E-vote 2011

Contractor Solution Specification

Project: E-vote 2011

Change log

Version	Date	Author	Description/changes
0.1	18.09.09		First version

CONTENT

1. Tenderer Solution Proposal

This tender is a delivery from Computas, Acando, Cybernetica and Opt2Vote, Computas being the prime contractor and single point of contact for the Customer. Computas has adopted a "best of breed strategy" in order to deliver a successful implementation of the requirements for the E-vote 2011.

Computas has a long tradition in delivering successful large and complex implementation projects for the public sector in Norway. The most recent and largest is the ongoing implementation of process and information control for The Norwegian Food Safety Authority.

To ensure that core competence related to Electronic Voting is integrated in the resource pool delivering E-vote 2011 to the Customer, Computas has elected the following vendors delivering parts of the overall systems;

- Opt2Vote Ltd (based in Northern Ireland)
- Cybernetica AS (based in Estonia)

In addition Computas AS has elected Acando AS (Norway) as a development partner in order to ensure that sufficient development resources are available throughout the specification and development phase. A brief summary of the companies are provided below.

Computas

Computas AS is a Norwegian software services company, established in 1985 and owned by the employees. Our business idea is to create added value for organizations by providing services, solutions and products to optimize the organizations usage of their knowledge.

Computas has currently 175 employees and the main office is at Lysaker, Oslo. 95 % of the employees have a Masters Degree or higher.

Our main competencies are:

- Process-oriented Workflow
- Knowledge Management
- Project Management
- System integration and Development
- Artificial Intelligence
- Portal Technology and Services
- IT Architecture
- Enterprise Architecture
- Consulting Services

Computas has a 20-year long experience with developing applications for different Norwegian customers and the Norwegian Government in particular. Our specialty is customized applications that have a crucial role in the customer's daily business. Typically this is complicated applications with hundreds of users that should work 24 hours 7 days a week. Our mission critical solutions delivered to UDI, NAV, the Police, the National Courts Administration and the Norwegian Food Safety Authority have been among the largest integration and development projects in Norway.

Computas' contribution to the project is experience and knowledge of how to deliver mission critical solutions to the Norwegian Government.

Company size: 175 employees

Opt2Vote Ltd

OPT2VOTE is one of the premier election service providers in the UK, providing outstanding expertise and knowledge across all areas of election management.

OPT2VOTE specialises in designing and delivering a range of solutions to address the changing needs of the UK electoral services market. Products and services incorporate traditional election services and innovations such as electronic voting by internet and telephone.

OPT2VOTE aims to provide the choice, convenience and simplicity necessary to improve participation and confidence in voting whilst achieving modernisation and advancement of the democratic process.

The OPT2VOTE portfolio includes the following products:

- Registration
- Print
- Postal Vote Management Solution
- Personal Identifier Matching Solution
- E-Counting
- Internet & Telephone Voting
- E-Voting
- Detailed EML knowledge
- Election preparation

Since its foundation, OPT2VOTE has acquired a first class reputation synonymous with quality, reliability and excellence and a proven track record of delivery that speaks for itself:

- Over 10 million Postal Ballots in last 3 years
- Election Services to over 100 local authorities
- Successful delivery of e-voting pilot projects

Opt2Vote's main contribution in the E-vote 2011 implementation is their core competence listed in the Opt2Vote services portfolio above.

Company size: 30 people

Cybernetica AS

Cybernetica is a private research and development company, original equipment manufacturer and solutions provider active in the field of Information and Communication Technologies.

Cybernetica's Department of Information Security focuses on:

- Consulting in the field of information security
- Software for solving information security problems
- Auditing of information systems

Cybernetica's Department of Information Security was established in 1992 to support the realization of the Estonian state information security program. Since then, Cybernetica has participated in several projects initiated by the Estonian state, such as:

- e-voting solution for Estonian National Electoral Committee
- information security and IT-related standardization
- launching of the ID-card project, drafting of the law on digital signature and development of an infrastructure supporting the implementation of the digital signature, including creation of an information system for the public certification registry,
- X-Road: a project environment for secure use of public databanks

Cybernetica is active in the field of cryptographic research. Scientific co-workers have shown substantial results in fields of time-stamping, integrity of databases, secure information flow in programs, analysis of cryptographic protocols, applications of attack trees in the security analysis of system, secure multiparty computation, privacy-preserving data mining. Cybernetica is experienced in providing cryptographic solutions to real-life problems with help of theoretical research.

Export markets: EU, Canada, China, Israel, Malaysia, Norway, Panama, Russia, Singapore, USA

Cybernetica's main contribution in the E-vote 2011 implementation is security and encryption in addition to E-election competence.

Company size: 104 people

Acando AS

Acando is a consultancy company that in partnership with its clients identifies and implements business improvements through information enabled by technology.
Acando provides a balance of high business value, short project times and low total cost. Acando is listed on the NASDAQ OMX Nordic. Acando's corporate culture is based on three core values: Team spirit, Passion and Results.

Acando creates measurable improvements through the development of processes, organisations and IT systems, ensuring that these support the client's operations. It is the task of Acando to acquire an overall view of the client's business and to ensure that each project yields a fast effect and improves the results. The client base is wide and includes small businesses as well as corporations and public authorities.

Acando's main contribution in the E-vote 2011 implementation is open source specification skills and development resources.

Company size: The Group employs more than 1,100 professionals in six European countries. In Norway Acando employ 100 people.

1.1. Overview of Proposed Functional Solution

The Tenderer's proposed solution will be a complete Election system covering integrated modules supporting the required functionality as requested by the Principal.

The Tenderer confirms that the proposed Election system will support the workflow of the Norwegian Election process. The process can be divided into four phases, each covering one or of 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

The Tenderer also confirms that the proposed Election system handles that some processes cover more than one phase:

Phase 1-3:
- Create/ update Electoral Roll

Phase 1-2:
- Exception process Electoral Roll

Phase 1-4:
- Auditing
- Authentication
- Reports

The Tenderer also confirms that the proposed election system will support the following user roles and users:

- **Electoral official user roles:**
  - National electoral committee users
  - County electoral committee users
  - Municipal electoral committee users
  - Local polling committee users
  - Other official users
- **System administrator user roles:**
  - Administrator users (custodian of user base, rights, etc.)
  - Operator users (Technical persons responsible for installation and sustained running of the system)
  - Scanning operators (at the scan centers for Electronic counting and verification of P-votes)
  - Support users (Competent persons helping other users solve problems)
- **Party/group user roles:**
  - Party/Group administrator users
  - Politician users
- **Voter user roles:**
  - E-voter users

- P-voters (both in advance voting and on Election Day)

- **Auditor user roles:**
  - National appointed auditor users
  - OSCE invited auditor users

Figure 1 - User roles in the Election System

The system will also be flexible enough to support the amendment of other user roles and users.

The high level functionality of the proposed Election system, covering all the phases and processes as listed above, can be illustrated like this:

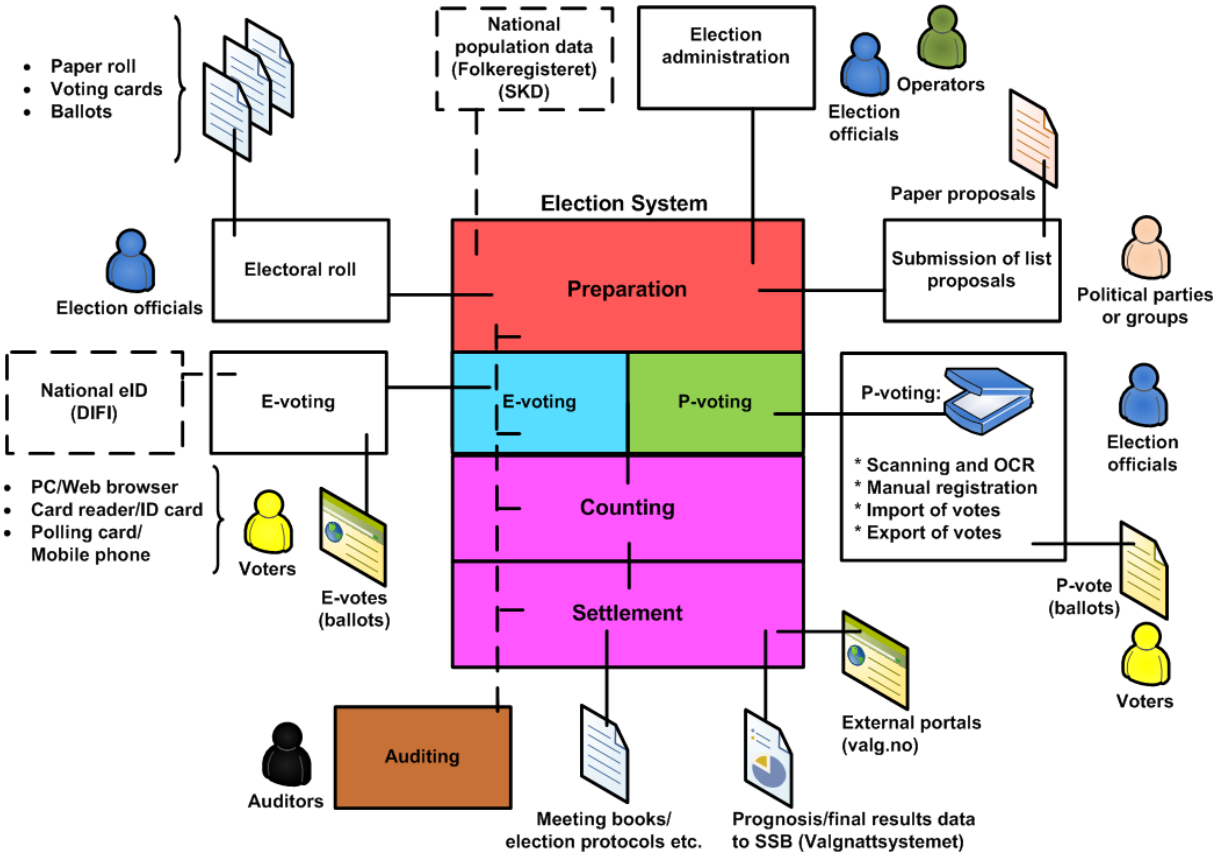

Figure 2 - Functional overview of the Election System

The Election system will be divided into modules covering the phases, processes and users described above. The figure below shows the high level modules in Election System. The arrows between the modules indicate in which direction the main flow of information between the various modules goes:

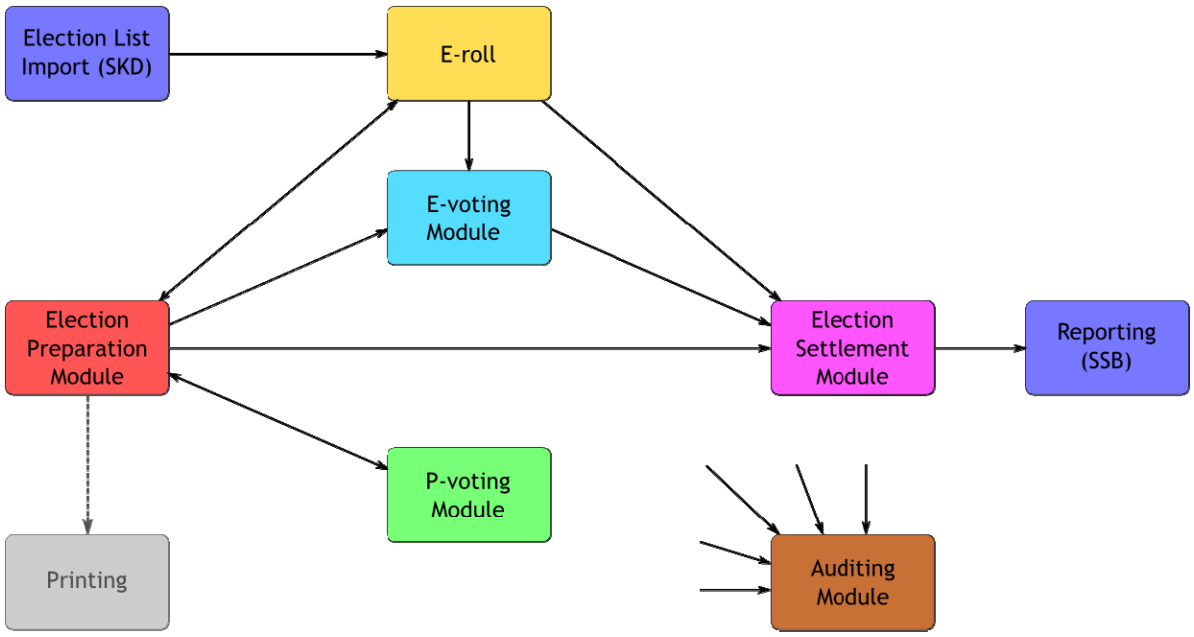

Figure 3 - Modules in the Election system

The E-roll is the module that will hold all information around the Electoral Roll. It will provide services to import data from SKD, have a self-service website where voters can verify that they are listed correctly, and the Polling Committee and Election Committees can use it to update the Electoral Roll when necessary. This module also serves as the electoral roll data source to the other modules in the Election System, including the Election Preparation Module, E-voting Module and Election Settlement Module.

