E-vote 2011

System Requirements Specification

Project: E-vote 2011

Change log

Version	Date	Author	Description/changes
0.1	18.09.09		First version
0.2	02.10.09		Draft for approving
1.0	08.10.09		Approved by Steering Committee

Distribution list

Version	Date	Name	Company
0.1	18.09.09		• Steering Committee • Political reference group • Expert reference group • Other reference groups • DNV
0.2	02.10.09		• Steering Committee • KRD • NDV
1.0	09.10.09		• Tenderers • Stake holders

CONTENT

1. Introduction

1.1. Background

In 2006 a working committee initiated by KRD delivered a report on e-voting entitled *"Electronic voting – challenges and opportunities"*. This report will provide the foundations of the project, but its conclusions will not represent absolute framework conditions.

In its discussion of the 2008 National Budget, the Storting has given its endorsement of e-voting trials at the 2011 municipal elections. In response to this, a project has been initiated under the direction of The Department of Local Government (KOMM) of The Ministry of Local Government and Regional Development (KRD).

1.2. Purpose of the system

The E-voting solution shall simplify voting, and shall provide better accessibility than current paper-based voting. The solution shall ensure rapid implementation of elections; shall ensure efficient resource usage in the municipalities; and shall facilitate the exercise of direct democracy. The present high level of trustworthiness at holding elections, based on the principle of secret ballots, shall be upheld.

1.3. Prerequisites for the e-vote system

- Transparency in project and solution
- The solution is programmed in open source code
- Standard PCs only for voting
- Authentication based on E-id
- Governmental ownership and responsibility for system running and maintenance

1.4. Project Goals

The primary objective of the project is to establish a secure electronic voting solution for political elections in Norway.

The main project goals are:

- To establish e-voting as a supplement to existing paper based voting.
- To plan, specify and procure a complete elections administrative system (including the required functionality for e-voting) to replace the system currently in use in the pilot municipalities. This will be done in close cooperation with the elections team in the KRD, which is responsible for the execution of elections and establishing a central elections administrative system.
- To engage with the political community through a political reference group. This engagement shall include goals and visions for the period after 2011.
- To initiate and participate in a public debate regarding the security, transparency and auditability of e-voting. This with the goal of raising the counter arguments, and thereby reducing skepticism and building trust in the longer term. Subjects shall include questions regarding the buying and selling of votes, coercion, family voting and black box issues.

- To establish and implement routines for e-voting which ensure a correct result and build trust.
- To establish government controlled running- and management organizations for the e-vote system in time for the 2011 pilots.
- To build expertise on e-voting within The Ministry of Local Government and Regional Development (KRD)
- To create a systematic regime for evaluation, and to evaluate the results of the e-vote 2011-project.
- Based on experience garnered in the 2011 pilots, the project shall lay plans for eventual full scale deployment of e-voting, making it available for the general voting public in all elections.

1.5. Intended Audience and Reading Suggestions

1.5.1. Audience

- Tenderer
- Stake holders
  - Steering Committee
  - Political reference group
  - Expert reference group
  - Other reference groups
- Others
  - External Quality Assurance (DNV)

1.5.2. Reading suggestions

Tenderers	Tenderer must read all documents; the System Requirements Specification (this document), Use Cases, Requirements Table and other requirements documentation.
Stake holders	
Steering Committee	Members of the Steering Committee should read the System Requirements Specification (this document) and the Use Cases for more in depth knowledge.
Political reference group	As for the Steering Committee.
Expert reference group	As for the Steering Committee.
Other reference groups	Chapters in the Requirements Specification (this document) on demand.
Others	
DNV	As for Tenderers.

2. Mandated Constraints

2.1. Solution Constraints

Identifier	Requirement description
MC1	The solution must satisfy all laws, regulations and recommendations listed in Chapters 2.1 and 2.2 in the "System Requirements Specification" document.

Laws, regulations and recommendations which must be satisfied are listed below.

2.1.1. Council of Europe e-vote Recommendation Rec (2004) 11

http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf
Recommendation Rec (2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting
(Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies)

In case of conflict between the Recommendation and the System Requirements Specification, the latter has priority.

2.1.2. Representation of the People Act (the Election Act)

http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf

2.1.3. ACT 2005-06-17 no. 102: Act on certain aspects relating to the political parties (The Political Parties Act).

http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Act_Politica_%20Parties_EN_version_120207.pdf

2.1.4. Representation of the People Regulations

http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_2003_EN_170609.pdf

2.1.5. Lov om Sametinget og andre samiske rettsforhold (sameloven).

http://www.lovdata.no/all/hl-19870612-056.html

2.1.6. Forskrift om valg til Sametinget

http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20081219-1480.html

2.1.7. Lov om behandling av personopplysninger (personopplysningsloven)

http://www.lovdata.no/all/nl-20000414-031.html

2.2. Rules and regulations for pilots on e-voting

The Ministry may, according to the Election Act section 15-1, carry out pilots in order to evaluate other ways of conducting elections, such as e-voting. The Ministry cannot make exceptions to fundamental democratic principles for the conduct of elections. In trials on e-voting exceptions from the Election Law is necessary. Rules and regulations for pilots on e-voting in 2011 will therefore be formulated in separate provisions given by the Ministry.

2.3. Open source code licensing

Identifier	Requirement description
MC2	The ownership of copyright and other related rights for software components developed for the Customer is transferred to the Customer in line with clause 10.1.1 of the main agreement. Any software developed by the Contractor, including standard software, shall be open source. The term «open source» is limited to mean that the source code shall as a minimum be made available to the Customer. The core system, i.e. those parts directly involved in e-voting or counting of e-votes or that otherwise use, store or manipulate election data where no paper audit trail exists, shall be open source. However, third party closed source standard components are allowed in the core provided certification requirements, as set out below, are met. With the exception of third party closed source standard components, the core system components must as a minimum be licensed to allow the Customer to make the source code available to the public and allow anyone to copy, modify, inspect, compile, debug and run the core for testing purposes. With the exception of third party closed source standard components, the license to all system components must as a minimum allow the Customer or anyone the Customer authorizes to copy, modify, inspect, compile, debug, run and make available the source code and derivative works based on the source code for use in academic research or for further development of the system for use in Norwegian elections. To avoid doubt, for third party standard components, the requirement for open source or a relevant certification applies only to core software components. The open source requirement and the certification requirement does not apply to third party software used for backup, monitoring or similar operational tasks. Nor does the open source requirement and the certification requirement apply to third party ICR/OCR-software, as a paper audit trail will exist. Database software that uses, stores or manipulates election data, cryptography software and card-reader software is considered a part of the core, and thus the open source requirement or the certification requirement for third party closed source standard components applies.

