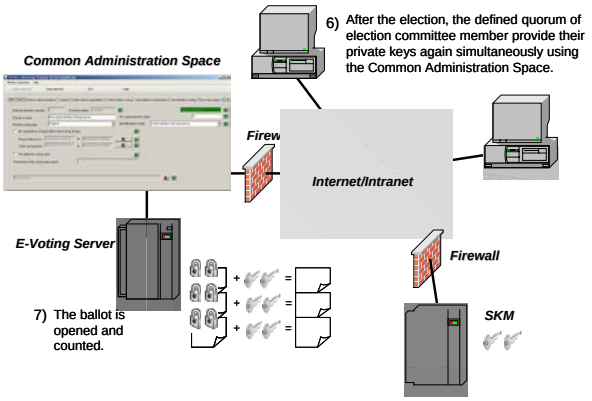


The Common Administration Space enables the election committee to enter and check all relevant parameters. Checking functions are provided to check integrity of the data. On release of a constituency/election the relevant parameters cannot be manipulated (Step 1).



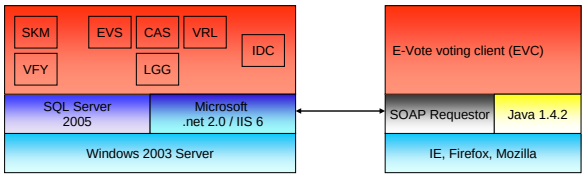
Upon release, the committee defines the opening quorum for the ballot box and each member generates a private/public key pair, where the public key is used to encrypt the vote in the voting client; each private key remains in the Key Server and can only be released by the respective committee member. Hence, neither the system administration of the Election Server nor any single committee member is able to manipulate the ballots (Steps 2 - 5).

EVOTE offers extensive monitoring tools both for the election committee and for the system administration. All sessions are traced (without corrupting voting secrecy!) and system administration is notified of suspicious activities.



After the election, the pre-defined quorum of committee members meet in the Administration Space, provide their private keys and the ballots are opened and counted (Steps 6 and 7).

System Architecture



The server side of EVOTE is based on industry-standard infrastructure, the Voting Client is Java-based and platform independent. Communications are based on standardized Web services which follow the SOAP specification and use the Election Markup Language (EML) for content exchange.

This architecture enables to flexibly combine the productivity and general support of industry standard infrastructure at the back-end with open standards and platform independence for the Voting Client.

It also enables one to flexibly add or replace components with third party products that support SOAP Web services and EML, such as third-party software managing the voter roll, external counting software, or external identification. At critical points in the process, EVOTE offers program exits where customers may “hook on” their own, custom made software to the voting system or the key server.

EVOTE is a software product incorporating the latest research results and the software is constantly adapted according to relevant progress in the field. EVOTE comes with maintenance services covering second and third level support, staff training and consulting on the use of the system.

Service providers running EVOTE may use the utility libraries, the logging and IDC component and the SKM key server for their own custom-made software systems in other areas run in their own organisations. To facilitate such reuse, EVOTE comes with extensive system documentation.

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