The Election Preparation Module handles, among other things, list proposals and the definition of roles and users throughout the Election System. It will export data to a printer supplier to print out the ballots and the polling cards, and receive data from the P-voting Module that takes care of the e-counting of the paper votes. The E-voting Module is the module that handles the e-voting process.

At the end of the election process, the Election Settlement Module enters the game. It will receive data from the E-roll, the E-voting Module and the Election Preparation Module to perform the final counting, distribution of seats, and generation of protocols and reports. The module is also responsible for the export of all relevant information to SSB.

The last module is the Auditing Module, which will receive auditing information from all other components in the Election System. It will create a central audit trail in addition to all the local audit trails on the various components.

The table below gives an overview over which modules that cover which use cases on a high level. (Some of the functional requirements in a use case may be covered by another module.)

E-roll	UC 0.3 Electoral Roll UC 0.4 Exception Process for Electoral Roll UC 3.1 Registration of p-votes in Electoral Roll UC 3.5 Approval of P-votes and Ballots
Election Preparation Module	UC 0.1 Definition of Roles UC 0.2 Configuration of Election System UC 1.1 Submission of List Proposals UC 1.2 Checking and Processing List Proposals UC 3.2 Manual Registration of P-vote Results
E-voting Module	UC 2.1 E-voting
P-voting Module	UC 3.3 Electronic Counting of P-votes (OCR)
Election Settlement Module	UC 3.4 Counting E-votes UC 4.1 Reporting of Results to SSB UC 4.2 Settlement UC 5.1 Reporting
Auditing Module	UC 5.2 Auditing

Table 1 - Module/use case coverage

UC 9.1 Authentication is to a large extent cross-cutting concern, and therefore not represented as such in the figure and table above.

More details on how the proposed Election System supports the functionality of each use case are given in the elaborations of requirements in the chapters below.

1.2. Functionality included in the Proposed Solution – free of charge for the Principal

(Intentionally left empty.)

1.3. Other Relevant Functionality Provided

(Intentionally left empty.)

1.4. Other Relevant Services Provided

(Intentionally left empty.)

2. Elaboration of General Requirements

Elaboration of Requirement GR1.3

The Tenderer confirms that the source code will be well commented and documented, and easily maintainable. Automated code formatting and the implementation of a coding standard will ensure that the source code will be easy to read, and that comments are present at appropriate places. High test coverage will help keep maintainability high.

Elaboration of Requirement GR3.10

The Tenderer confirms that central configuration of the system will be provided and user training will be provided as specified in Appendix 5 and Appendix 7. System support for e-voting will be provided 8 – 16 for one week, system support for election administration will be provided 7 -16 from March 1st until election day and system support for e-voting will be provided 24/7 from July 1st to election day as specified in Appendix 7.

3. Elaboration of Use Case Requirements

3.1. Use Case 0.1 Definition of Roles

Elaboration of Requirement F 0.1.1

The Tenderer confirms that the system has the functionality for the management of users. The system contains an intuitive User Management Interface which facilitates the following:

- Creation of new users

Each new user created will have a unique identifier assigned automatically using a database ID field. Additional security information will be captured to simplify password management. This information can be used to verify the authenticity of a password reset request and therefore permit the reset to be handled automatically.

When the administrator selected the preferred authentication method by the user or for the role, checks will be performed to ensure that the user is a member of the selected authentication method service via the Common Authentication Interface (CAI). [1]The user will be created locally with an 'Awaiting Approval' state. An authenticated Election Administrator with the appropriate access rights must approve the new user account. At that point the user becomes active. The user will be informed e.g. via email when the account is created and subsequently approved.

Users can be created at various electoral levels e.g. Municipal, County; i.e. a user account can be created with administration rights only for a specified county, or for that county and the municipalities it covers, or only for a specified municipality. Users with account administration rights at the higher level, automatically have account administration rights at the lower level, i.e. an account administrator at county level (the account will be associated with a specific county) will automatically have the same rights in each Municipality within that county unless the inheritance is disabled.

- Maintenance of existing users

The system will permit the maintenance of existing users. Changes can be performed by an individual with the appropriate access rights. Automatic password resets can be configured; the request verification will be performed by validating responses to security questions, the answers to which having been captured when the account was first created. If verified, the request can be forwarded to the CAI. This process can also be performed by submitting password requests to an authorized approver if preferred. The approver has

[1] The Tenderer recommends that all changes that increase the privileges of a user should require approval by a second official. This ensures that a single administrator cannot create or update accounts to facilitate fraudulent behaviour without detection by other officials and is therefore stated in all appropriate responses. This will not be mandatory however and can be disabled if preferred.

responsibility for validating the request. Any other changes to a user's role, change in individual permissions or change in authentication method must be approved by a second Election Administrator with the appropriate access rights.

- De-activation of Users

User accounts can be de-activated. User accounts can be disabled preventing access to the system. The accounts however will not be deleted at this stage to ensure the integrity of any audit information relating to all user accounts. Any re-activation of a disabled account will require approval by a second election administrator with the appropriate access rights. A separate deletion option will be available listing only de-activated accounts. Account deletion will require approval by a second Election Administrator with the appropriate access rights. All other User Management options will only display active accounts.

- Assignment of Authentication method to a user

The authentication method for a user must be selected at account creation and can be altered through the account maintenance interface. In both cases, the account in question will be confirmed as a valid user for that authentication method and further approval by a second Election Administrator with the appropriate access rights will be required.

System Administrators will be able to provide users with a link to a web page where they can communicate their needs regarding functionality access. This web page offers an online form where a user can submit requests to create a new account or update an existing account. The online form will therefore be available to non-registered staff. The request must however include a valid email address for the domain or domains in which the election system is available and should include information relating to the level and type of functionality required and why so that appropriate roles can be assigned.

The User Management Interface is available to authenticated users with the appropriate access rights. The authentication method selected for a group of users with user management responsibility must be two-factor.

Elaboration of Requirement F 0.1.2

The Tenderer confirms that the system will have the ability to assign users to one or more roles.

When a new user account is created, access to functionality will be provided by assigning a role to a user account. Each role is a group of individual access rights to specific items of functionality and will be based on defined roles within the election process. When a role is assigned, the user account will be provided access to all functionality defined as part of that role. Any account must be assigned at least one role and can be assigned multiple roles. If multiple roles are assigned to a user account, the user account can access the functionality in each of the roles selected. Roles can also be un-assigned from accounts.

Elaboration of Requirement F 0.1.3

The Tenderer confirms that the system will provide functionality for the management of the roles. A role based authorisation component forms part of the solution. This functionality within this component includes:

- Creation of new roles

A new role will be defined within the system by assigning individual access rights to specific functionality and securable objects.

The role definition can either be performed by defining a new role and adding rights to the new role or using a copy of an existing role as the starting point and adding and/or removing rights. In both cases, the new role will be assigned a unique identifier within the system. Rights are added or removed from a role by selecting a checkbox beside a full set of access rights e.g. reports; or be expanding the set to list individual items and selecting one or more checkboxes within the set e.g. report-a, report-b etc.

When a new role is created, it does not become active and therefore cannot be assigned to any particular user account until the role has been approved by an Election Administrator with the appropriate access rights.

- Maintenance of existing roles

The system will permit the maintenance of existing role definitions .Access rights can be removed or added as necessary. Any addition of access rights will require separate approval. Changes to any particular role will be automatically applied to all user accounts assigned to the role when the user account next accesses the system.

- Deactivation of roles

Roles definitions can be deactivated. All access rights granted by the role to a user account will be revoked the next time a user logs in. A role deletion option will also be available and will only list deactivated roles. Role deletion will require approval by an Election Administrator with the appropriate access rights.

- Securable Objects

All securable objects defined within the system can be added to or removed from a particular role in the same way elements of functionality are added or removed. The specific actions that can be performed on each securable object can be specified in detail i.e. Full Control, Create, Read, Update and Delete. If securable objects form part of a hierarchy e.g. reports, database tables; access rights will be automatically passed to any and all child objects or the parent object exclusively.

- Authentication Method

The preferred authentication method can be selected at role level. This will require each individual account assigned to the role to use the specified authentication method to access the system. Authentication methods can also be specified at individual account level. The account level value will supercede any role level method specified.

- Owner

Each role will have assigned owners. A role can be assigned one or more owners. Ownership will provide a user with a level of administrative rights to that role. Any change of ownership will require approval by a second election administrator with the appropriate access rights.

Each role can have defined a list (zero or more) of other roles against which the assignment is mutually exclusive. Any proposed changes to a mutually exclusive list will require an investigation of current role assignments and would prevent the proposed change. The change cannot be fully implemented until the conflict, if any, has been fully resolved.

Elaboration of Requirement F 0.1.4

The Tenderer confirms that the system will have the functionality to map all securable objects to a role definition. The securable objects defined within the election system can be added to or removed from a particular role. Securable objects will be presented via the user interface in the same manner as items of system functionality. The user can select the securable objects that can be included or excluded from a role specification.

Elaboration of Requirement F 0.1.5

The Tenderer confirms that the system will have the functionality to map permissions to a role. The specific actions that can be performed on each securable object can be specified in more detail i.e. Full Control, Create, Read, Update and Delete. Where securable objects form part of a hierarchy e.g. reports, database tables; access rights can be automatically passed to child objects or restricted to a single level of the hierarchy.

Elaboration of Requirement F 0.1.6

The Tenderer confirms that the system will have the functionality for the management of permissions. The system will facilitate the management of all permissions relating to securable objects and logical units of functionality.

A user interface will allow the user to map permissions to roles/ securable objects etc. This interface will allow selection of a particular securable object from the current available list and then display all base permissions available and relevant to that object.

Base permission levels available (Create, Read, Modify, Delete, Approve, etc) will be relevant to the securable object or unit of functionality itself.

- Permission levels can be created for existing securable objects and units of functionality, derived from the existing base permission levels.
- Existing permissions and permission levels associated with securable objects can be reviewed and maintained.
- Existing permission levels associated with securable objects and units of functionality can be deactivated. Deactivated permissions levels can be deleted through a separate option. Only deactivated permissions will be presented and the deletion will require approval by an Election Administrator with the appropriate access rights.

Elaboration of Requirement F 0.1.7

The Tenderer confirms that the system will have the functionality to manage securable objects. All securable objects defined within the election system will be listed.

An option is provided to view details regarding a specific securable object. This will state

- any child or parent objects associated with the selection

- Permissions inherited from other objects
- Roles assigned from other objects.

The solution will allow objects to inherit permissions from other objects. Inheritance will be controlled by the parent object.

When selecting a parent object, any security configurations inherited by child objects (the default setting) can be broken. All child objects will not inherit the parent security configuration and will thus require independent configuration.

Elaboration of Requirement F 0.1.8

The Tenderer confirms that the system has the functionality to search/filter on user, role, securable object or permission. The role definition system provides a search and filter capability. This will return and display result sets to the user when interrogating the user, role and securable object configuration.

As many aspects of security model has a hierarchical structure (users, security objects etc), the configuration will be viewed in tree diagram form with the user permitted to expand and retract branches on demand.

Elaboration of Requirement F 0.1.9

The Tenderer confirms that the system will present the relations between the user, role, securable object and permission. As the security model has a hierarchical structure, the configuration can be viewed in tree diagram form with the user permitted to expand and retract branches on demand.

3.2. Use Case 0.2 Configuration of the Election System

Elaboration of Requirement F 0.2.1

The Tenderer confirms that the central/local system administrator will be able to retrieve an existing configuration or create a new one.

All information entered into the system including election configurations, will be registered to an election event e.g. 'Municipal 2011'. An authenticated user with the relevant privilege levels, such as the central/local system administrator, will list all current election events stored within the system. The user can then select the event for which the configuration needs to be viewed and/or updated, or create a new configuration by creating a new election event.

Elaboration of Requirement F 0.2.2

The Tenderer confirms that the central/local system administrator will be able to either create a brand new configuration or a new configuration based on an existing template.

An authenticated user with the relevant privilege levels, such as the central/local system administrator, will list all current election events stored within the system. The user can create a new configuration by creating a new election event.

New configurations can be based on any existing configurations for a current election event or a default template. When a new configuration is created, a date must be entered determining the date beyond which no

further changes may be permitted. Any subsequent access to the configuration management interface by a user with less than the highest level of administration rights will be unable to alter this value.

Elaboration of Requirement F 0.2.3

The Tenderer confirms that the Central/Local system administrator will be able to perform configuration in a design environment.

The Tenderer confirms that the configuration management process for the system is facilitated by a step-by-step process similar to an 'install and configure' processes. Users will commence the configuration process for a new election event by selecting a default template or a copy of an existing and active configuration. Users are then presented with a separate input page for each stage of the configuration process. The user can move backwards and forwards through the input pages or move directly to a specific configuration screen as required. At every stage of the process, a display will indicate to the user the current stage of the configuration process e.g. Step 4 of 10;

The steps in the configuration process and input pages will facilitate the following:

1. **Maintenance of core election system data**

   The data required will be determined by the current EML schema specification. Data can be entered and updated via an online form or imported by loading an XML/EML data file of the appropriate schema. Validation conducted on all fields, including mandatory fields will be driven from the schema specification.