	The operating system on which the system runs shall either be licensed under a generally recognized open source license that is accepted by The Open Source Initiative or meet the same certification requirements as set out below for closed source core components.
MC3	It must be possible for anyone to compile the open source components of the core system, but not necessarily to set up a complete e-voting system.
MC4	For all components in the system, the use of a generally recognized open source license that is accepted by The Open Source Initiative is *preferable* to closed source.
MC5	Closed source core components, must hold a relevant, recognized security certification, that is a Common Criteria EAL 4 or FIPS 140-2 Security Level 2 or higher certification. Closed source core components in the process of being certified for the aforementioned certifications are also acceptable. A Common Criteria or FIPS 140-2 certification will make certain assumptions about the operating environment, which must be taken into account. Exceptions may be made for third party hardware device drivers if no viable certified or open source alternative exists. Such exceptions must be identified and a proper justification given in the elaborations to this requirement.

2.4. Implementation environment of the system

Identifier	Requirement description
MC6	The operations partner is yet to be decided. The Contractor must describe the conditions for running the system as defined by the requirements.

3. Naming Conventions and Definitions

3.1. Dictionary

English	Norwegian	Explanation
Accepted vote	Godkjent stemmegivning	A vote that has been approved according to the law
Advance vote	Forhåndsstemme	A vote that is cast prior to Election Day
Air gap	Luftrom	An air-gap shall ensure that a secure network is completely physically, electrically, and electromagnetically isolated from any other computer network.
Authentication	Autentisering	The provision of assurance of the claimed identity of a person or data
Authorized individual	Autorisert individ	An individual that has been given a certain role in the system.
Ballot/Ballot paper	Stemmeseddel	The legally recognized means by which the voter can express his or her choice of voting option
Ballot box	Urne	Where the ballots are stored until being counted. The ballot box can be physical and electronic.
Brønnøysund Register Centre	Brønnøysundregistrene	A registry of all Norwegian organizations and their authorized officers.
Candidate		Person representing a party/group listed for election.
Cast vote	Avgi stemme	Submission of vote
Central system administrator		A system administrator which have access to configure at all levels
Common Criteria	En internasjonalt anerkjent standard for evaluering av sikkerheten i programvare	An internationally recognized standard for evaluating the security in software products
Constituency	Valgkrets	An election area within a municipality or a county.
Contest		Contest is an element from the Election Markup Language (EML) Version 5.0. A contest relates to the seats within a constituency the various parties/candidates are competing for in an election. A contest may vary depending on the type of election. (E.g. Parliamentary election is divided into many

English	Norwegian	Explanation
		contests – one for each county). For further description of EML schemas – see http://docs.oasis-open.org/election/eml/v5.0/cs01/EML-Schema-Descriptions-v5.0.html#_Toc172600803
Corrected vote	Rettet stemmeseddel	The legal term for a vote with changes made by the voter (e.g strike outs and/or personal votes)
County	Fylke	
County Council	Fylkesting	
County Council Election	Fylkestingsvalg	
County Electoral Committee	Fylkesvalgstyre	Electoral Committee – County level
Cover envelope	Omslagskonvolutt er fellesbetegnelse for konvolutt som benyttes ved forhåndsstemmegivning, utenlandsstemmegivning og for stemmegivninger lagt i særskilt omslag på valgdag)	Cover envelope is a term describing the physical envelope concealing: 1. Votes received on Election Day including: a. Voters that have cast an advance paper vote b. Voters that do not exist in the Electoral Roll of the municipality 2. Advance votes including: a. Domestic votes b. Votes from abroad
DIFI	Direktoratet for forvaltning og IKT	The Agency for Public Management and eGovernment
Directorate of Taxes	Skattedirektoratet	
Distribution of seats	Fordeling av mandater	
eID / electronic ID	En metode for elektronisk identifikasjon og signatur	A method for electronic identification and signature
Election	Valg	Election is an element from the Election Markup Language (EML) Version 5.0. An Election relates to the characteristics describing an actual election/referendum (E.g. Parliamentary election, Sami election etc.). For further description of EML schemas – see

English	Norwegian	Explanation
		http://docs.oasis-open.org/election/eml/v5.0/cs01/EML-Schema-Descriptions-v5.0.html#_Toc172600803
Election Auditor	Person eller personer med oppgave å revidere valget	Person(s) tasked with auditing the election
Election Element	Valgelement	Election entity used in EML. Examples of election elements are: Election event, Election and Contest.
Election Event	EML entitet som beskriver karakteristikker ihht valgperiode	Election Event is an element from the Election Markup Language (EML) Version 5.0. An Election Event relates to the characteristics regarding the period in which an election/referendum is held. (E.g. Parliamentary election in 2009). For further description of EML schemas – see http://docs.oasis-open.org/election/eml/v5.0/cs01/EML-Schema-Descriptions-v5.0.html#_Toc172600803
Election Law	Valgloven	
Election Regulation	Valgforskriften	
Election System	Valgsystem	The Election System is a total election management system that encompasses all use cases
Electoral Committee	Valgstyre	Electoral Committee – Municipality level
Electoral manual	Valghåndbok	Practical guidance to complete election
Electoral Roll	Manntall	A registry of all eligible voters in Norway.
EML Schema		A schema related to EML. The schemas have a three digit number.
e-election or e-referendum	E-valg eller folkeavstemning	A political election or referendum in which electronic means are used in one or more stages
e-vote	e-stemme	A vote that is cast electronically
e-voting	e-stemmegivning	An e-election or e-referendum that involves the use of electronic means in at least the casting of the vote
Final count	Endelig opptelling	Final count is the last count conducted by county or municipality.

English	Norwegian	Explanation
Final e-Vote	Tellende stemme	The last e-vote cast by a voter.
FIPS-140-2	FIPS-140-2, en amerikansk standard for evaluering av kryptografiske produkter	An American standard for evaluating cryptographic products.
Hardware security module	Hardware sikkerhetsmodul	Used to protect and store cryptographic keys
Hashing algorithm	En algoritme som basert på en melding av varierende lengde produserer en streng av en fast lengde. En enveis hashalgoritme brukes for å produsere en streng som ikke kan benyttes for å utlede den opprinnelige meldingen.	A hashing algorithm takes a variable length data message and creates a fixed size message digest. When a one-way hashing algorithm is used to generate the message digest the input cannot be determined from the output.
Increased share of the poll	Stemmetillegg	Term used for predefined prioritized candidates on list proposal.
Import schedule	Tidsplan for import	Import schedule refers to the date/time and frequency of imports from separate system(s)
List proposal	Listeforslag	A proposed list of all candidates from a party or group standing in a particular election.
List proposal Candidate	Kandidat på et listeforslag	
Local system administrator	Lokal systemadministrator	A system administrator which have access to configure at a local level
Mark off in Electoral Roll	Kryss i manntall for endelig godkjent stemmegivning	Mark off in the electoral roll for final approval of votes.
Member	Valgt kandidat	Elected Candidate
Ministry of Local Government and Regional Development	Kommunal- og regionaldepartementet	

