e-Vote 2011 Security Objectives

NORWEGIAN MINISTRY OF LOCAL GOVERNMENT
AND REGIONAL DEVELOPMENT

Content

1. Introduction

This document provides a statement of security objectives for the Electronic Voting system. It is not a statement of requirements, and is subject to change during the dialogue phase.

The document has the following structure:

Ch. 2: The security environment based on a simple system model

Ch. 3: Threats to e-voting services

Ch. 4: System security objectives

The document is largely based on the *e-Voting Security Study, Issue 1.2,* delivered by CESG, the UKs National Technical Authority for Information Assurance in 2002.

The intention of this document is to highlight high level security requirements applicable to all elements of the e-vote system including environment and operation. Furthermore, the CoE Recommendation Rec(2004)11 contains significant procedural and technical requirements, to which the project wishes to adhere – at least in spirit.

Despite the attempts to secure the system, it is probably impossible to make any system perfect at reasonable cost. This leads to the conclusion that a sensible risk management-based approach needs to be established.

The Contractor will therefore be required to keep a continuously updated threat model enumerating the identified threats, vulnerabilities and corresponding mitigations, as well as a risk assessment of his/her deliverables including required security in the operating environment of the deliverables.

The key questions to be answered by the Contractor are what is the remaining risk given the application of security mechanisms and why should the remaining risk be acceptable to e-vote 2011 project?

2. Security Environment

2.1 Environmental Assumptions

The voting system will consist of several major parts:

a. the administrative parts, used for election preparation
b. the e-voting parts, used during on-line e-voting
c. the election result parts, used during the compilation and export of the election results.

Apart from paper-voting, the delivery of election services may take place across the open Internet. The security domain model is illustrated in figure 1.