2. **Create/Maintain Party and Group information**

   Party and group information will be created and maintained by entering data and/or updating forms. As the information will be extensive the data entry forms will be logically ordered to permit navigation through the levels of data. On the first page, a summary of the party or group information is presented and a detailed description of roles, codes etc are presented at appropriate lower level pages. A data import facility is also provided.

3. **Create/Maintain terms for an election**

   All text which is to be displayed as captions, menu text, help text, error messages etc will be loaded from a language resource file. A user with the appropriate permissions will be able to access a page to add, update and delete the contents of the language resource file. As the keys to the resource file must be known by the system before the text value can be loaded, new terms cannot be created without the system also being updated to load the new value. This mechanism is also used to support multi-lingual requirements (including Norwegian Bokmål, Nynorsk and English). An initial language selection will indicate the relevant resource file to load. These files exist in an exported XML format and can be used as the basis for further translations into additional languages which can then be made available to the solution automatically.

4. **Create/Maintain roles:**

   The system will facilitate the creation and maintenance of roles within the election system. This configuration interface will provide access to the role maintenance module.

5. Create/Maintain reports:

The system will facilitate the creation and maintenance of reports. This configuration interface will provide access to the report designer.

6. **Create/Maintain workflows:**

The system will provide workflow management for the main transition of data through the system and allow maintenance of key attributes of that workflow process. The workflow description will be presented in both flowchart and textual format ensuring the process is clear and accessible to all users. Workflow attributes such as 'Approval Requirements' (Y/N), 'Number of Approval Stages' (0..n) and 'Alerts Generated' (Y/N) will be easily configured through the workflow maintenance interface.

The various workflow attributes defined in the system will be displayed. Individual entries can be selected to configure user alerts to occur when a defined event has taken place, e.g. when a ballot paper proof is ready for review. The system can be configured to define different users of equal or higher privilege who must approve the event changes, if an alert is generated and the individual(s) or role(s) who will receive the alert.

7. Create/Maintain rules:

The system will provide the ability to alter key parameters of the business rules. Key parameters that can be amended include the divisor values of the count method and aspects of the e-counting of p-votes, e.g. ballot marks can be configured for automatic acceptance or rejection (e.g. √ vs X) during the scanning phase.

The default values for these automatic acceptance or rejection parameters are set to off, and the election officials must select to include the automatic business rules. It should be noted that changes to the count method, if approved, will require transfer to the air-gapped count system before they are active.

8. Create/Maintain layouts

The system provides a proofing capability for printed election material e.g. ballot papers, poll cards allowing administrators to verify layouts based on printer specifications. The layouts for documents must be verified by the selected print supplier. The system provides the ability to upload print product templates and merge live data onto the templates thereby allowing printer quality proofs to be viewed, verified and signed-off. This process is highlighted in the system screenshots below.

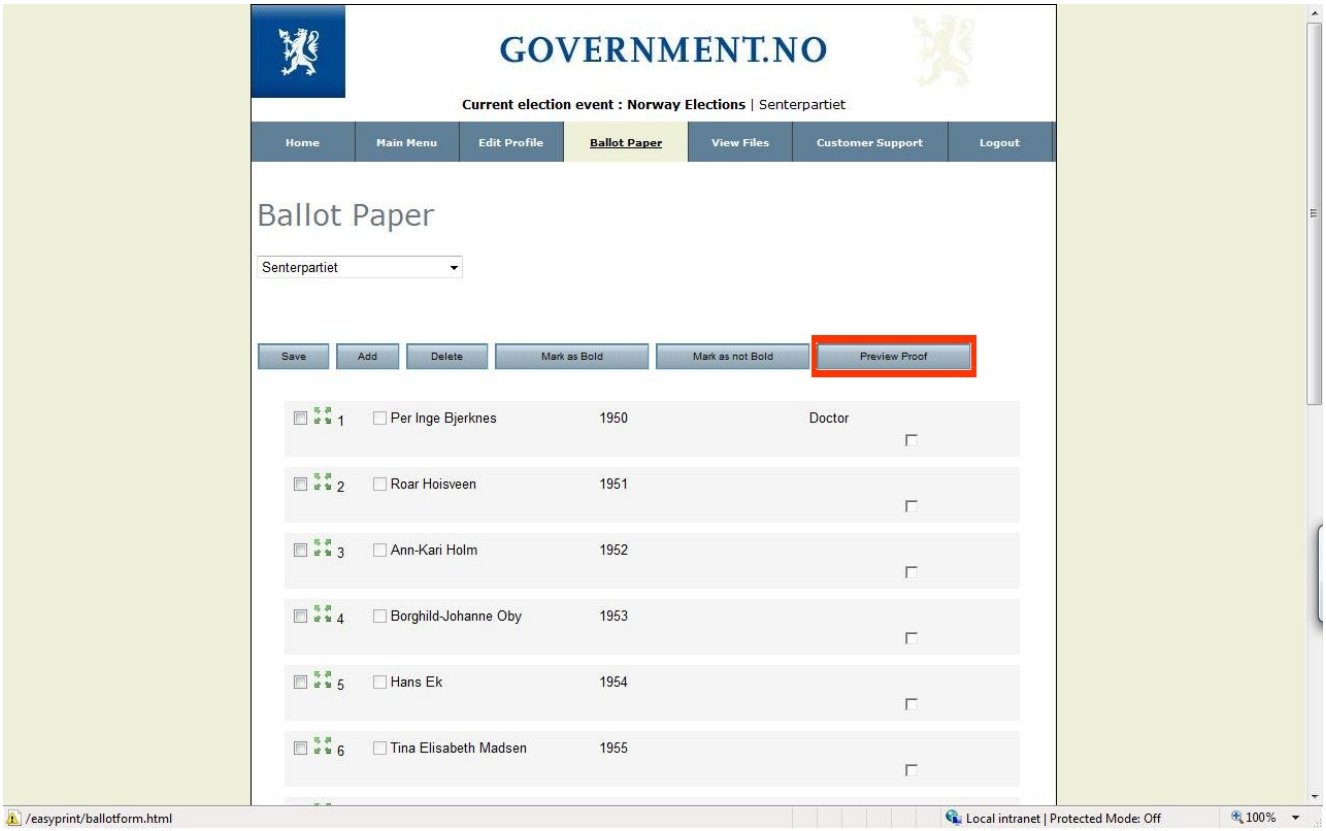

Figure 4 Example of ballot preparation process

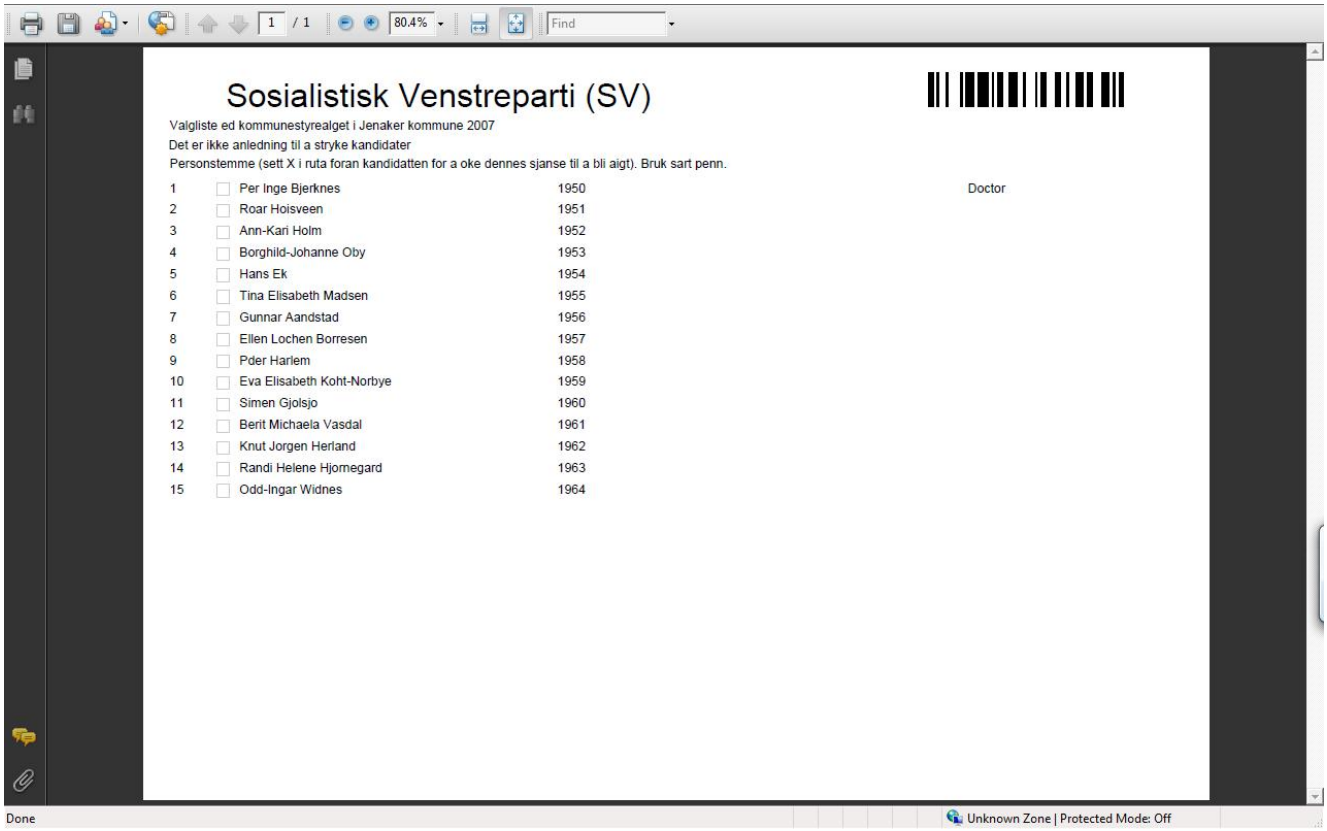

Figure 5 Example of printer proofs generated from the system

This streamlines the end-to-end print process, reducing the time taken to prepare and proof ballots and provides the election administrator the earliest possible delivery of the final printed materials.

9. Configure external interfaces and web services

Any external interfaces available to the system or calls to internal web services can be enabled or disabled as required. If disabled, any other modules which attempt to avail of the external or internal service will return an error indicating calls to the service are not currently permitted. Additionally, any key attributes such as response timeout plus schedule information where appropriate can also be altered. Changing the timeout setting is achieved by simply changing the current timeout value (set in seconds) via an online form. The error message text displayed when the interface is disabled can also be updated.

10. Import/Export of an entire configuration

The entire configuration can be exported to, or imported from an XML/EML format file.

All changes have a final confirmation stage where a summary of the changes are presented to the user. The summary page also provides quick navigation back to the relevant screen selected, to verify further information if desired. Any attempt to leave the configuration phases without confirming will generate a warning message and a subsequent audit record. New and updated changes to the configuration always require further approval by another authorised user.

Elaboration of Requirement F 0.2.4

The Tenderer confirms that the Central/Local system administrator must be able to see a preview of the configuration and test the configuration.

A summary of the current configuration or configuration awaiting approval can be selected and displayed. Further options are available to view more detail for each sub-system's configuration.

The entire election system can be placed into 'test' mode before any new or updated configuration is approved. Users currently accessing the 'live' system will be alerted to the fact that a change from 'live' to 'test' mode has been requested. The change from 'live' to 'test' mode cannot proceed if users remain logged into the system in 'live' mode. When all active sessions have ceased, an administrator changes the system to 'test' mode triggering a full database archive.

All system interfaces will have the live CSS files temporarily replaced with test CSS files altering the primary colour scheme of the system. This will provide a clear visual indication to the user that the system is now in 'test' mode. All page titles will also be changed from 'LIVE – <Page Title>' to <TEST - <Page Title>. When the move to 'test' mode is complete, administrators can change the updated configuration to 'Active' and access all aspects of the election management system and verify the new configuration. When all checks have been completed, the administrator can change the system status back to 'live'. This will restore the 'live' CSS files, and the database archive taken immediately prior to the change to 'test' mode. The new election configuration can then be approved and officially made active in 'live' system mode.

Elaboration of Requirement F 0.2.6

The Tenderer confirms that an authorized individual must be able to approve the configuration

The creation of a new election configuration or changes to an existing configuration will be reviewed and must be approved by a second user with the appropriate privilege. The approval will be audited.

Elaboration of Requirement F 0.2.8

The Tenderer confirms that the central/local system administrator must be able to edit an existing configuration up until a preconfigured date.

When a new configuration is created, a date must be entered determining the date after which no further changes are permitted. Any subsequent access to the configuration management interface by a user with less than the highest level of administration rights will be unable to alter the value.

Elaboration of Requirement F 0.2.9

The Tenderer confirms the central/local system administrator must be able to create a new configuration based on an existing configuration (With or without template data).

An authenticated user with the relevant privilege levels, such as the central/local system administrator, will list all current election events stored within the system. The user can create a new configuration by creating a new election event. New configurations can be based on any existing configurations for a current election event or a default template.