English	Norwegian	Explanation
Municipal Council	Kommunestyre	
Municipal Council Election	Kommunestyrevalg	
Municipality	Kommune	
National Electoral Committee	Riksvalgsstyret	
N-version architecture	Systemarkitektur som skal gi høy grad av sikkerhet ved at de samme dataene behandles i parallell av N ulike undersystemer og resultatene sammenliknes. Avviker resultatene, foreligger en feil og mindretallsresultatet utelukkes. Kan betraktes som en spesiell form for redundans.	A system architecture used when the tolerance of program errors is extremely low. The same inputs are given to N different sub-systems and results are compared. If results differ, there is a malfunction in one or mopre of the sub-systems and the minority is shut out. May be regarded as a particular form of redundancy.
Optical reader	Utstyr som leser trykte og skrevne tegn, evt. strekkoder, fra papir og omsetter disse dataene til bitmønstre.	Device for reading printed or handwritten symbols or barcodes from paper and translating these to bitmaps.
Out-of-band	Kommunikasjon sies å være ”out-of-band” når et svar sendes tilbake på en annen kanal enn forespørselen ble sendt på. Eksempelvis kan en SMS være et out-of-band svar på en forespørsel innsendt over Internett. Teknikken benyttes for å gjøre det (mye) vanskeligere å avlytte kommunikasjon.	Communications are out-of-band when a response is sent back on a different channel than the request was received on. For example, an SMS-message may be an out-of-band response to a request sent across the Internet. The technique is used to make it (a lot) more difficult to intercept communications undetected.
OWASP Top Ten	Open Web Application Security-prosjektet publiserer med ujevne	The OWASP Top Ten is a list of the 10 most dangerous current Web application security flaws, along with effective methods of dealing with those flaws. OWASP (Open Web

English	Norwegian	Explanation
	mellomrom en liste over de 10 vanligste sikkerhetsfeilene i web-applikasjoner, samt metoder for effektivt å løse slike feil.	Application Security Project) is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications.
Party	Parti	Political party registered in The Register of Political Parties according to The Political Parties Act.
Polling Card	Valgkort	Unique voter identifier consisting of voter information extracted from the Electoral Roll Example: 
Polling Committee	Stemmestyre	Responsible for conducting voting at the polling station.
Polling station	Valglokale	
Population Registry	Folkeregisteret	
Preliminary Mark off in Electoral Roll	Foreløpig markering i manntallet i påvente av endelig godkjenning	Preliminary mark off is a term used for a vote that awaits final approval (Status before the vote is approved).
Preliminary result/count	Foreløpige resultater/opptelling	Provisional results/count
P-vote	Papirstemme	Vote cast on a paper ballot.
Referendum	Folkeavstemning	
Regulation	Forskrift	

English	Norwegian	Explanation
Rejected ballot	Forkastet stemmeseddel	
Rejected vote	Forkastet stemmegivning	
Sami Election	Sametingsvalg	
SAML 2.0 protocol	Protokoll for føderering av autentisering fra en sentral produsent til distribuerte konsumenter	Security assertion markup language, a protocol for federating authentication from a provider to a consumer.
Seat	Plass (mandat)	
Securable object	Sikkerhetsobjekt	An object within the application which can be set up with its own combination of roles and permissions. A securable object can be a web page, a control on the page, a record within the application etc.
Signature (Signer ID)	ID til person som har signert for listeforslag	ID (Name and/or personal identification number) of person that has signed their name on a list proposal
St. Laguës modified method	Metode for beregning av mandater	Method for distribution of seats between the electoral list.
Storting Election	Stortingsvalg	Parliament Election in Norway
Strong authentication		Two factor authentication or better
Submitted vote	Avgitt stemme	See ‘cast vote’.
The Register of Political Parties	Partiregisteret	Managed by Brønnøysund Register Centre
User	Bruker	A person accessing the system
Valid e-Vote		The latest e-vote cast by a given voter, under condition that the e-vote is not overridden by a higher priority vote (e.g. a p-vote or an e-vote cast in an controlled environment)
Vote cast in another constituency	Fremmed stemme	Vote cast in a constituency where the voter is not enlisted.
Vote with adjustments	Rettet stemmeseddel	See ‘corrected vote’.

English	Norwegian	Explanation
Voting channel	Valgkanal	The way by which the voter can cast a vote
Voting period	Stemmeperiode	The period in which polls are open

3.2. Abbreviations

English	Norwegian	Explanation
AGM		Air Gap Module
AI		Authorized individual (Approver of configuration)
API	Programmerings-grensesnitt	Application Programming Interface
CAI	DIFIs autentiseringsportal	Common Authentication Infrastructure
CEC		County Electoral Committee
EML		Election Markup Language
ES		Election System
HSM	Maskinvarebasert sikkerhetsmodul	Hardware security module
KRD	Kommunal- og regionaldepartementet	Ministry of Local Government and Regional affairs
NER	Landsdekkende mantal	National Electoral Roll
PC		Polling Committee
RPA	Valgloven	Representation of the People Act
SKD	Skattedirektoratet	The Norwegian National Tax Authority Owner of folkeregisteret
SSB	Statistisk Sentralbyrå	Statistics Norway Provides the public and organisations with statistics such as election results

4. General requirements

4.1. Technical requirements

Identifier	Requirement description
GR1.1	All system components shall communicate across open and well defined interfaces, such as EML.
GR1.2	The system shall have an architecture facilitating the easy replacement of system software components.
GR1.3	The system source code shall be well commented and documented, and easily maintainable.
GR1.4	The Elections System shall be able to exchange daily updates of the Electoral Roll in a structured format with systems delivered to other municipalities by other vendors.
GR1.5	In the event of a loss of communication, the Electoral Roll shall still be available locally on client PCs in polling stations. The local copy of the Electoral Roll shall automatically synchronize with the central master copy on restoration of communication. The user in the polling station shall be notified of the loss of and restoration of communications.

4.2. A Security Methodology

To achieve real security, the entire software development lifecycle must be security conscious. A secure software development life cycle process (SSDLC) takes threats, vulnerabilities and mitigation into consideration from the initial feasibility studies and through development, testing, deployment and maintenance. A number of SSDLCs exist, and the Contractor shall document the process according to which they will work.

For the purposes of certification and security testing, detailed design documentation is required. The Contractor shall therefore be certified to, or work according to ISO 27001, and prepare the required documentation for the specified Common Criteria assurance levels.