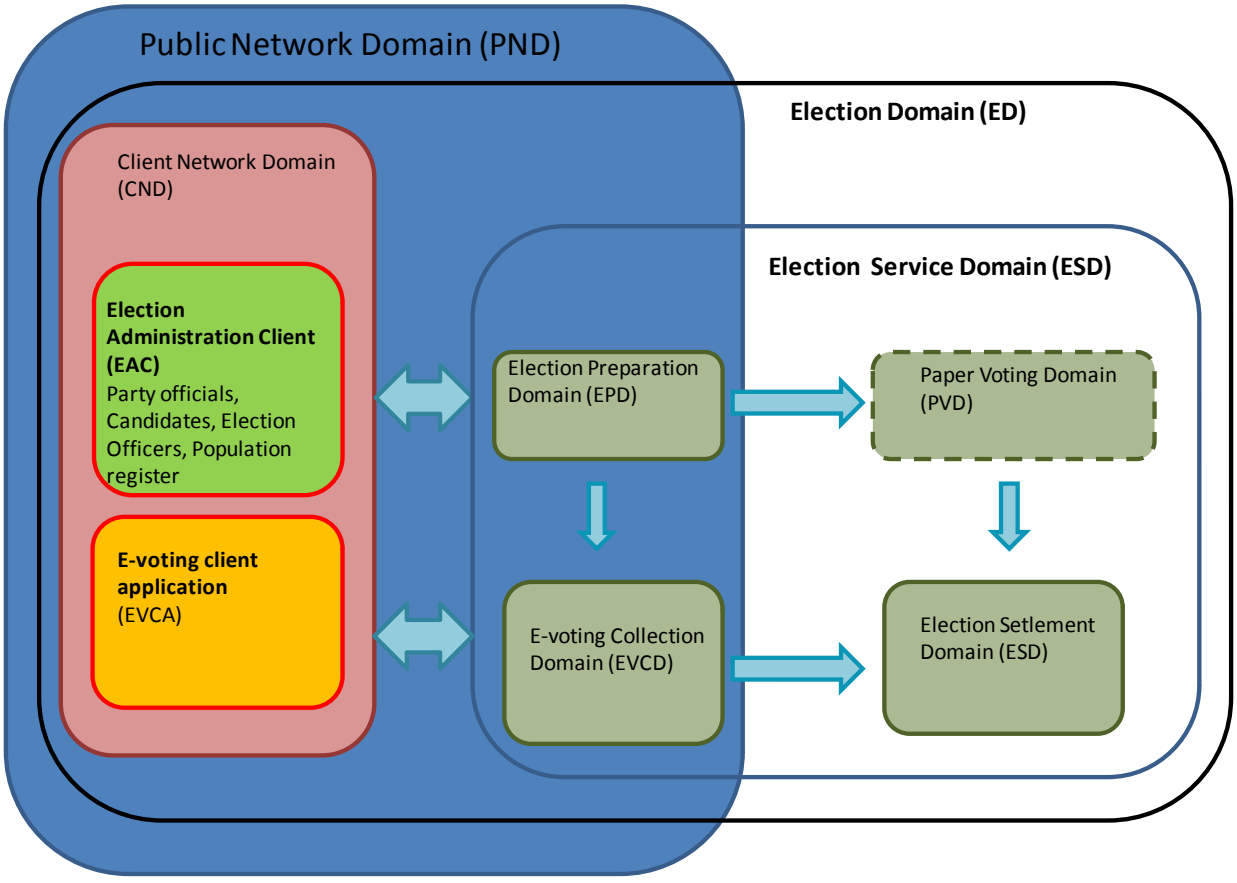

Fig 1: Election System security domains

- **Election Domain (ED)** contains all the Election and Voting Services, with the exception of casting and counting paper vote ballots, that are necessary to prepare and complete an election.
- **Public Network Domain (PND)** contains that part of the communications infrastructure which is not under the control of the Election Service operators and clients. In the case of Internet delivery, it must be assumed to be accessible to potential threat agents and to provide a transmission capability without service quality elements (e.g. integrity or confidentiality). In the e-voting context, the PND includes the Internet.
- **Election Service Domain (ESD)** contains that part of the communications and processing infrastructure which will be under the Government's control. It is used to host the election

preparation sevices, the e-voting registration and collection services, as well as the election settlement services. The different domains are described below:

- **Election Preparation Domain (EPD)** contains all the services required to prepare an election. Election preparation shall provide abilities both for paper-voting and for electronic voting. The EPD may extend to facilities beyond the authorities immediate control for processes such as secure printing.
- The **e-Voting Collection Domain (EVCD)** contains the IT infrastructure to host all or part of the electronic ballot collection process. The EVCD should be physically separate from the EPD and ESD to facilitate the anonymity of the ballot.
- The **Election Settlement Domain (ESD)** contains the IT infrastructure to host all of the election settlement processes. The results of both paper-votes and e-votes are merged into the final election results, seats are distributed and the election results are computed for publication. The IT infrastructure of the ESD shall be off-line (airgapped).
- The **Client Network Domain (CND)** is that element of the infrastructure under client control, which is used to support access to the Election Service. It is likely that the CND will be a single domestic personal Computer connected via an ISP to the EVRD, in this case the ISP lies within the PND. The CND consists of two separate domains described below:
- **Election Administration Client (EPC)**, contains functions for election preparation, i.e to perform the administrative part of election setup, preparation and administration.
- **E-Voting Client Application (EVCA)** is that element of the CND that is supplied by the election service and is installed within the CND to encapsulate important trusted elements of service. The election service management will exercise some control over the content (but not necessarily the delivery of) the EVCA.

3. Threats to e-voting Services

Electronic Voting has the potential to break down the geographic barriers of traditional election systems. The election system is no longer by necessity confined to the local polling station; conceivably it is accessible world-wide, thus increasing the potential number of attackers and attack vectors dramatically.

By its very nature, the election process is an attractive target for malicious actions. An online voting system would need to win public confidence, which could easily be undermined by an election-day horror story.

No assumptions are made in what follows with regards to the configuration the e-Voting system. The assessment is based on the assumption that the e-Voting system will have external connections (remote electronic voting - REV), affording external access, and the information will potentially be available online and of a personal nature

3.1 Potential Sources of attack

3.1.1 Internal

Legitimate users

Legitimate users of the Elections System may seek to misuse or damage the election system and may have significant technical resources and skills at their disposal, with a strong motivation to subvert the system – frequently for financial gain. Since they are legitimate users, they are subject to legal sanctions if the subversive activity is traced to them.