3.3. Use Case 0.3 Electoral Roll

Elaboration of Requirement F 0.3.2

The Tenderer confirms that the Election System will be able to load the initial Electoral Roll dataset. The system will expect to find the electoral roll data in a file on a disk share that is available to the E-roll Server. An administrative user will be able to specify to the system where the file can be found, and start the initial import manually.

The file will be formatted as a flat text file that can easily be parsed. The file will be loaded into the system and parsed, and all data will be persisted in a local database to build up an electoral roll.

The transmission of the electoral roll data from SKD happens outside the system, and is therefore out of scope.

Elaboration of Requirement F 0.3.4

The Tenderer confirms that it will be possible to import updates to the E-roll. It will be possible to configure in the system how often and when it should check for new files with updates to the electoral roll from SKD. The files will, just like the initial electoral roll data file, be stored on a disk share that is available to the E-roll Server. Their name will use a fixed, unique numbering scheme, such that it is possible for the E-roll Server to ensure completeness and correctness of the electoral roll database.

The update files will be automatically loaded into the system and parsed, and all data will be persisted in a local database in the same way as for the initial data file. Any errors that occur during this process will be logged, and a copy will be sent to a dedicated administrator as a task in the system.

Prior to the import of a file, a first round on the file is done to filter out errors that have been corrected in later transactions in the same update file.

The transmission of the updates to the electoral roll from SKD happens outside the system, and is therefore out of scope.

A website, called the E-roll Self-Service, will be built where each voter can check whether all information about him is registered correctly. Voters will be able to log into the website using eID. The voter will be able to request corrections through a special form, according to Use Case 0.4 Exception process for listing in Electoral Roll.

Elaboration of Requirement P 0.3.1

The Tenderer confirms that the system will be able to handle as many as 1 million transactions per hour at peak. Performance testing will ensure that the component that parses the initial file and the updates to the electoral roll data will be able to handle this load.

3.4. Use Case 0.4 Exception Process for Electoral Roll

Elaboration of Requirement F 0.4.1

The Tenderer confirms that the system will have an interface allowing the voter, party/group to fill in a predefined application form. In this form, the voter will be able to specify amongst other things the following information:

- Street address
- Municipality
- Mobile phone number

Elaboration of Requirement F 0.4.4

The Tenderer confirms that the Electoral Committee will be able to approve or reject the application from within the system. The Electoral Committee will have a mailbox where it will receive the requests to correct information in the electoral roll as specified in Requirement F 0.4.1. For every request, the Electoral Committee will be able to inspect the information provided by the voter together with the information currently stored in the Electoral Roll for that voter (if any is available). When the Electoral Committee has inspected the information, it will be able to choose whether to approve the request, reject it, or delay a decision.

Elaboration of Requirement F 0.4.5

The Tenderer confirms that the Electoral Committee will be able to update the Electoral Roll. The update will be done in accordance to the information provided by the voter in the request.

3.5. Use Case 1.1 Submission of List Proposals

Elaboration of Requirement F 1.1.1

The Tenderer confirms that Party/group representative will be able to select the election/referendum he/she wants to manage candidates/signatures for.

All parties/group representatives will be able to select the election/referendum for which they wish to manage candidates and/or signatures. All updates to the system will follow the initial selection of an election event. The party/group user will be prompted to select an active election event and then the election/referendum to which all actions are linked. The user will then be able to manage the candidates and signatures for the specified election/referendum.

All updates to the system must follow an initial selection of an election event. Consequently when accessing the system, a party/group user will be first prompted to select an active election event to which all subsequent actions will be linked including the management of candidates and signatures.

Elaboration of Requirement F 1.1.2

The Tenderer confirms that a representative for a party/group will be able to enter or import (csv, xls, etc.), edit and delete list proposal candidates and signatures.

The list proposal candidates and signatures will be capable of being entered into the system in a variety of ways by a party/group representative.

- **File import**

  Core candidate information can be imported (csv, xls, xml) or can be entered using a web page form. The system will facilitate edits and deletions to the list proposals and signatures.

- **A scanned image can be uploaded to capture the signatures**

  Using a pre-defined form, the party/group representative will upload images scanned locally in black and white and at a quality of 300dpi. The solution will utilize ICR to interpret the entries on the form and allow corrections if necessary. The ICR process will capture signatures from the form. The list proposal generated from this process will include a link to the submitted image from which the list data was extracted.

- **Digital Pen**

  If required, the list and data can also be captured using a digital pen solution which is unique to the Tenderer. This additional option provides the ability to capture the list proposal details and collect all signatures electronically.

  List forms are designed and printed on 'encoded' paper. The forms are completed and the digital pen captures the information written onto the form electronically. A camera within the digital pen captures the pen strokes, maps them to the unique form design and records the information electronically. As the system simply records pen strokes, no clear text data is recorded, and the information is effectively encrypted as the pen stroke information is meaningless until it is interpreted by the central pen server component.

  When using the digital pen a paper form is still produced and can be kept as an additional audit trail mimicking the traditional paper based process.

  The recorded pen strokes are also uploaded to the system by docking the pen into a docking station with appropriate connectivity. The central processing software translates the penstrokes into an electronic copy of the form and permits correction of the information recorded. An illustration of the facility is shown below. Each individual field on the form will have bespoke validation thereby enhancing the accuracy of the data interpretation.

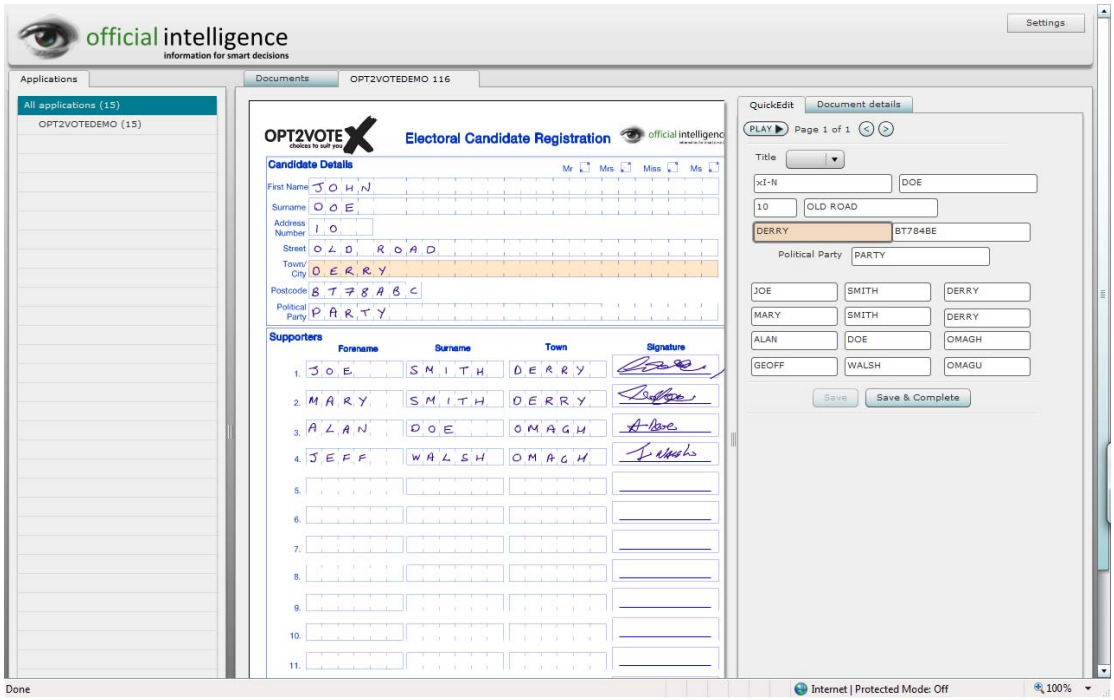

Figure 6 Example of List Proposal Display

The information recorded from the pen also includes the order in which the fields were filled out. This can be replayed on the system, providing the added value of detect fraudulent behaviour. (Fraudulent behavior can be identified by the order in which the data was written to the original form. e.g. Forms completed by filling out all names sequentially, followed by addresses sequentially, and signatures sequentially.)

The system is capable of accepting manual corrections to the form data. When any necessary corrections have been made, the data can be confirmed by the party and submitted as a list proposal. Additionally, an electronic copy of the form in .PDF format can be linked to the list proposal data for the purposes of signature verification.

Additional functionality available through the digital pen solution includes a realtime submission of the form data through a Bluetooth connection to a mobile phone which if required can replace the physical docking station. Additionally functionality may be utilized using a Bluetooth connection to a GPRS enabled mobile phone to capture the location at which a particular form was completed.

When all list proposal data is captured, the system provides an interface to permit alteration of the final ballot layout. This includes changes to the ordering sequence of candidates and the ability to highlight particular candidates in the list.

At any stage, the party or group representative can preview the ballot in printer ready format providing an accurate representation of how the ballot paper will look in a printed form.

Amendments and withdrawals can continue to be made until a pre-defined date. This date is configured at the event creation stage. Any change in data status including final confirmation or withdrawal will generate an email and/or SMS alert to the election team and the parties.

Elaboration of Requirement F 1.1.4

The Tenderer confirms that the system will check candidates and identification from signatures (signer ID) against the Electoral Roll and the system will also check the number of names of candidates and signatures on a list proposal according to §6-2 and §6-3. Candidates can be approved in turn and each entry updated to show the current status of the entire list.

Figure 7 - Dialog Showing Whether Candidates are Accepted or Not

The election configuration process includes the management of attributes defining the necessary number of candidates and signatures according to the election rules. The system will use data from historical returns for the particular party or group in previous elections to check the number of names of candidates and signatures on a list proposal.

Elaboration of Requirement F 1.1.5

The Tenderer confirms that the system will be able to detect duplicates candidates and signatures across list proposals.

The system will cross-check all list proposals within the selected election event and identify any possible duplicates by name or by signature. Duplicates will be displayed to the user to permit one or both to be rejected

or accepted. In both cases, reasons for the decision will be recorded and will be included in the associated audit record(s).

Elaboration of Requirement F 1.1.7

The Tenderer confirms that the system will have functionality for approving a list proposal by an authorized party/group representative.

When all data in a list proposal has be verified by an election official, the status of the list proposal will move to 'Awaiting Approval'. This status change will generate alerts via email or SMS to the relevant individuals, and specifically the representative for the party or group. Representatives from the party or group can then access the system, select the List Proposal and approve the data. This will change the status to 'Approved' and generate a further alert to the election official with responsibility for this contest.

Elaboration of Requirement F 1.1.10

The Tenderer confirms that from the received notification the Electoral Committee will be able to publish the list proposals

When the election representative has been alerted to the 'Approved' status of a particular list proposal, and assuming the election official has appropriate access rights, the official can set the status of the list proposal to the 'Published' status. This published status will place a copy of the list proposal onto a publically available website for review.

This publication process is also linked to the defined print provider with responsibility for printing the ballot papers to indicate that the print process for the approved ballot papers may commence. The details of the printer(s) who will receive alerts are defined during the election configuration stage.

3.6. Use Case 1.2 Processing List Proposals

Elaboration of Requirement F 1.2.1

The Tenderer confirms that the system will present all list proposals submitted by the parties/groups

The user will be prompted to select an active election event; all subsequent actions are linked to this selected event. The list proposals will be displayed to any party or group participating in the selected election event.

The display of list proposals will include the current status of each submission e.g. Submitted, Awaiting Approval, Approved, Published, Rejected.

Elaboration of Requirement F 1.2.2

The Tenderer confirms that the Electoral Committee will be able to approve/reject a list proposal.

The user will select a proposal from the list submitted for an event. The user can approve the list on behalf of the Electoral Committee moving the file to a 'Published' status or rejecting the submission by changing the status to 'Rejected'. The reason for rejection plus any additional comments must be noted as part of the

rejection process. The party or group that has submitted the list proposal will additionally receive an alert, by SMS and/or email to ensure they are notified of the status change.

Elaboration of Requirement F 1.2.5

The Tenderer confirms that the Electoral Committee will be able to publish a list of approved parties on a web page that is available to the general public.

A copy of the list proposals with 'Published' status will have a copy automatically transferred to a publically available web site. The website URL will be defined and stored in the system during the election configuration phase.

Elaboration of Requirement F 1.2.6

The Tenderer confirms that the Electoral Committee will be able to edit (Create, update or remove) candidates and signatures on a list proposal if necessary.

An authenticated user with appropriate privilege will be able to edit the list proposal using the web interface. All changes will be fully audited. Changes will include adding, updating or removing entries on the list. All communication between the Electoral Committee and the Party or Group in relation to the changes will take place using the web interface. The Electoral Committee and party/group will submit requests using an online form, known as 'customer requests'. The customer requests facility ensures all dialogue/negotiations are fully recorded within the system.

3.7. Use Case 2.1 E-voting

Elaboration of Requirement F 2.1.1

The Tenderer confirms that the system will provide valid elections/referendums to the voter based on their rights in the Electoral Roll. When the voter has logged on to the E-Voting Client Application, a list with all valid elections and referendums for the voter will be presented. The list will be sorted according to the DisplayOrder, as defined in the EML standard.