Identifier	Requirement description
GR2.1	The supplier shall be certified to, or work according to ISO 27001
GR2.2	The supplier shall have documented and implemented a Secure Software Lifecycle Development process
GR2.3	The supplier shall in the development process create the necessary documentation for a formal review process and Common Criteria certification to EAL4+ of all components directly related to e-voting, including counting and returning of members.
GR2.4	The supplier shall in the development process of Election System components *not* directly related to e-voting create the necessary documentation for a Common Criteria certification to EAL2.

4.3. Scope for deliverables and implementation

4.3.1. Part deliverables 2010

Identifier	Requirement description
GR3.1	The system must be divided into partial deliveries. Each delivery must be a complete subsystem. It must be possible to perform part acceptance tests on each partial delivery.

4.3.2. Final acceptance test November 2010

Identifier	Requirement description
GR3.2	The system must be ready for customer acceptance test November 1st 2010 (full scale, all elections). All customer acceptance tests and all vendor correction of system errors, and regression tests should be finished within December 31th 2010.

4.3.3. Pilots 2011

The full system shall be tested in 3-10 pilot municipalities and a single county for the election in September 2011. The local municipalities will be selected in December 2009. In addition, we might include ex-patriot voters abroad in the pilot. We are planning for a total of 200 000 possible voters. This number of possible voters might increase, especially if including foreign voters.

Identifier	Requirement description
GR3.3	First deadline is submission of list proposal from the political parties is March 31th 2011. The system must be configured and ready for use by the local communities from March 1st 2011.
GR3.4	The Principal has an option to order services to assist the local Municipalities in the following: system support 24/7 from July 1st, user training, e-counting support (24/7 for one week).

4.3.4. Full implementation after 2011

The pilots will be evaluated, and the implementation plan will be decided in 2012.

Identifier	Requirement description
GR3.5	The system must scale for full implementation in Norway.
GR3.6	The Principal must have an option to acquire software licenses for full scale implementation if this is not included in the software delivered for the pilots in 2011. The Principal prefer to have a license for unlimited use in Norway. But if such license is not offered, the Contractor must base pricing e-counting on 200 scan-centers with the average of 3 scanners (600 scanners totally).

4.3.5. Work conditions

Identifier	Requirement description
GR3.7	The Contractor's core team must be located in Oslo, Norway.
GR3.8	The Contractor must provide an office in Oslo, Norway, with work space for the core team and meeting facilities.
GR3.9	The Contractor has to cover own expenses for development environment and infrastructure and hardware cost related to their own development and testing.

4.3.6. Services

Identifier	Requirement description
GR3.10	The Contractor *must* provide services to assist the Principal in the following: User training, system support (Working days 08:00-16:00) and central configuration of system.

4.4. Standards for Software Quality and IT Service Management Systems

Identifier	Requirement description
ST4.1	The Contractor shall be certified to or work according to ISO 9001/TickIT (ISO/IEC 12207). Documentation from the Contractor is needed.
ST4.2	The system shall be developed to satisfy the requirements of a data centre operator certified to or working according to ISO/IEC 20000-1 and ISO 27001. Documentation from the Contractor is needed.
ST4.3	For work covered by the Maintenance Agreement-option, the Contractor shall be certified to or work according to ISO/IEC 20000-1. Documentation from the Contractor is needed.
ST4.4	The Contractor shall describe the methodology and development infrastructure including tools used for software development, source control, build and release management.
ST4.5	The Contractor shall describe their test strategy including methodology and tools for testing (usability testing, unit testing, accessibility testing, system testing, regression testing, volume testing, performance testing, security testing, acceptance testing) bug reporting and change management.

5. System Features

All requirements from this chapter are listed in the requirements table (Excel document).

5.1. Overall workflow

The workflow for the e-voting process is divided in 4 phases (see figure below). Each of them consists of one or more processes.

Phase 1: Preparations
- Configuration of Election System
- Definition of Roles
- Submission of list proposals
- Processing list proposals

Phase 2: Voting
- E-voting
- Manual registration of p-votes in Electoral Roll

Phase 3: Counting
- Approval of votes and ballots
- Counting e-votes
- Manual registration of p-vote results
- Electronic counting of p-votes

Phase 4: Settlement
- Settlement

Some processes cover more than one phase. They are:

Phase 1-3:
- Create/ update Electoral Roll

Phase 1-2:
- Exception process Electoral Roll

Phase 1-4:
- Auditing
- Authentication
- Reports

Figure 1: Workflow for e-voting

5.2. Use Cases

A complete Use Case description is given in separate Use Case documents. The Use cases are:

0.1 Definition of roles
0.2 Configuration of The Election System
0.3 Electoral Roll
0.4 Exception process for listing in Electoral Roll
1.1 Submission of list proposals
1.2 Processing list proposals

2.1 E-voting
3.1 Registration of p-votes in Electoral Roll
3.2 Manual registration of p-vote results
3.3 Electronic counting of p-votes
3.4 Counting e-votes
3.5 Approval of p-votes and ballots
4.1 Reporting of results to SSB
4.2 Settlement
5.1 Reporting
5.2 Auditing
9.1 Authentication

The symbols used in the process models in the Use Cases are explained below.

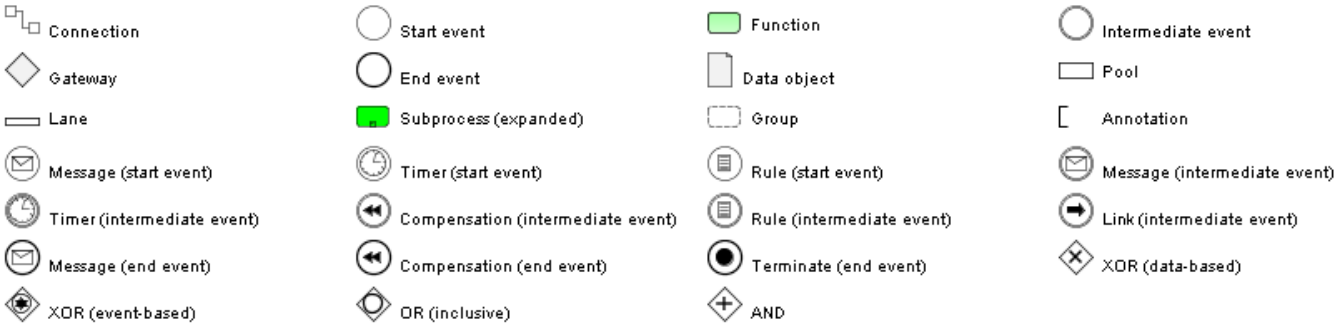

Figure 2: Business Process Management Notation

Each Use Case contains a number of functional and non-functional requirements. These requirements are also listed in the requirements table (Excel document).

For a short explanation to the Use Cases, we have below repeated the Executive Summary from the Use Case documents.