System developers

Developers of the Elections System possess significant resources and technical skills, have privileged access to the source code and are in a position to hide malicious code in the system, causing it to malfunction at a specific time or event. They may have strong motivation to subvert the system for financial or political gain. System developers will be employees of The Contractor or their subcontractors and may or may not be subject to legal sanctions, depending on their location.

System operators

The Elections System operators may seek to exploit their privileged position. They may include government employees or their agents or employees of outside organizations contributing to election services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation could be desire to defraud the election process, either for financial gain or personal satisfaction. Service operators and government employees are readily subject to sanction in the event that security breaches are traced to them.

Other Insiders

Government employees and their agents who may have access to the Elections System, but are not associated with the provision of election services, may conduct insider attacks. These individuals may possess a strong motivation to mount an attack for financial or personal gains. Such individuals will be readily subject to sanction.

3.1.2 External

Hostile Individuals

Individual hackers may seek to cause disruption to systems because of a personal grudge, for the challenge of attacking a government system or in protest against government policies. They may also wish to access, corrupt or steal data, either for personal gain or for publicity purposes.

Criminal Organizations

Criminals or others, such as information brokers, may also wish to access systems in order to obtain personal details for exploitation.

Protest Groups

Protest groups or hackers ("hacktivists") may seek to attack systems in order to demonstrate opposition to e-voting, to disrupt the e-voting mechanism or to obtain data to exploit, for information or corruption purposes.

Foreign Intelligence Services

Foreign Intelligence Services may see an advantage in obtaining personal information, for intelligence-gathering and targeting purposes. They may also wish to access systems for political information-gathering purposes or to manipulate voting information in order to influence the outcome.

Terrorist Organizations

Terrorist organizations may be interested in personal information stored on the system for targeting and intelligence-gathering purposes. They may also wish to interrogate the system in order to understand voting intentions, to affect the outcome or to cause disruption to the process.

3.2 Possible Methods of attack

3.2.1 Electronic Attack

Hacking

Penetration of the Elections System would have very serious ramifications, both for public confidence in online voting, and possibly in the political process itself. To be effective, such an attack need not even modify the data stored in the system, merely put it into the public domain. Penetration of the system need not take place during the polling period, but potentially any time prior to or after the event. Large amounts of potentially sensitive personal information may be divulged. This information could be used to link votes with individuals, undermining voter anonymity. There is also the potentially less serious threat of the appearance of the site being changed (defaced); this would undermine public confidence in the system. If the hyperlinks on the site were changed this could affect the integrity and confidentiality of the votes cast; this might result in the election being declared void.

Individual client platforms are unlikely to be attractive targets for the hacker. However public Internet terminals would provide an attractive target and would need to be secured accordingly.

Malicious Software («malware»)

There is a risk of introduction of malicious software being introduced onto the e-voting server before or during the election. Furthermore, the connection of huge numbers of PCs to the Elections System may increase the chances of malware being spread to the Elections System. This could cause damage to the server and potentially propagate to other PCs. The government could potentially be liable for any resultant damage. If a program such as a «Trojan Horse» were to be installed on the e-voting server, the confidentiality and integrity of the votes could be adversely affected, in the worst case resulting in an election being declared void.

The insecurity of browsers and operating systems on the client platform will invariably make it possible to subversively install malicious software. It is possible for an attacker to introduce malware that has an activation delay on to the client platform, where it would remain undetected until activated on the date of the election. Installation of a program such as a «Trojan Horse» could compromise the confidentiality and integrity of an individual's vote, by communicating information on how an individual voted to a third party, or by changing the vote before transmission without the user's knowledge respectively. The well known existence of large botnets means that this attack can feasibly be scaled to affect the outcome of an election.

Denial of Service

An exceptionally high volume of voters using the REV-system may cause it to become temporarily unavailable. A malicious attack or mass unintentional misuse may also cause the REV-system to become unavailable, either temporarily, or in the worst case for the duration of the election.

The client may be denied service by an attack on the delivery channel. It is also possible that a client device is attacked using a program to initiate a large number of redundant computations, which could render the device useless.