Elaboration of Requirement F 2.1.2

The Tenderer confirms that this requirement will be met by the system. The voter will be able to select an election or referendum from the list described in Requirement F 2.1.1, register his vote for that election or referendum, and then continue to select other elections or referendums as he wants. It will be possible to select an election or referendum he already has voted for in the current session, and change his vote if he wants to. He will not be required to re-authenticate within one such session. It will not be a requirement that he has registered a vote for each valid election and referendum before he can submit his ballots to the server.

Please also refer to our E-voting Client Application prototype for a visual presentation of how we intend to solve this requirement.

Elaboration of Requirement F 2.1.3

The Tenderer confirms that this requirement will be met by the system. When a voter has selected an election or referendum, a set of steps and options to complete the ballot for that election or referendum will be presented according to the ELMER 2 standard. These steps and options depend on the configuration of the election or referendum in the Election Preparation System.

If the voter has selected an election, he will be presented a list with valid parties in random order. Depending on the configuration of the election in the Election Preparation System, the voter will have the possibility to make various adjustments to the ballot. Searching for candidates from other party to write them in on a ballot will be one of those possibilities. The E-Voting Client Application will be designed to avoid erroneous adjustments to the ballot.

If the voter has selected a referendum, he will be presented with the valid options for the referendum. If the DisplayOrder attribute, as defined in the EML standard, is provided with the options, the options will be ordered accordingly. Otherwise the options will appear in random order.

Please also refer to our E-voting Client Application prototype for a visual presentation of how we intend to solve this requirement.

Elaboration of Requirement F 2.1.4

The Tenderer confirms that the voter will be able to cast his vote. When the voter has finished registering his votes for the valid elections and referendums according to Requirement F 2.1.2 and Requirement F 2.1.3, the voter can, if he is happy with all his choices, submit his ballots. The ballots will then be encrypted and the voter will be asked to sign them by filling in his digitally signing credentials. When the ballots have been signed, they will be transferred to the E-Voting Collection Server.

Elaboration of Requirement F 2.1.5

The Tenderer confirms that the vote will be stored and a preliminary mark off will be made in the Electoral Roll. When the E-Voting Collection Server has received the voter's vote, and all checks and controls, including the verification of the digital signature, were positive, the system will register in the Electoral Roll that the voter has cast a vote. These registration will a.o. include the following attributes:

- A time stamp
- Voting media (electronic or paper)
- Environment from which the vote has been cast (controlled or uncontrolled)

Notice that voters who cast more than one vote will have more than one such registration. The e/p-merging process will make sure that only one vote is selected as the valid one, and votes cast in a controlled environment will have precedence over votes cast an uncontrolled environment.

The votes will be stored securely in the system in accordance to the security objectives.

Elaboration of Requirement F 2.1.6

The Tenderer confirms that the voter will be notified that their vote has been cast. When the voter has cast his vote, he will receive two confirmation messages. The first confirmation message will be sent from the E-Voting Collection Server to the E-Voting Client Application, as a simple reply to the REST call. This confirmation message will only contain some basic information that can be displayed in the E-Voting Client Application.

In addition to the first simple confirmation message, another confirmation will be sent to the voter using SMS. This confirmation message will a.o. contain a time stamp and a verification code, so that the voter can use his polling card to verify that his vote was registered by the server in accordance to his intentions. Please refer to the paper On Achieving E-Vote Integrity in The Presence of Malicious Trojans attached to this appendix for more details on how this verification code is generated.

Elaboration of Requirement F 2.1.7

The Tenderer confirms that this requirement will be met by the system. If the voter does not exist in the Electoral Roll, a new entry for that voter will be created in the Electoral Roll. The entry will contain some basic information about the identity of the voter, and marked as a voter who has tried to log on. The voter will not be allowed to submit a vote.

Elaboration of Requirement F 2.1.8

The Tenderer confirms that this requirement will be met by the system. When a voter who doesn't exist in the Electoral Roll tries to log on, the E-Voting Client Application will display a message explaining that he isn't registered. The message will contain information about his options in order to apply for membership in the Electoral Roll, including a link to the E-roll Self-Service website mentioned in our elaborations of Requirement F 0.4.1.

Elaboration of Requirement P 2.1.1

The Tenderer confirms that the system will be easily scalable. The system architecture permits to increase the computing power of the E-Voting Collection Server (EVCS) by adding more collection server instances. Extensive performance testing will show how many parallel servers will be required to secure good performance in peak hours. In addition, monitoring can be used to make proactive changes.

Elaboration of Requirement NF 2.1.1

The Tenderer confirms that the voter won't receive a message about previous votes at any step in the process. The E-Voting Collection Server won't release any information to the E-Voting Client Application about previous sessions. It will therefore not be possible to get any knowledge about whether a voter has voted previously or not, when he would have done that, the content of previous votes or from which environment they were accepted through the E-Voting Collection Server.

3.8. Use Case 3.1 Registration of p-votes in Electoral Roll

Elaboration of Requirement F 3.1.1

The Tenderer confirms that the Polling Committee/Electoral Committee will be able to check the voter against the Electoral Roll.

There will be two client applications available: the E-roll Administration Client Application and the E-roll Polling Station Client Application, and it will be possible to check the voter against the Electoral Roll in both applications. The Polling Committees/Electoral Committees can use them to look up voters and determine if they are listed in the Electoral Roll, which municipality they belong to and whether voters already have cast advance votes.

The search screen facilitates the scanning of the voting card barcode for automatic lookup of the voter as well as manually entering search criteria for finding the voter. Scanning can only be used if the voter has brought his voting card. Manual search criteria can be a combination of name, birth date, address, municipality etc. Scanning of the voting card bar code will result in one hit while entering manual search criteria may result in a list to select from if the criteria entered were not precise enough.

Figure 8 – E-roll Polling Station Client Application Search/Scan screen

Please refer to our E-roll Polling Station Client Application mock-up for more visualization of how we intend to solve this requirement, added as attachment 4 to this appendix.

Elaboration of Requirement F 3.1.2

The Tenderer confirms that the Polling Committee/Electoral Committee will be able to mark off voters in the Electoral Roll for voters belonging to the municipality and who haven't voted on paper yet.

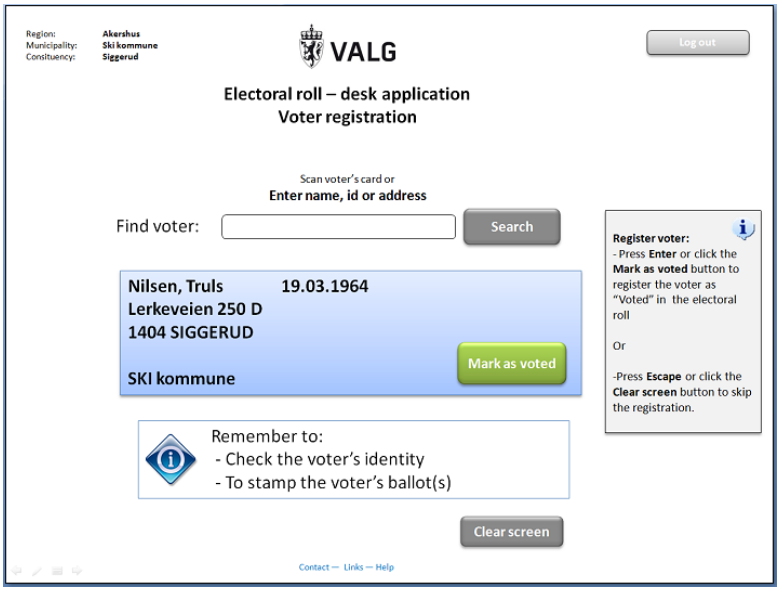

Figure 9 E-roll Polling Station Client Application Mark off voter screen

Please refer to our E-roll Polling Station Client Application mock-up for more visualization of how we intend to solve this requirement, added as attachment 4 to this appendix.

Elaboration of Requirement F 3.1.4

The Tenderer confirms that this requirement will be met by the system. The E-roll application will have support for registering reasons for voters that cannot be marked off temporarily or finally in the Electoral Roll. If a voter does not exist in the Electoral Roll of the current municipality or already has cast an advance or a final vote at another Polling Station, data can be registered in a dedicated section of the voter details page of the looked up voter. If a voter does not exist in the Electoral Roll at all, the E-roll application will allow for the registration of voter credentials and the reason so that the Electoral Committee later can determine whether this is a valid vote or not. Exceptions will be posted (notified) to the relevant Electoral Committee as a task to act upon later in the process (UC 3.5 Approval of p-votes and ballots).

Please also refer to our E-roll Polling Station Client Application mock-up for a visual presentation of how we intend to solve parts of this requirement, added as attachment 4 to this appendix.

Elaboration of Requirement F 3.1.7

The Tenderer confirms that the system will be able to store preliminary mark offs. At the advance polling stations, the PC will preliminary mark off the voter as advanced voted he if he exists in the E-roll. The preliminary mark off generates a serial number which the PC writes on the backside of the outer envelope together with the voter's credentials. The double envelope is then shipped off to the voter's home municipality. When the EC in the voter's home municipality later on in the process picks up the advance votes (UC 3.5 Approval of p-votes and ballots), the serial number is then as used as a quick reference lookup for acceptance or rejection of the advance vote. If the advance vote is accepted, the EC then separates the outer envelope with the voter credentials and the inner envelope with the voter's ballots. The EC places the voter's ballots in the advance ballot box.

3.9. Use Case 3.2 Manual registration of p-vote results

Elaboration of Requirement F 3.2.1

The Tender confirms that Polling Committee Electoral Committee and County Electoral Committee will be able to enter results at various stages e.g. Advance results, Preliminary results etc

The system will provide the functionality for the Polling Committee, Electoral Committee and County Electoral Committee to input P-Vote results at relevant stages using the Manual Registration of p-vote results (m-register) component.

The m-register component will be available to authenticated users with the appropriate system permissions. Additional workflow criteria can be specified to restrict access to the functionality, such as:

- Date and/or time lock threshold;
- Users registered as belonging to counties and/or municipals with currently active contests or election events

All data entered into the solution requires the selection of an appropriate election event. Any contests within this event and within the locale of the authenticated user are then presented i.e. only county and/or municipal contests within which the user is registered. The required contest is selected and the appropriate data is entered into the system.

The data input page allows the user to identify the type of result entry by using radio buttons and/ or drop-down lists e.g. Advance or Election-day results and Preliminary or Final results. The data-entry form also provides the functionality to browse for a file, and enable the data to be uploaded as a data file in various formats (.CSV, .XLS, .XML). (Note: The exact file format for data imports must be defined within the system in advance).

When the data file has been uploaded, the data will be presented to the user for confirmation. The upload process will include verification that the data being uploaded is for the contest previously selected.

No entered or uploaded data will become active until it has been approved by another system user with appropriate access credentials. If the data was manually keyed originally, the approval process will request that the data be re-keyed as an additionally protection against human error.

If data has already been received for a particular contest within a particular event, the existing data will be presented automatically on the data entry screen. The user will have the ability to amend totals but will be warned on submission that the current data will be 'overwritten' if the most recent set of amendments are made. If the amendments are accepted, the data will not be 'overwritten' until the amendments have been approved by another system user with appropriate access credentials and system permissions. Audit entries are generated for every stage of this process providing the relevant responsible parties with full visibility and transparency of the process.

Any data entered by an individual but not confirmed will be discarded. A warning will be presented stating that any unsaved data will be lost. If the cancellation is confirmed, the data will be discarded and an appropriate audit entry generated.

Elaboration of Requirement F 3.2.2

The Tenderer confirms that the Electoral Committee, Polling Committee and County Electoral Committee will be able to register data for the election protocol.

All data relevant to the election protocol may be entered using the m-register component. Additional data may include information relating to questionable ballots, number of votes received in a cover envelope etc.

Elaboration of Requirement F 3.2.4

The Tenderer confirms that the system will present preliminary and final results for the various levels depending on election and show differences between those results.

The information entered during the Manual Registration stage will be displayed at the various levels depending on election. The data presentation will also calculate and highlight any differences between the preliminary and final totals.

Elaboration of Requirement F 3.2.5

The Tenderer confirms that authorised election members will be able to approve the results.

Authenticated users with the appropriately assigned access rights will be able to approve data relating to the manual entry of p-votes. This will exclude the authenticated user who initially entered the data. The election system maintains a list of outstanding actions for all roles. When a user initially logs in and selects the relevant election event, the 'Home' screen will highlight any outstanding actions for that user or role to which the user belongs. This ensures that any key actions are performed in a timely manner and assists in ensuring no key steps are omitted. Additionally, no election event can be considered complete and results published if any outstanding actions still remain. As a safeguard, the system will prevent final steps until all key actions are complete.

The approval process will include a display of the data entered and flag whether this is re-count data or whether the approval process will supercede any previous data entry. If this is confirmed, the system will audit the approval action and the updated data will be published as the current live state. This approval action will generate alerts to the appropriate users (e.g. Electoral Committee) in the contest via email and/or SMS channels.

Elaboration of Requirement F 3.2.8

The Tenderer confirms that the relevant Committee must be able to overwrite the results if there is a difference between the preliminary and final results.