5.2.1. 0.1 Definition of roles

In order to meet security objective OS 7 (Ref [2]), the system shall have a role based security model. The system must have functionality that supports:

1. The creation, amendment and inactivation of roles
2. The mapping of users to roles
3. The creation, amendment and inactivation of permissions
4. The mapping of roles to permissions
5. The listing of securable objects
6. The mapping of permissions to securable objects
7. Filtering and searching for users, groups, permissions and securable objects returning the relations between these. The administrator must be able to see what securable objects the various roles/users have access to and what their access level is in relation to that object.

5.2.2. 0.2 Configuration of The Election System

The system shall include a 'configuration module' which allows central/local administrators to:

1. Create a new configuration for an election/referendum. It must be possible to create a new configuration based on an existing configuration (With or without template data)
2. Amend an existing configuration

Configuration includes:

1. The creation and maintenance of Elections (General Election, County Election, Municipality Election, Referendums, and Sami Election) system data based on the EML schema using relevant EML elements and attributes. The current version is described in Election Markup Language (EML) Version 5.0. The user must be able to set attribute values describing the characteristics of the election/referendum.
2. Create and/or maintain Party/Group details, codes, roles etc.
3. The creation and/or maintenance of system terms and the translation of these (Captions, menu texts, help texts, error messages etc.). It must be possible to create a new language, copy all existing terms and export these for translation. The system must also facilitate the import of translated terms. Norwegian Bokmål, Nynorsk and English terms must be translated and available in the system for the 2011 election.
4. The creation and/or maintenance of roles (See use case 0.1 'Definition of roles')
5. The creation and/or maintenance of reports (See use case 5.1 'Reporting')
6. The creation and/or maintenance of workflows (Approvals, alerts etc.)
7. The creation and/or maintenance of rules (See 'Representation of the People Act')
8. The creation and/or maintenance of layouts for ballot papers and polling cards
9. The configuration of external interfaces and web services (Electoral Roll, Interface to SSB etc.)
10. The import/export of a configuration (EML/XML).

The system shall also facilitate the approval of a new configuration or the approval of amendments made to an existing one.

5.2.3. 0.3 Electoral Roll

The system shall include a service providing Electoral Roll updates from the Population Registry during the election period. The Directorate of Taxes provides the Electoral Roll schema based on a specification supplied by the Ministry.

5.2.4. 0.4 Exception process for listing in Electoral Roll

The system must have functionality for handling voters that are not enlisted in the Electoral Roll. The voter must be able to fill in an application which is submitted to the Electoral Committee for approval. The Electoral Committee must be able to:

- Approve or reject the application
- Update the Electoral Roll

The voter shall be notified whether their application has been approved or rejected.

5.2.5. 1.1 Submission of list proposals

The system must facilitate the submission of list proposals by political groups and parties for an election. The format of the lists proposals is based on a pre-configured template (See use case 0.2 'Configuration of the Election System'). The following functionality must be available:

1. Manual data entry/import of list proposal candidates
2. Verification of candidates against the Electoral Roll
3. Duplication check of candidates
4. Registration of list proposal signatures (Signer ID)
5. Verification of signatures against the Electoral Roll
6. Duplication check of signatures
7. Approval of list proposal by representatives from party/group
8. Publishing of list proposals to the general public
9. Notification to all candidates that they have been added to the list proposals.

5.2.6. 1.2 Processing list proposals

After the list proposals have been submitted by the parties/groups, the Electoral Committe must be able to:

1. View submitted list proposals
2. Approve/reject list proposals
3. Edit candidates and signatures
4. Publish approved parties

5.2.7. 2.1 E-voting

The system must facilitate a secure and user friendly environment for the submission of e-votes. The system shall guide the user through a set of steps where:

1. The voter is authenticated (See use case 9.1. authentication)
2. The system checks voter against the Electoral Roll
3. The system presents valid elections/referendums based on voter rights
4. The voter selects election/referendum options, makes adjustments and cast their vote
5. The system makes a mark off against the voter in the Electoral Roll and flags whether the vote has been cast in a controlled or uncontrolled environment
6. The vote is stored securely in the system

The voter shall be able to cast a vote any number of times within the voting period/phase. The voter must also be able to cast votes for any number of elections within a session.

The system shall notify voters that do not exist in electoral roll. The notification message shall describe the process for applying for membership in electoral roll. See use case 0.4 'Exception process for Electoral Roll' for the exception handling process.

5.2.8. 3.1 Registration of p-votes in Electoral Roll

The Polling Committee/Electoral Committee must be able to check and mark off voters against the Electoral Roll for both advance votes and votes received on Election Day. The system must also facilitate the registration of exceptions. Exceptions are:

1. Votes from voters that do not exist in the Electoral Roll
2. Votes from voters that do not exist in the Electoral Roll of the municipality
3. Votes from voters that have already cast an advance p-vote

5.2.9. 3.2 Manual registration of p-vote results

The election system must facilitate the entry and approval of p-vote results. The Polling Committee, Electoral Committee, and County Electoral Committee must be able at various stages to enter:

1. Advance results:
    a. Preliminary results (Party totals)
    b. Final results (Party and candidate totals)
2. Election day results:
    a. Preliminary results (Party totals)
    b. Final results (Party and candidate totals)

5.2.10. 3.3 Electronic counting of p-votes

The system must have functionality for the optical character recognition of image files produced during scanning. The relevant Committee must be able to enter file metadata describing ballot characteristics that cannot be read from the image. The system must be able to pick up exceptions where recognition fails and allow for validation and correction.

The election system must facilitate the scanning of ballots providing:

1. Advance results:
    a. Preliminary results (Party/group totals)
    b. Final results (Party/group and candidate totals)
2. Election day results (Party/group and candidate totals):
    a. Preliminary results (Party/group totals)
    b. Final results (Party/group and candidate totals)

5.2.11. 3.4 Counting e-votes

The system shall facilitate the secure and verifiable counting of e-votes, while safeguarding the principles of one voter/one vote maintaining the secrecy and anonymity of the vote. The system must have functionality for the counting valid e-votes maintaining the rules that:

    a. P-votes overrides any e-votes
    b. E-vote cast in a controlled environment overrides any e-votes later cast in an uncontrolled environment

5.2.12. 3.5 Approval of p-votes and ballots

The system must facilitate the approval of:

3. Votes and ballots received in a cover envelope. Votes received in cover envelopes are:
    a. Votes received on Election Day including:
        i. Voters that have cast an advance paper vote
        ii. Voters that do not exist in the Electoral Roll of the municipality
    b. Advance votes including:
        i. Domestic votes
        ii. Votes from abroad
4. Ballots received on Election Day. This includes questionable ballots (that may not meet the requirements §10-3) identified by the Polling Committee.

The Electoral Committee is responsible for the approval of votes and ballots.

Rejected votes and ballots must be stored in the system with a reason. Approved votes and ballots will form the basis for the use cases 'Electronic Counting of p-votes' and 'Manual registration of vote results'.