Domain Name Service (DNS) Attacks

It is possible that an attacker may alter an entry in a DNS lookup table to point to a bogus web address. This would enable the owner of the bogus Site to undermine the vote of the redirected voter. The same effect can be achieved by introducing a program that tells the browser to use a certain web address as a proxy, essentially affording a «man-in-the-middle» attack.

3.2.2 Other attack approaches

Vote buying/selling and coercion

Such activities are only possible on a small-scale as a large operation would be difficult to orchestrate without being detected. However, steps must be taken to mitigate this risk, as it could seriously undermine confidence in the political process if it becomes widespread. Even if detected, large scale vote selling and buying will undermine confidence in the e-voting system.

Theft or forgery of election details

Theft and forgery of voter details is possible either electronically or from the postal system, if it were used. Once again this is unlikely to occur on a large scale since such activities would be detectable. The use of "level 4" e-ID will further reduce the damage potential.

Deliberate repudiation of transaction

An attacker could potentially go to the media and claim —I did not vote that way!" This could be used in an attempt to undermine online voting; how credible such a claim would be is questionable. This nevertheless underlines the importance of strong non-repudiation inherent in the e-ID and in the e-Voting system.

Accidental damage

Users

Legitimate users may unintentionally misuse the REV System and potentially cause damage to the System. Large numbers of voters using the System incorrectly could result in unnecessary loss in performance of the System or even causing it to crash.

Operators

Operators may, through incompetence or inadequate training, cause damage to the system

or loss of data. Such individuals are not specifically motivated to carry out such an attack but, due to their privileged access rights, may unwittingly cause significant damage.

Equipment
Equipment or software failure may lead to suspension of service or loss of information.

«Acts of God»
An accident or other natural disaster may destroy the service provision or stored information.

4. Security Objectives

4.1 System/Service Control Principles

Voter Authenticity - ensuring that the voters must identify themselves (in some manner) to be entitled to vote;

Voter Anonymity - ensuring that votes must not be associated with voter identity;

Data Confidentiality - ensuring that the vote is secret;

Data Integrity - ensuring that each vote is recorded as intended;

System Accountability - ensuring that system operations are logged and audited;

System Integrity - ensuring that the system cannot be re-configured during operation;

System Disclosability/Openness - allowing the system and process to be open to external inspection and auditing;

System Availability - ensuring that the system is protected against accidental and malicious denial of service attacks;

System Reliability - developing the system in a manner that minimizes accidental bugs and ensures there is no malicious code;

Personnel Integrity - those developing and operating the voting system should have unquestionable records of behavior;

Operator Authentication and Control - ensuring that those operating and administering the system are authenticated and have functional access on the system strictly controlled.

4.2 System/Service Control Objectives

The security control objective statements distill the threat, assets, environmental assumptions and security principles into a set of control objectives that, if they are all met, ensure that the threats identified are properly countered in the declared environment.

The objectives are necessarily high level and seek to minimize the constraints on candidate implementations. Some of the objectives will be levied on the environment and trace to security requirements that the environment must be shown to meet.

Security Control Objective	Notes
OS1 - Effective Voter Registration Voting permission is only granted to those whose bona fides have been established.	A combination of procedural and technical measures to ensure that voters are properly identified before being granted permission to vote and that multiple and false identities cannot be registered
OS2 - Effective Voter Authenticity E-voting services are only available to those eligible to vote.	Access to e-voting services can only be obtained on the presentation of properly constructed access credentials. Voter authentication will be provided by using a “level 4” authentication scheme at the national authentication portal or possibly an equivalent foreign e-ID. The SAML v2 protocol will be used for authentication.