If data has previously been received for a particular contest in a particular event, (either preliminary or final) the existing data will be displayed automatically on the m-register component display. The user will have the ability to amend totals but will be warned on submission that the displayed data will supersede the current totals. If accepted, the displayed data value will not become the active until these amendments have been approved by another system user with appropriate access credentials and system. Audit entries are generated for each instance of this process providing full visibility and transparency of the process.

3.10. Use Case 3.3 Electronic counting of p-votes

Elaboration of Requirement F 3.3.1

The Tenderer confirms that the relevant committee can select the appropriate election and contest as required and enter file meta-data describing ballot characteristics that cannot be read from the image.

The user will select the election and contest and the preliminary election data is entered into the e-count component. The P-votes (ballot papers) are grouped into batches ready for scanning. The batches of p-votes are then scanned into the e-count system.

The system can provide pre-printed ballot batch identification forms which are scanned as the first item in any batch and the batch identification forms link the batch information to all ballots in the associated physical batch.

Alternatively if the ballots have been pre-scanned (according to industry standards for ICR), the e-count system offers the facility to input batch related meta-data into the system replacing the pre-printed ballot batch identification form. ICR processing is then initiated by browsing to the directory of pre-scanned images instead of feeding documents into a scanner.

Elaboration of Requirement F 3.3.2

The Tenderer confirms that the system shall enable the relevant committee to scan ballots through any TWAIN compliant commercial off-the-shelf scanner solution utilising the p-vote module. Images scanned utilising the p-vote module scanning interface should be captured at a quality of 300dpi and black-and-white colour setting.

Elaboration of Requirement F 3.3.3

The Tenderer confirms that system uses Intelligent Character Recognition (ICR) technology to process the ballot paper images. The values processed on the ballot paper will include:

- The Party selected. The Party identifier will form part of the unique ballot identifier and should be in Code 3of9 barcode format.
- Any additional personal votes marked on the ballot paper will be captured, interpreted and recorded
- Any votes for candidates from other parties will also be captured, interpreted and recorded.
- Any marks outside of these permitted values will also be captured

When the p-vote module processes a ballot paper with a mark that cannot be confidently determined electronically, the system provides a user interface for manual verification and update (if required).

The Tenderer will work with the Ministry of Local Government and Regional Development to ensure the ballot paper designs (field segmentation) and print quality assist in the realisation of the 99% accuracy requirement. The system will be able to cross validate the system-read party abbreviation against a defined list, and cross validate the candidate number and candidate name against each other. Therefore the ballot paper design, ICR accuracy and solution logic combined will ensure the necessary accuracy is obtained.

The unique barcode on the ballot paper will facilitate duplicate detection. The system will report and allow the user to mark as rejected all duplicates identified during the image processing phase.

The specific ballot design to assist the visually impaired should not hinder the solution providing the same voter intent marking is produced. Should this differ, the p-vote solution can be amended to support the necessary ballot design.

Elaboration of Requirement F 3.3.5

The Tenderer confirms that the system will be able to present preliminary and final results and the difference between preliminary and final results.

When the capture and processing of the ballot papers has been completed, preliminary results can be made available immediately.

A second tally process will calculate the final results. The data presentation of these results calculates and highlights differences between the preliminary and final totals.

Elaboration of Requirement F 3.3.6

The Tenderer confirms that the relevant committee will be capable of approving the results.

As results are obtained, they will need to undergo a formal approval process. A system user with the correct privileges will upload the results, which are then reviewed by a primary authorised user and a secondary authorised user of equal or higher privilege. The primary and secondary users will collaboratively review and approve the results.

Elaboration of Requirement F 3.3.9

The Tenderer confirms that the relevant Committee will be able to overwrite the results if there is a difference between the preliminary and final results. If the final and preliminary results differ, the system will permit the formal results be updated as necessary to record the new values. Any updates/overwrites will require approval by an authorised user of higher privilege.

Elaboration of Requirement F 3.3.12

The Tenderer confirms that the Electoral Committee will be able to check rejected ballots.

The p-vote system will provide a facility for authorised users of the appropriate privilege to view accepted and rejected ballots. Viewing the accepted ballots verifies that the system is functioning correctly. Viewing rejected ballots allows for a level of manual verification of the rejection process. This review process also allows the interpreted results from the ballot paper to be adjusted as necessary and the captured ballot data to be updated for the process of final tally. All actions and user decisions in relation to the verification process are audited to provide full visibility and transparency of the process.

The user interface will display the image of the rejected ballot and the reasons for rejection highlighted.

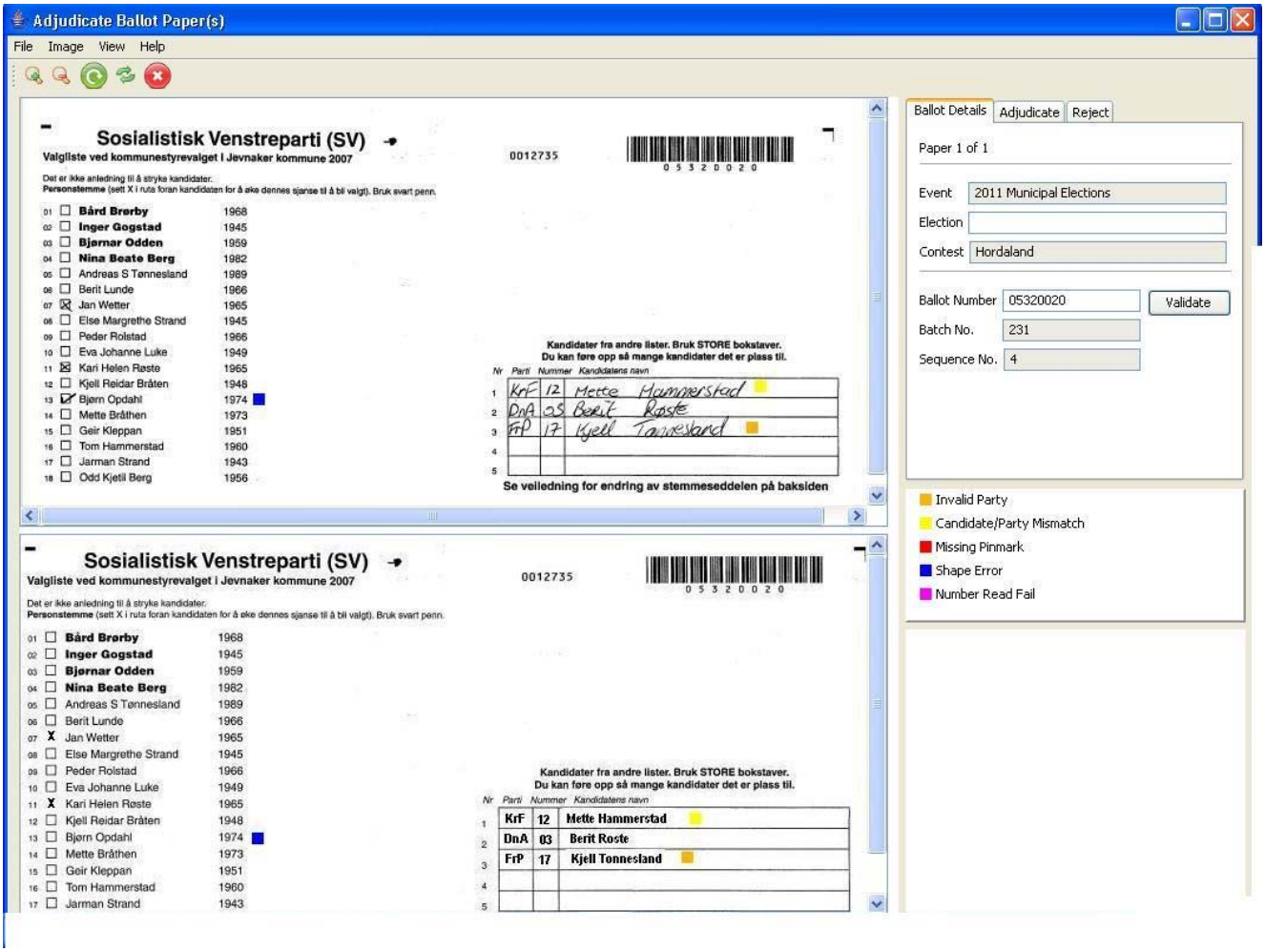

Figure 10 Illustration of ballot paper adjudication

The display will also provide information to assist in locating the original paper copy of the rejected ballot e.g. batch number and sequence number.

3.11. Use Case 3.4 Counting of e-votes

Elaboration of Requirement F 3.4.1

The counting of the e-votes will be done in two steps: anonymization and tabulation. During the anonymization step, input from the Electoral Roll will be used to remove the e-votes of the voters that have p-voted. In addition, if the voter has cast an e-vote from a controlled environment, the e-votes from the uncontrolled environment will be removed too, otherwise the last e-vote from the uncontrolled environment will be used.

During the tabulation process, all regulations that apply to the system will be followed, including that for small constituencies, results will not be published unless merged with another constituency.

Elaboration of Requirement P 3.4.1

In order to count 2,000,000 e-votes in 30 minutes using the voting protocol we have proposed, the system will have to make approximately 1,200 decryptions per second. This speed is achievable in the tabulation application with the HSM.

3.12. Use Case 3.5 Approval of p-votes and ballots

Elaboration of Requirement F 3.5.1

The Tenderer confirms that the Electoral Committee (EC) will have a screen where they can register votes received in a cover envelope and that should be verified according to the regulations (§10.1 and §10.2). This screen will be part of the E-roll Administration Client Application. If the vote is rejected, the EC selects the rejected status. This generates a serial number. The EC writes this number on the cover envelope for later referencing or re-verification. The EC can also enter a text (reason) for the rejection. The rejected cover envelope is put into a separate (rejected votes) pile. If the vote is accepted, the process is continued in the next use case (see F 3.5.2 below).

Elaboration of Requirement F 3.5.2

The Tenderer confirms that this requirement will be met.

If the vote is accepted, the voter can be looked up in the E-roll from the credentials on the cover envelope. The Electoral Committee can then set the marked off as (paper) voted in the E-roll. If the ballot inside the cover envelope is OK, it is put into the ballot box; otherwise it has to be rejected (see use case F 3.5.4 below).

Elaboration of Requirement F 3.5.3

The Tenderer confirms that the approved vote and final mark off will be stored in the E-roll (database).

Elaboration of Requirement F 3.5.4

The Tenderer confirms that this requirement will be met.

If ballots are questionable, either received in cover envelopes or from the Polling Committee on the Election Day they must be registered with status rejected by the Electoral Committee (EC) and put into a separate (rejected ballots) pile. Serial numbers are generated for rejected ballots. The EC writes this number on the ballot for later referencing or re-verification. The EC can also enter a text (reason) for the rejection.

Elaboration of Requirement F 3.5.5

The Tenderer confirms as stated above (see use case F 3.5.1) that the Electoral Committee will have functionality to register rejected votes both setting a rejected status and entering a text (reason) for the rejection.

Elaboration of Requirement F 3.5.7

The Tenderer confirms as stated above (see use case F 3.5.4) that the Electoral Committee will have functionality to register rejected ballots both setting a rejected status and entering a text (reason) for the rejection.

3.13. Use Case 4.1 Reporting to SSB

Elaboration of Requirement F 4.1.1

The Tenderer confirms that the Election System will present which reports can be run. The SSB reporting module will support transfer of data from Election System to SSB both in the preparation and the settlement phases. In the preparation phase, system data like party codes, contest information etc. will be transferred. In the settlement phase, prognosis and results will be transferred. Data transferred to SSB will form the basis for information available about the election contests to the media and the public.

The SSB reporting module will present the ECs with a list of reports grouped by contests to choose (select) from depending on the state of the ES.

Elaboration of Requirement F 4.1.2

The Tenderer confirms that the Electoral Committee will be able to select reports or system data from a contest and run an export data to SSB. This will be implemented in an easy point and click interface.

Results to SSB can be transferred even if the final count is not yet done, e.g. that the personal votes are missing in the first transfers. Until the final results are transferred, data to SSB serves for prognosis purposes only. Prognosis calculation is assumed to be carried out by SSB.

Elaboration of Requirement F 4.1.3

The Tenderer confirms that the Election System will export data via a service in the formats defined by the SSB. The Tenderer assumes that this will be a set of web services.

Elaboration of Requirement F 4.1.6

The Tenderer confirms that the Election System will interact with SSB confirmation messages about the transfer success or failure, as defined by SSB. The confirmation message (code) from SSB about each transfer will be stored in Election System connected to each run and exported report. The status for both success and failure (exception) will be stored.

Elaboration of Requirement F 4.1.8

Please note. Appendix 2B requested an elaboration on F4.1.9, not F4.1.8 as here in Appendix 2A. As F4.1.9 is a store exception, hence, we interpret the request to be an elaboration on F4.1.8.

The Tenderer confirms that the SSB reporting module will have a view of the log and status (confirmation or exception) of each run and exported report. The Election Committee will automatically be notified both on success or failure. On an exception (failure), the Election Committee will be notified as a task to act upon. The Election Committee can then log into the SSB reporting module and view the exception message from SSB. The SSB reporting module will allow for re-transmission of failed transfers.