5.2.13. 4.1 Reporting of results to SSB

The system must facilitate the export of data (system data and results) according to formats defined by SSB The system must facilitate the export of data (system data and results) according to formats defined by SSB (See attachment from SSB 'File import election 2009'). It is expected that all system data and reports are available for export in the predefined formats. The system shall receive a confirmation from SSB regarding whether the data transfer succeeded or failed. The list below shows an example of data that may be transferred to SSB:

System data:

1. Configuration data (Party codes, contest information etc.)
2. List proposals

Election results:

1. Preliminary advance p-vote results
2. Final advance p-vote results
3. Preliminary Election Day results
4. Final Election Day results
5. E-vote results County
6. Total settlement (Municipal council election, Council election, Parliament election)

An export to SSB is triggered by the Electoral Committee, the County Electoral Committee or the National Electoral Committee.

5.2.14. 4.2 Settlement

The system must facilitate a secure and reliable method for merging of e-votes and p-votes (Calculate total distribution on parties and candidates).

- E-vote results are available for merging on completion of use case 3.4 'Counting e-votes'.
- P-vote results are available for merging at various stages throughout the election. See use cases 3.2 'Manual registration of vote results' and 3.3 'Electronic counting of p-votes'.

The system must be able to use these results for the distribution of seats and returning of members.

Use case 5.1 'Reporting' and use case 'Reporting of results to SSB' describes the output formats required for merged and distributed results.

5.2.15. 5.1 Reporting

The system must have a 'report design module' which allows authorized individuals to design, edit and delete reports. The 'report design module' shall provide alternate modes so that the user can choose whether to work in visual mode or directly in the query language. Reports may be designed at any phase in the process (Prior to, during and after an election/referendum,) and for all kinds of data within the system (System data, election results etc.).

The Electoral Committee must be able to open a reporting module, find and select reports from any election/referendum, run these reports and manipulate the results in terms of filtering, sorting and grouping of data. The system must present functionality for export of report results (SSB) and functionality for saving report results to the system or locally on a PC in various formats (XML, EML, format required for the production of ballot papers, formats required for publishing information on public portals etc.). The system shall also have functionality for saving the reports to a location where they can be downloaded by authorized individuals (For printing).

The system must be able to produce reports of the records of Elections (§10-7 'Representation of the People Act'). For further details, see send out 2 (AS – IS Process Models & Preliminary functional requirements TO - BE, chapter 4) and send out 3 (Functional specification TO-BE and Preliminary functional requirements, chapter 2.5). Further requirements for the records are detailed in chapter 9 in regulations relating to parliamentary and local government elections (Representation of the People Regulations).

5.2.16. 5.2 Auditing

The system shall provide an 'audit module' with easy access to all audit logs. The audit module must have functionality for:

1. Logging of all events. All logs must be immutable.
2. Accessing, filtering and searching in audit logs
3. Creating audit reports
4. Detecting abnormal behaviour and present warning messages (Monitoring agent)
5. Functionality for configuring monitoring parameters

The auditing of the election system comprises two parts:

1. The audit of the actual election must show exactly what happened and when it happened.
2. A technical audit shall ensure that the election system is set up as agreed, and that only approved and audited software is running on the system.

5.2.17. 9.1 Authentication

The system must facilitate the authentication of all users. The system shall interface with a common identity provider operated by DIFI, which in 2011 will provide authentication and signing services. It federates authentication over the SAML 2.0 protocol. The system must have functionality for:

1. Log in using approved electronic Ids
2. Login using temporary ID within a controlled environment (For voters that have arrived at the Polling Station without approved ID)

Login using other strong authentication method for other systems (e.g. Air gapped systems)

6. Accessibility and Usability

The requirements for accessibility and usability are described in “Accessibility and usability requirements.doc”. They are also listed in the requirements table (Excel document).

The document gives specific requirements related to:

- Adherence to WCAG 2.0
- ELMER 2
- Cross-platform independence
- Methods for testing and evaluating accessibility and usability
- Method for the design process
- Other accessibility and usability requirements

.

.

7. Security

7.1. Introduction

Well functioning elections are fundamental to any democracy and the rewards of e-voting are limited. As such the level of acceptable risk in introducing e-voting is very low, and all efforts must be made in the system development to ensure that the residual risk is as low as reasonably possible (the ALARP-principle).

Security in the context of e-voting is a complex and wide ranging subject. Solutions to what are really functional requirements of an e-voting system, such as preserving the anonymity of the voter, the secrecy of the ballot and the impossibility of ballot stuffing, are best evaluated using information security methodologies. Hence these requirements are left in the hands of information security specialists. Delivering a truly secure and future proof e-voting system is a daunting task indeed. The high level threat model described in the Security Objectives assumes that the client is under the control of an attacker. This means that we cannot rely on the integrity of information submitted by or presented on the client. The voter may therefore be presented with a manipulated ballot, or the ballot may be manipulated after the voter has confirmed his or her choice, but prior to encryption. For this reason it is an absolute requirement that the voter be able to verify that a ballot has been lodged in an integral state, correctly representing the voter's intent. This must happen without decryption of the vote by the server side, and prior to the end of the voting period, to ensure that the voter can take appropriate action if he/she discovers that it has been manipulated.

Furthermore it is of vital importance that the counting of e-votes be a transparent and painstakingly correct procedure, where no one can legitimately question the result. Ideally, the system will be able to somehow prove the end-to-end correctness of the result (i.e. that every valid vote was counted as the voters intended). Any and all measures must be taken to ensure that no single person - application developer, systems operator or election officer - is in a position to compromise the integrity or anonymity of the election. Possible solutions include multi party computations and N-version architectures.