Security Control Objective	Notes
OS3 - Effective Voter Anonymity Neither during the voting process nor at the ballot count should the identity of the voter be disclosed.	A combination of technical and procedural measures to ensure that votes cannot be attributed to individuals either whilst they are voting or during the ballot count.
OS4 - Effective Vote Confidentiality E-voting services must guarantee the confidentiality of the vote.	A combination of technical, procedural and out of band measures to ensure that votes cannot be attributed to an individual candidate during the voting process. To reduce the effectiveness of coercion and vote selling in the REV context, the following is proposed: • A voter should be able to change his or her vote an indefinite number of times in the e-voting period. • The REV-system shall not indicate to the voter if he/she has previously cast a ballot – electronic or on paper. • A voter may at any time cast a paper ballot in a polling station. This will invalidate any past or future electronic ballot.
OS5 – Effective System Identification and Authentication Accountable e-voting service processes are only accessible to those individuals and systems that have been authorized to access such processes.	A requirement for technical measures to ensure that access, to the EVSD, can only be obtained on presentation of properly constructed access credentials
OS6 – Effective System Registration Access permission to e-voting service processes is only granted to those who bona fides have been established.	A combination of technical and procedural measures to ensure that users, within the EVSD, are properly identified and authenticated, and can access only those parts of the system and assets necessary to perform the authorized task.
OS7 – Effective System Access Control Access granted to e-voting service application and assets is the minimum necessary for the identified user to obtain services required.	Will map on to a requirement to ensure that a user/administrator within the EVSD, once identified and authenticated, can access only those part of the system and assets necessary to perform the authorized task.
OS8 – Information Integrity Ensuring that the voter's intention is received as intended.	Information transmitted and received by the e-voting service must not be altered or otherwise subverted.
OS9 – Service Availability Continuing access to the e-voting service as and when required must be assured Fallback routines must be in place in case of unavailability of the e-voting system.	Users of the e-voting service must be able to depend on the continuing availability of the service in order for them to meet their obligation to vote – subject to limits imposed by the availability of the PND. Voters must not be turned away from a polling station in case of (temporary) service unavailability. The fallback should not disrupt the operation of the e-voting system once service is restored.

Security Control Objective	Notes
OS10 – Information Availability Continued access to e-voting data assets as and when required must be assured.	Data assets of the e-voting service are an important record and must not be lost through accidental, careless or deliberate acts of e-voting service users, or administrative staff, or in the event of equipment failure
OS11 – Service Protection The e-voting service implementation and associated assets must be protected from external interference and penetration.	The e-voting service must be adequately protected from outside attack mounted against the service application or the underlying network infrastructure
OS12 – Operator Integrity Those operating and administering the e-voting service should be of an unquestionable record of behavior.	The personnel administering the e-voting services may be in an enhanced position to attack the system.
OS13 – Open Auditing and Accounting The e-voting service must keep a proper record of significant transactions	A general requirement for a proper record of significant events that may have to be revisited. This will include system configuration to enable external observers to determine that no collusion could have taken place
OS14 – System Disclosability/Openness The e-voting service must be open to external inspection.	This is a general requirement of the e-voting system. The system software, hardware, documentation, microcode, and any custom circuitry must be open for random inspection at any time. An N-version[1] architecture may be desirable to address the following issues: • Accurate transmission and recording of voter intent, due to an architecture that performs fault detection and correction. • Prevention of malicious internal fraud involving changing or specifically developing malicious voting system components. • Improving openness and transparency in the process by allowing third parties to develop and run an e-voting system in parallel with the Government owned system.

[1] http://vote.caltech.edu/drupal/files/working_paper/vtp_wp12.pdf

4.3 External Control Objectives

The principal external assumptions, also known as environmental, that relate to the provision of e-voting services are tabulated below.

External Control Objective	Notes
Open Delivery e-voting services are delivered over public networks over which the e-voting service provider has little or no control.	The requirement is that no government special infrastructure is necessary to deliver the services. The Internet is seen as the delivery mechanism of choice. No statement can be made about the assurance of the client computer.
Existing Secure Networks The systems hosting e-voting services are installed and managed in accordance with existing policy and practice for government systems connected to other networks.	A statement about the environment, which cross-references to existing codes of practice and policy on government and other service supplier networks. It is expected that any large vote collection and counting systems should conform to current government best practice.
Unassured Client Domain e-voting services must be implemented in a way that permits adequate trust relationships without requiring strong controls or constraints on the terminals used to access the services.	The equipment used by members of the public to access the service is uncontrolled and typically under non- technical management control that is unaware of the security risks. Government cannot place constraints on the state of such equipment as a condition for e-voting service access. Security approaches should allow for this.