3.14. Use Case 4.2 Settlement

Elaboration of Requirement F 4.2.1

The Tenderer confirms that the Election System will have functionality to aggregate the e-votes and p-votes results, and calculate the correct result. The output of the merge module is the total distribution of votes on parties/groups and candidates at each contest level.

After performing this operation, the relevant Electoral Committee for each contest has a complete overview of votes on parties and candidates for that contest. The function may be re-activated any number of times. Every time, the previous merger result will be time stamped and appended to a history folder, with the current merger result overwriting the previous one.

Elaboration of Requirement F 4.2.2

The Tenderer confirms that the Election System will calculate the correct distribution of seats and returning of members according to a preconfigured and selected method during the configuration setup. The E-valg 2011 delivery will ship only with support for Norwegian Parliamentary, Sami, County and Municipality Elections, i.e. only the modified Sainte-Laguës method to choose/select. Later on other, when moving the system to other countries and other regulations, other preconfigured distribution methods can be added. The interface for making new preconfigured distribution methods will be documented as a part of the E-valg 2011 delivery.

3.15. Use Case 5.1 Reporting

Elaboration of Requirement F 5.1.1

The Tenderer confirms that the designer will be able to select an election or referendum to edit or create a report for. The Election System will be delivered with a set of pre made template reports necessary to produce the output (election protocols, statistics and other content) necessary to meet the requirements given by the law and regulations for Norwegian Elections. A few templates for referendums will also be a part of the delivery. The premade report templates can be inherited or overridden (edited) for each individual election or referendum set up in the system. New report templates can be added at the election or referendum type level or at each individual election or referendum contest level.

The Report Design Component will present the designer with a list (tree view) of available elections and referendums either at type or contest level. Selecting the appropriate entry point will result a list of available report templates at the selected level. The designer can then choose to edit (override) an existing report template or to create a new one. Report templates can be set in-active or deleted. Deletion can only be done on custom made reports.

Elaboration of Requirement F 5.1.2

The Tenderer confirms that the designer will be able to create and configure new reports. When creating a new report, the designer can choose to base the new report on an existing report template or create it from scratch.

The proposed reporting tool (see SSA-U Appendix 3 for technical details) ships with a visual design tool. This makes it easy to do visual changes (e.g. changes in layout, rearrange elements and sections) to a report without requiring a deep understanding of the underlying system data structure. The data queries of a report can be made through an interactive point and click interface or by entering e.g. SQL queries directly. The data part of

report creation, as an opposite of visual designing, requires that the designer has a deep understanding of the Election System structure with its services and tables. This understanding can be obtained by studying the system documentation which will be included in the delivery.

The reports can be configured (set up) to run automatically at given a date/time or state in the Election process.

Elaboration of Requirement F 5.1.3

The Tenderer confirms that the system will be able to present a preview of the report. This is standard functionality that is part in the proposed reporting tool.

Elaboration of Requirement F 5.1.4

The Tenderer confirms that the Election System will be able to store the reports in the system. When a report is saved, it will immediately show up as a selectable and/or to run at a given election process date/time or stage report in the Report Run Component.

Elaboration of Requirement F 5.1.5

The Tenderer confirms that the Electoral Committee will have access to functionality in the Election Settlement Client Application to find and select elections and referenda, and extract reports from them. The elections and referenda will be presented in a list, and when an election or referendum has been selected, a list of available reports will be presented.

Elaboration of Requirement F 5.1.6

The Tenderer confirms that the Electoral Committee will have access to functionality in the Election Settlement Client Application to find and select elections and referenda, and extract reports from them. The elections and referenda will be presented in a list, and when an election of referendum has been selected, a list of available reports will be presented.

Elaboration of Requirement F 5.1.7

The Tenderer confirms that when a report on an election or referendum is selected, the results will be presented to the user. From there, the user will have access to functionality to manipulate the report, as described in Requirement F 5.1.8.

Elaboration of Requirement F 5.1.8

The Tenderer confirms that the Electoral Committee will have the possibility to manipulate the report results. The result window will, depending on the report type, have functions for sorting, filtering and grouping of the output. There will also be a save function to store the report result either in the Election System or to a local machine (e.g. for testing purposes). The system will log each report run. If the report result is stored back into the system, it will also be possible to view the output again later. Report results stored in the Election System will be tagged with run date/time or stage. The run and stored reports will be available in a list.

The proposed report tool can by default export reports to the most popular exchange formats, including CSV, HTML, PDF, RTF, XLS and XML. Other export formats can be supported by adding (installing) custom made plug-ins. The proposed report tool has several independent vendors of exchange format plugins, but these

plugins are not part of the proposed solution. The Tenderer proposes to discuss whether any of these plugins should be needed during the detailed design phase, including the consequences for security these plugins may have.

The Tenderer confirms that the Election System will have functionality to export data in the EML format. Relevant EML documents will be available as reports for elections and reports to the Electoral Committee in the Election System in the same menu where the other reports will be available.

The Tenderer confirms that the Election System will have functionality to export reports in formats required for the production of ballots and polling cards. This functionality will be designed to be OCR and ICR readable by the electronic counting of p-votes module (see Use Case 3.3). The report for production of voting cards will be designed with voter unique bar codes to allow scanning and direct lookup of voters in the E-roll application (see UC 3.1).

The Tenderer confirms that it will be possible to export reports that are to be published on public portals in standard exchange formats. In addition, non-standard exchange formats can be ordered as custom-made or separately available plugins to the proposed reporting tool, but they are not part of the proposed solution.

The Tenderer confirms that it will be possible to attach the reports exported in one of the formats mentioned above to e-mails. The procedure to do this will be to save the report locally to a file, and then attach the file to an e-mail created in the user's e-mail client.

The Tenderer confirms that reports that are to be transferred to SSB will conform to the services and data exchange formats defined by the SSB (see Use Case 4.1).

The Tenderer confirms that the Election System will have functionality to approve reports, like e.g. Election Protocols. In these scenarios, the appropriate users, e.g. the Electoral Committee leader, will be notified with an approval task to act upon. When approved, the report result (output) can then either by published or transferred automatically or manually depending on the report type.

Elaboration of Requirement F 5.1.9

The Tenderer confirms that the Report Designer Component will allow the designer to choose from existing reports. See F 5.1.1 above for more information.

Elaboration of Requirement F 5.1.10

The Tenderer confirms that the Report Designer Component will allow the designer to edit existing reports. See F 5.1.2 above for more information.

3.16. Use Case 5.2 Auditing

Elaboration of Requirement F 5.2.1

The Tenderer confirms that all significant events in the system will generate audit entries. Each audit entry will have an associated timestamp clearly recorded. The audit entry also includes a digital timestamp proving the authenticity of the entry and protecting the integrity of the log. This digital timestamp is obtained from a trusted time-stamping service in the Auditing Server and will ensure that any tampering of audit trails is identifiable.

Time-stamping service is based upon binary-linking schemes described more deeply in an article "Time-Stamping with Binary Linking Schemes" which is added as attachment 3 to this appendix.

Discrete software components from across the entire solution will all generate component specific audit events. These can include election transactions, election configuration changes, electoral roll updates, list submission alterations, approvals, changes in the state of a ballot etc. All audit entries will be recorded in local data stores maintained by the software component. All entries will have a digital time-stamp generated from the same trusted service.

Separate operating system level events identifying system access, failures, malfunctions and potential threats will be recorded in the relevant system logs. Each entry will be digitally time-stamped. Periodically, and on demand, each discrete system will generate an EML 480 export and transmit the information to a central audit receiver, the Auditing Server. This component will integrate all separate logs into one complete audit trail for the entire election system. The individual component logs will be retained to provide an additional fraud prevention measure.

Elaboration of Requirement F 5.2.2

The Tenderer confirms that the central audit receiver will provide the auditor with access to review, filter and search through a complete audit trail of significant events. Search and filter capability will be available through an audit management console, whilst distinct reports can be created and accessed through the report generator component.

Elaboration of Requirement F 5.2.3

The Tenderer confirms that the auditor will have the ability to create and run reports against the audit trail. These reports will be created using the functionality described in Use Case 5.1 Reports, using the database engine of the Auditing Server as the data source.

Elaboration of Requirement F 5.2.4

The Tenderer confirms that the central logging facility will have a monitoring service active at all times seeking events that indicate abnormal behavior within the election system. Abnormal behavior can include a substantial number of e-votes cast within a timeframe from a single account, or administration or e-voting accounts being locked out. The abnormal behavior can be presented to the auditor either visually via a dashboard display and/or by an alert message via e-mail and/or SMS.

Elaboration of Requirement F 5.2.5

The Tenderer confirms that the auditor can request that a particular event or pattern generate an alert and therefore to be notified more urgently of a particular occurrence. All patterns specified to the monitor service can also be configured to generate an alert message.

If any of the separate systems generate an audit entry that has been configured through the election management system as worthy of immediate alert, the source system will automatically trigger an EML480 export to the central audit receiver when the appropriate audit record has been committed locally. This ensures that the auditor is made aware as early as possible of the marked event. Subsequent periodic EML480 exports will continue as normal.

Elaboration of Requirement F 5.2.6

The Tenderer confirms that the auditor will be able to alter parameters for detecting abnormal behavior within the system. Certain behavior patterns will need to be predefined within the monitor service, however, the attributes measured by these patterns such as 'number of attempts' or 'within *n* minutes' can be amended using the Auditing Application. Additionally, if these patterns are detected, the auditor can elect to receive an alert message via the same console.

Elaboration of Requirement P 5.2.1

The Tenderer confirms that the audit functions and any analysis of audit entries will have no impact on the voting system capacity. Calls to the time stamping service will provide no measurable delay in the system capacity to handle the associated process. All reporting and searching will be performed on a dedicated system and therefore have no impact on any aspect of the election process.

Elaboration of Requirement P 5.2.2

The Tenderer confirms that, as the primary monitoring and reporting will be performed on a dedicated system with dedicated database engine, the solution can be tuned to provide optimum response times.

3.17. Use Case 9.1 Authentication

Elaboration of Requirement F 9.1.3

The Tenderer confirms that the user will be able to access the system. The voter accesses the E-Voting Client Application by entering the correct URL in his browser. The URL will be made public and included on the polling cards, as to minimize phishing attacks. An unauthenticated user will only see a simple welcome page with some general information about the website, including some information about how he can log on.

Elaboration of Requirement F 9.1.9

The Tenderer confirms that the Election System will check the user rights when the user has logged on. An overview over de roles will be returned to the user, who can then select the appropriate role for the task he wants to perform. The roles in the list will be in accordance with Use Case 0.1 Definition of Roles.

Elaboration of Requirement F 9.1.10

The Tenderer confirms that the user will be able to select the role he wants to use when he has logged on to the system. The user will be able to select the appropriate role for the task he wants to perform in an intuitive way, e.g. by selecting it from a drop-down list. From that point on, the user will gain access rights to the various services of the Election System in accordance with the role he chose.

Elaboration of Requirement F 9.1.11

If authorized individuals would be allowed to issue temporary credentials to voters who arrive at the Polling Station without an approved eID, then it would not be possible to use these temporary credentials to sign the e-vote digitally. It is therefore the Tenderer's opinion that this requirement is in conflict with some of the security requirements, and should not be implemented.

Elaboration of Requirement F 9.1.12

If authorized individuals would be allowed to issue temporary credentials to voters who arrive at the Polling Station without an approved eID, then it would not be possible to use these temporary credentials to sign the e-vote digitally. It is therefore the Tenderer's opinion that this requirement is in conflict with some of the security requirements, and should not be implemented.

Elaboration of Requirement F 9.1.13

If authorized individuals would be allowed to issue temporary credentials to voters who arrive at the Polling Station without an approved eID, then it would not be possible to use these temporary credentials to sign the e-vote digitally. It is therefore the Tenderer's opinion that this requirement is in conflict with some of the security requirements, and should not be implemented.

Elaboration of Requirement F 9.1.14

If authorized individuals would be allowed to issue temporary credentials to voters who arrive at the Polling Station without an approved eID, then it would not be possible to use these temporary credentials to sign the e-vote digitally. It is therefore the Tenderer's opinion that this requirement is in conflict with some of the security requirements, and should not be implemented.

4. Elaboration of Accessibility and Usability Requirements

Elaboration of Requirement AU 1

The Tenderer confirms that the applications will provide HTML structured according to the logical information flow to support all users also those in need of assistive devices.

Elaboration of Requirement AU2

The Tenderer confirms that the E-voting client will support the browsers and platforms (operating systems) supported by eID. Due to our use of JavaScript, the user will be given a message if the browser doesn't support JavaScript or if JavaScript is turned off or is uninstalled.

Elaboration of Requirement AU3

The Tenderer confirms that the user can change language. The language will be decided by the user before he logs in to the system, so the correct language files will be fetched. For the e-vote client, the default language set in the operating system will be detected to present the application in this language. The user can thereafter decide to change to another language if decided.

Elaboration of Requirement AU4

The Tenderer confirms that possible file attachments will be provided in the following required formats depending on use and application:

- PDF 1.4 or newer, or PDF/A – ISO 19005-1
- ODF – ISO/IEC 26300

- OOXML

Elaboration of Requirement AU5

The E-voting client is designed to only call the server on login and when the vote is being sent. During the first server call all needed information (HTML, JavaScript, CSS and images) will be downloaded to the client machine. We will exceed the 200 kb limit a little bit, but this only in the login process. During the voting process there will be no communication with the server until the votes are submitted.