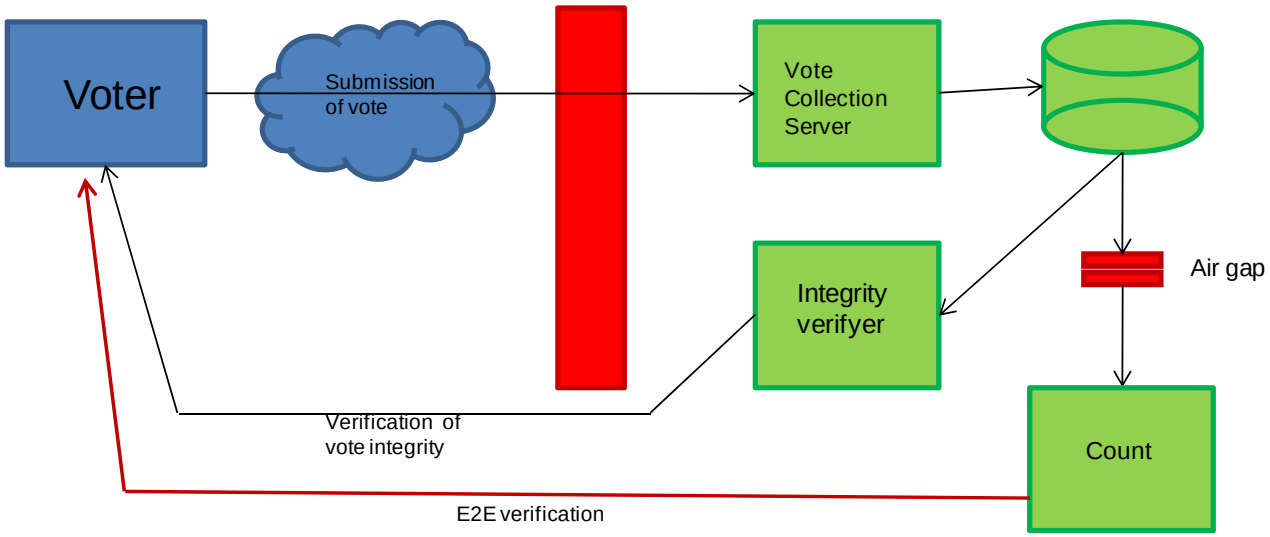

Figure 3: A high level e-voting security architecture

7.2. Security Objectives

For the final invitation to tender, the Security Objectives have been updated – mainly to reflect the full scope of the project, as the security architecture needs to address the requirements of a full elections administrative system.

The Security Objectives describe the security domains to be secured, and the security control objectives to be met by the Elections System:

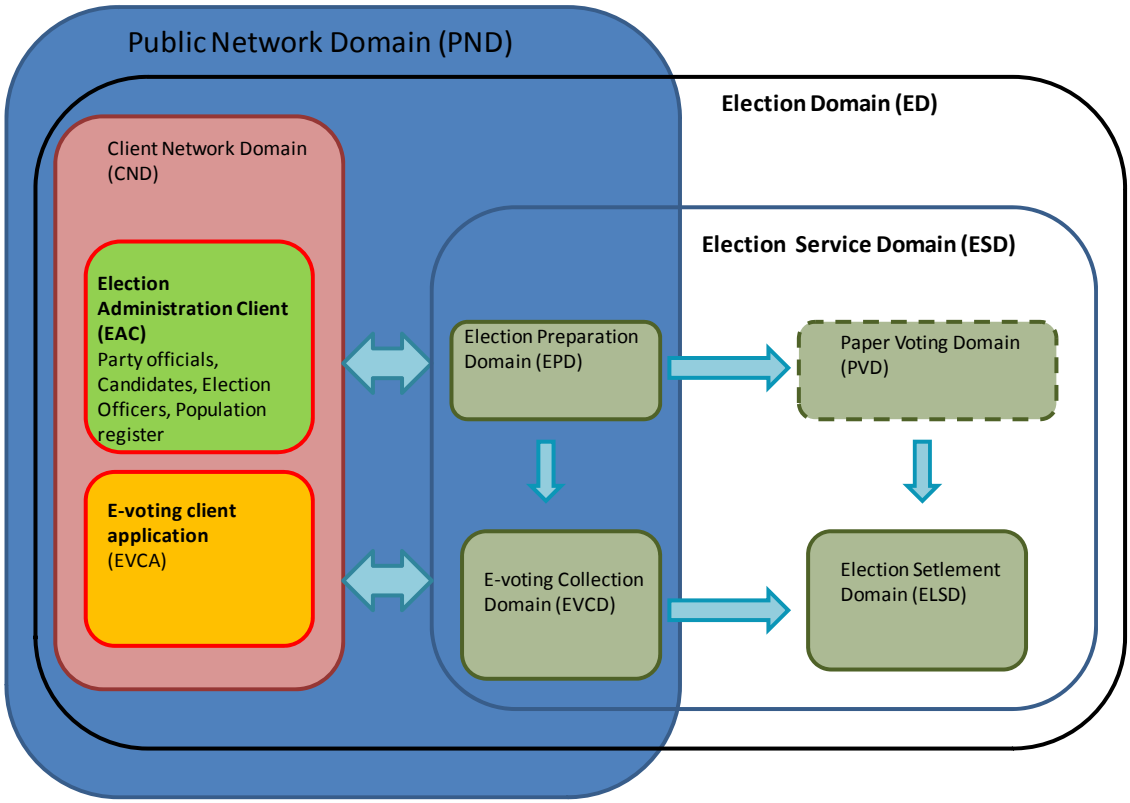

Figure 4: Election System security domains

- **Election Domain (ED)** contains all the Election and Voting Services 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 services, the e-voting collection services, as well as the election settlement services.

- **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 ELSD to facilitate the anonymity of the ballot.
- The **Election Settlement Domain (ELSD)** 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 ELSD shall be off-line (air gapped).
- The **Client Network Domain (CND)** is that element of the infrastructure under client control, which is used to support access to the Election Service. The CND may be a municipal LAN used to access the EPD or a single domestic personal computer used to access the EVCD.
- **Election Administration Client (EAC)** contains functions for election 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.

14 security control objectives to be met by the Elections System have been defined:

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 an approved authentication scheme at the national authentication portal or possibly an equivalent foreign e-ID.
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	A combination of technical, procedural and

Security Control Objective	Notes
E-voting services must guarantee the confidentiality of the vote.	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 ESD, 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 ESD, 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 ESD, 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.

The principal external assumptions that relate to the provision of e-voting services are tabulated below:

External Control Objective	Notes
Open Delivery	The requirement is that no government

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

External Control Objective	Notes
e-voting services are delivered over public networks over which the e-voting service provider has little or no control.	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.

7.3. Requirements

The security requirements have been formulated to reach the security control objectives while taking into consideration the external control objectives.

With regards to the requirements, emphasis is on the properties of the desired solution, not the implementation. Tenderers should find that there is generally a considerable degree of freedom in terms of how you choose to satisfy a particular requirement. However it should be noted that your proposed solutions will be evaluated in depth. Hence, if your proposal includes the re-use or modification of existing components, it is necessary for you to provide the required technical design documentation to enable an in depth evaluation. Any new or custom created cryptographic protocols must be fully documented.

All security requirements apply to the entire Elections System at all times. However, in certain use cases, certain security requirements have been given special emphasis. **This does not mean that only these requirements apply to this particular use case, or that these requirements only apply to this use case.** It only serves to emphasize the importance of a particular requirement in a particular context.

The Requirements Table, containing all security requirements, is enclosed with this document as Appendix 2A.

8. External Interface Requirements

The purpose of this chapter is to provide an overview of requirements regarding interfaces to other systems and external entities within the project scope. This is used to estimate the effort required to develop and implement external interfaces. All external interfaces, with the exception of The Register of Political Parties, involve re-using existing, established and well defined interfaces.

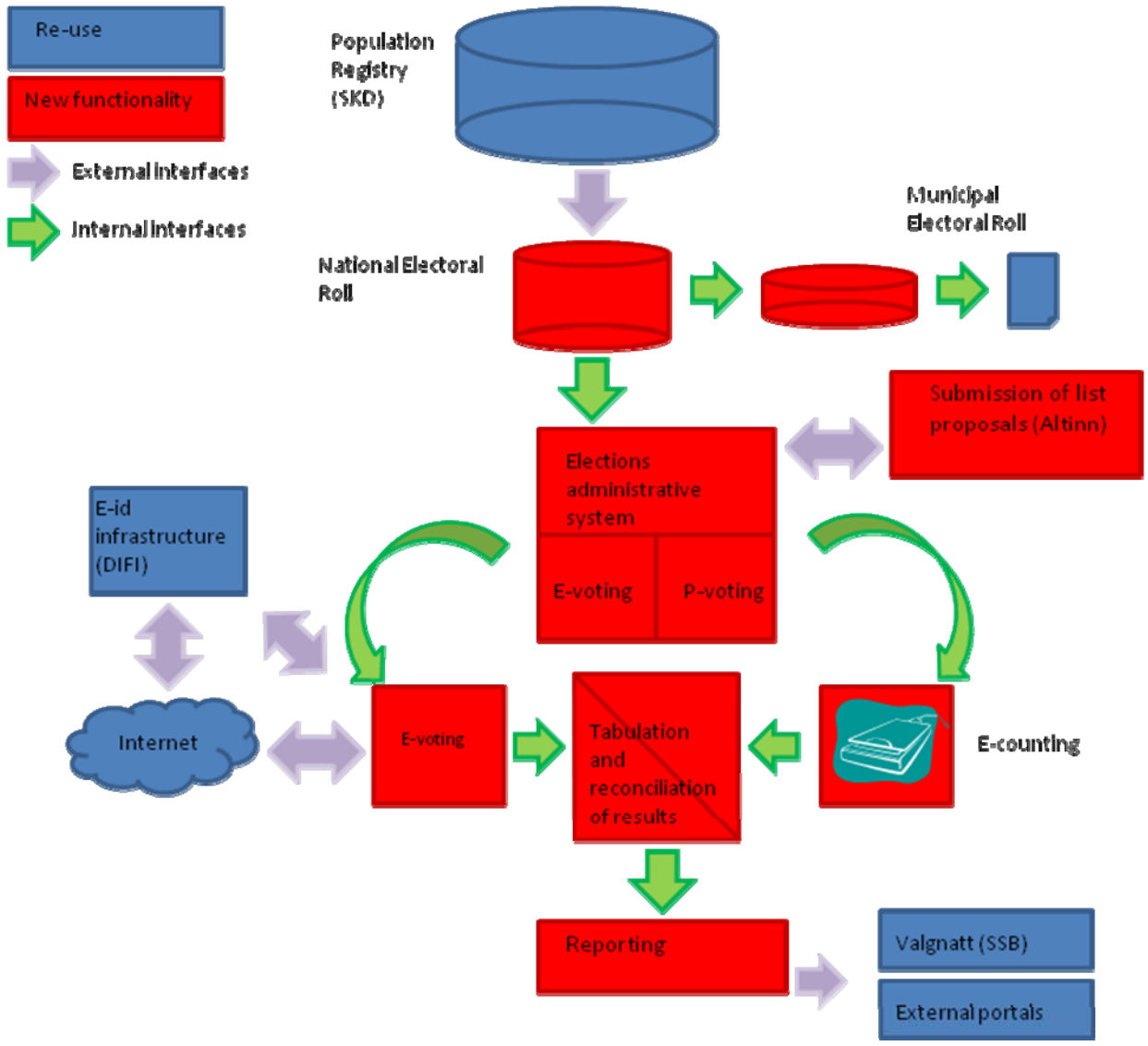

Figure 5: Interface model

8.1. Software

Identifier	Requirement description
EIS1	The system shall interface with the Population Registry for updates of the Electoral Roll during an election. This requirement is detailed in use case 0.3.
EIS2	The system shall interface with SSB for election results and other election data. This requirement is detailed in use case 4.1 Reporting of results to SSB.
EIS3	The system shall interface with external portals for the publishing of list proposals and election results (valgresultat.no). This requirement is detailed in use case 5.1 Reporting.
EIS4	The system shall interface with a common authentication infrastructure. This requirement is detailed in use case 9.1 Authentication. In the event that the CAI from DIFI is not available in 2011, the Elections System may fall back on the Altinn portal, which uses the same interface (SAML v2.0) and technology (Sun OpenSSO).
EIS5	The system shall interface with Altinn for the submission of list proposals (option).
EIS6	The Elections System shall be able to import structured information on count results from systems delivered to municipalities by other vendors for the distribution of seats and reporting on a county level.

8.2. Hardware

Identifier	Requirement description
EIH1	The system shall interface with industry standard scanners (TWAIN and ISIS). This requirement is detailed in use case 3.3 Electronic Counting of p-vote.
EIH2	The system shall interface with printers for the production of polling cards, voting cards etc. This requirement is detailed in use case 5.1 Reporting.

9. Documentation

Three kind of documentation are required:

1. Technical documentation
2. Installation and operational documentation
3. User documentation

The Contractor must specify what the deliveries are intended to be in each category (referring to standards etc).

9.1. Language

Identifier	Requirement description
D1	1. User documentation shall be written in Norwegian ("bokmål" and/or "nynorsk"). 2. All other documentation shall be written in English or Norwegian.

9.2. Technical documentation

This should be system documentation with a detailed description of the system and its manner of operation; that means at least:

1. High level design documents (architecture and design documentation)
2. Documentation of code, algorithms, interfaces, and APIs
3. Certification requirements

Identifier	Requirement description
D2	Describe delivered technical documentation according to Chapter 9 "Documentation" in the "System Requirements Specification" document.

9.3. Installation and operations

This should be installation guidelines with advice as to the choice of set-up and operational documentation with advice as to how operational procedures should be prepared, what back-up copies should be made and how often, what parameters it would be prudent to monitor, etc.

At least this should be:

1. Low Level Documentation (LLD)
2. Installation Guide
3. Configuration Guide
4. Deployment plan

Identifier	Requirement description
D3	Describe delivered documentation for installation and operations according to Chapter 9 "Documentation" in the "System Requirements Specification" document.

9.4. User Documentation

End user documentation is mainly used for education and learning. This is description intended for super user/systems manager that shows the relationship between the various parts of the system, advanced user functions, etc. At least this should be:

1. Description of systems functionality
2. User Guide for administrative officers and key personnel

Identifier	Requirement description
D4	Describe delivered user documentation according to Chapter 9 “Documentation” in the “System Requirements Specification” document.