Elaboration of Requirement AU6

The Tenderer confirms that the thin client applications in the system will be unit independent. Our E-voting client, an internet application, can be used independently of place or unit. Our Election Preparation solution, another internet application, can be used independently of place or unit. Our thick client scanning application can be deployed on any PC running a Windows client OS (XP, Vista) that has a scanner attached with the necessary TWAIN drivers installed to operate the scanner.

Elaboration of Requirement AU7

The Tenderer confirms that the applications will support and function well within the defined standard resolution ranges (800x600 and up).

Elaboration of Requirement AU8

The Tenderer confirms that the possibility to change text size and contrast will be available in the final solution.

Elaboration of Requirement AU9

The Tenderer confirms that the system will work (consistent and standardized) with both mouse pointers and keyboards. Our structure of information will make use of keyboard function in an easy and efficient manner. The system has been design to be device independent.

Elaboration of Requirement AU10

The application is using CSS (Cascading Style Sheets) with Thiresias as the first choice of font and then Arial, Verdana and sans-serif as the following. The final solution will have the possibility to change font sizes to handle demands of the Norwegian association of the Blind and Partially Sighted (Blindeforbundet).

Elaboration of Requirement AU11

The Tenderer confirms that the login process will be as accessible and user friendly as possible, indeed this premise applies to the complete system as a whole.

Elaboration of Requirement AU12

The Tenderer confirms that the system does not make use of applets, flash or plug-ins, and does not have any technology-related barriers for the users.

Elaboration of Requirement AU13

Our development tool for the E-voting client, GWT (Google Web Toolkit) for making RIA (Rich Internet Applications), generates JavaScript. GWT's support for ARIA-roles (Accessibility in RIA) will make the E-voting client confirm to the accessibility requirements.

Elaboration of Requirement AU14

The E-voting client makes no server calls between login and submitting the ballots. This makes our solution faster and will guarantee a minimum wait for the requested page to be loaded.

Regarding Requirements WG 1.2 Time based media

Note that Tenderer will provide the possibility to show media if needed, but not the content of the media (video, audio and transcripts). The customer will have to provide the content.

5. Elaboration of Security Requirements

General note on the elaborations in this section

The architecture of the internet voting system is detailed in Appendix 3, "Customer Technical Platform". Several elaborations refer to this document.

Elaboration of Requirement OS 0.4

The Tenderer confirms that this requirement will be met via technological, not cryptographical means: correct software design and implementation. Although each voter is allowed to vote several times electronically, only the last ballot is taken into account per contest. The distinction between ballots to be tallied and the ballots to be discarded is done by the Anonymizer application right before the anonymization of the voter's ballot.

The loss of ballots can only occur if both instances of Storage Module fail or are destroyed at the same time.

Elaboration of Requirement OS 0.6

The Tenderer confirms that this requirement will be met via technological and cryptographical means: synchronized E-vote Stores, integrity checking in E-vote Stores, and public key cryptography.

A ballot is kept double-enveloped in the E-vote Store, as explained in the section "Security aspects" in Appendix 3. The only way through which a ballot could be inserted in the E-vote Stores is through an authenticated SSL channel with E-voting Collection Server. This can be achieved via E-voting Client Application, and it will be only possible way to do so. The E-vote Stores maintain their database integrity with trusted execution environment. To bypass this mechanism the attacker must modify the contents of the environment. The fact that several co-operating election officials have compromised the trusted execution environment will be discovered by auditors executing the remote attestation protocol. The same mechanism also protects against the deletion of ballots. See the section "Trusted execution" in Appendix 3 for more information.

Elaboration of Requirement OS 0.9

The Tenderer confirms that this requirement will be met through the system architecture.

	Failure recovery
E-voting Collection Server	The E-voting Collection Server has an easily restorable read-only state. In case back-up of data and code for the E-voting Collection Server is saved in the pre-election stage, no fatal loss of data can occur here.
Messenger	The Messenger has an easily restorable read-only state. In case back-up of data and code for the Messenger is saved in the pre-election stage, no fatal loss of data can occur here. The Messenger has a private key stored in an HSM. This key must be backed-up to an external token and stored in a safe.
E-vote Stores	In the E-vote Stores data loss can occur. If both E-vote Stores cease to exist at the same time, then the election cannot be restored. There are two synchronized E-vote Stores in the system, both of them using high availability hardware. In case one of the E-vote Stores fails, the election will not be operational until another unit is set-up and synchronized with the existing unit.
Anonymizer	The Anonymizer application performs a function that can always be executed once more, given that the inputs are present.
Tabulation	The Tabulation application performs a function that can always be executed once more, given that the inputs are present. The Tabulation application has a private key stored in an HSM. This key must be backed-up to an external token and stored in a safe.

Network errors will only cause availability problems, and recovery from them will be automatic.

In case any SSL keys are stored in the HSMs, those keys should be backed-up too.

Elaboration of Requirement OS 0.12

The Tenderer confirms that this requirement will be met by the design of voting protocol. The E-voting Client Application will receive a notification from the E-voting Collection Server after the E-vote Stores have reported the fact of storage.

Elaboration of Requirement OS 0.12B

The Tenderer confirms that this requirement can be met as an option. The current state of the cryptographic protocol used needs additional research to find a suitable end-to-end proof method that wouldn't dramatically decrease the system scalability. It is to be noted that as in most cases, here too a decision between security and scalability has to be made. Indeed, methods for end-to-end proofs tend to have high computational complexity.

However, the Tenderer wants to point out that the requirement will already be met functionally in the base solution. Through the Auditing Module the system will be able to provide an auditing trail up to the tabulation process, but the tabulation process itself has to be trusted. This compromise is sensible as the correctness of the tabulation code is relatively easy to prove, and with the help of trusted execution hardware we can ensure that the audited code gets executed. See also Appendix 3, "Trusted execution".

Elaboration of Requirement OS 0.13

The Tenderer confirms that this requirement will be met via technical and cryptographical means. The Messenger will send integrity check-codes to the voters about the ballots that were stored in the E-vote Stores. Two E-vote Stores will store the vote in a synchronized and integrity-preserving way.

Elaboration of Requirement OS 0.14

The Tenderer confirms that this requirement will be met via the architecture of the E-voting Collection Server and Election Settlement Server. The execution of this architecture relies on organizational protocols, and the architectural decisions support those protocols. The functionality that allows the removal of double-envelopes – the anonymization step– is only available after the end of the election stage. Only then can the votes be tabulated and results acquired. The tabulation process, executed in an air-gapped system, requires the presence of N of M election officers (5 of 9 for example) to be started.

No information is published by the Tabulation application itself: these processes are initiated by election officers on the Election Settlement Server.

Elaboration of Requirement OS 0.15

The Tenderer confirms that the Election System will be able to maintain reliable synchronized time sources. However, this requires an external source for the precise time, e.g. by a simple GPS receiver or an official source of precise time, if any is available. The servers that have a connection to the precise time source will run an NTP server, while all other servers in the system will synchronize their clocks using NTP.

Elaboration of Requirement OS 0.17

The Tenderer confirms that lists forwarded for the production of ballot papers shall be protected against unauthorized access and changes. List proposals submitted to the Election System remain within the solution for the lifetime of the data. Only authorized users will have access to the system and access rights must be granted before changes can be made. All changes are fully audited and key events require secondary approval by another official with equal or higher privilege. When the lists have been fully verified and approved, the selected print supplier will access the data directly from the Election Preparation system through the printer interface to facilitate the production of ballot papers.

Elaboration of Requirement OS 0.18

The Tenderer confirms that the requirement will be met via the system architecture. The E-voting Collection Server will have no means to remove a voter from electoral roll.

Elaboration of Requirement OS 1.2

The Tenderer confirms that the requirement will be met via organizational, technical and cryptographical means. The voters are distinguished by the fact that they are on the electoral roll and have sufficient means to prove so. This means that:

- The voter is on the electoral roll, has an eID and is able to use it to authenticate himself.
- The voter is on the electoral roll and has credentials that identify him to an official in the polling station.

The Norwegian person number (*personnummer*) can be used as a unique identification number for every voter.

Elaboration of Requirement OS 3.1

The Tenderer confirms that the requirement will be met via technical and cryptographical means. There is no place on the server side where the voter's identity and the clear-text ballot can be linked to each other. The only part of the system where the clear-text ballot and voter's identity are available at the same time is in the E-voting Client Application. On the server side the vote is stored securely, i.e. in a double-enveloped manner. Those components that see the voter's identity will only see a double-enveloped ballot and cannot open the inner envelope. The Tabulation application can open the inner envelopes, but will receive the votes already anonymized, i.e. with the outer envelopes containing the digital identities removed. Decrypted ballots contain no information that will link them back to the actual voter.

Elaboration of Requirement OS 3.3

The Tenderer confirms that the requirement will be met via technical and cryptographical means. There is no place on the server side where the voter's identity and the clear-text ballot can be linked to each other. The only part of the system where the clear-text ballot and voter's identity are available at the same time is in the E-voting Client Application. On the server side the vote is stored securely, i.e. in a double-enveloped manner. Those components that see the voter's identity will only see a double-enveloped ballot and cannot open the inner envelope. The Tabulation application can open the inner envelopes, but will receive the votes already anonymized, i.e. with the outer envelopes containing the digital identities removed. Decrypted ballots contain no information that will link them back to the actual voter.

Elaboration of Requirement OS 3.4

The Tenderer confirms that the requirement will be met via technical and cryptographical means. There is no place on the server side where the voter's identity and the clear-text ballot can be linked to each other. The Tabulation application can open the inner envelopes, but will receive the votes already anonymized, i.e. with the outer envelopes containing the digital identities removed. Decrypted ballots contain no information that will link them back to the actual voter. No results will be published for counts containing fewer than 100 votes.

Elaboration of Requirement OS 3.5

The Tenderer confirms that the requirement will be met via technical and cryptographical means. The E-voting Collection Server cannot open the inner envelope and present its contents to the E-voting Client Application. The integrity check-codes sent to voter are specific to the voter and do not contain direct information about the voter’s vote in clear-text. No information about whether the vote shall be counted or not shall be given. See also Appendix 3, "Security aspects" for more information.

Elaboration of Requirement OS 3.6

The Tenderer confirms that the requirement will be met via the system architecture. As there is no place in the system where the voter's identity and the clear-text ballot can be linked to each other, the auditing system will have no way of connecting them either. See Appendix 3, "Security aspects" for more information.

Elaboration of Requirement OS 4.1

The Tenderer confirms that the requirement will be met via cryptographical means. Vote confidentiality is achieved through a public-key encryption scheme. The inner envelope is produced using a public key encryption method (ElGamal) to the ballot in E-voting Client Application. This inner envelope can only be

opened by the owner of the corresponding private key, i.e. the Tabulation application. No information about voter's identity will be inside in the inner envelope.

Elaboration of Requirement OS 4.2

The Tenderer confirms that the requirement will be met via the system architecture. The Tabulation application and Messenger both have private keys, used to ensure vote confidentiality. These keys are stored on both a physical and logical security level according to FIPS 140-2 level 3 and CC EAL4+. See also Appendix 3, "Components" for more information.

Elaboration of Requirement OS 4.3

The Tenderer confirms that the requirement will be met via technical and cryptographic means. Access to the voters' registers stored in the E-voting Collection Server will only be granted to successfully authenticated election officials. Voters will only have access to data they have sufficient credentials for. In addition, the communication between different components is secured. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 4.7

The Tenderer confirms that the requirement will be met. In the cryptographic protocol, ElGamal with a key length of 2048 bits or ECC with a key length of 224 will be used. These respective key lengths are generally considered to be equivalent to an RSA key length of 2048 bits. In addition, wherever SSL is used, it will be configured such that the strength is equivalent or better than RSA with 2048 bit keys for asymmetric algorithms, and AES-256 for symmetric algorithms.

Elaboration of Requirement OS 4.8

The Tenderer confirms that wherever hashing algorithms will be used, included in the cryptographic protocol, they will have a strength equivalent to SHA2 or better.

Elaboration of Requirement OS 4.9

The Tenderer confirms that this requirement will be met. Votes are stored in double envelopes which provide both encryption and integrity. See also Appendix 3, "Security aspects" for more information.

Elaboration of Requirement OS 4.11

The Tenderer confirms that this requirement will be met. The Tabulation application and Messenger both have private keys, used to ensure vote confidentiality. These keys are stored on both a physical and logical security level according to FIPS 140-2 level 3 and CC EAL4+. Tokens protecting access to the keys of the Tabulation application and the Messenger will be stored on smart cards or similar devices. See also Appendix 3, "Components" for more information.

Elaboration of Requirement OS 5.1

The Tenderer confirms that this requirement will be met via the system architecture. The connection between the E-voting Client Application and the E-voting Collection Server is mutually authenticated, and documentation will be written to explain to the general public how the verify this. The same applies to the

verification of the authenticity of the ballot presented in the E-voting Client Application. Organizational measures must be taken to publish the necessary information in the media. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 5.4

The Tenderer confirms that this requirement will be met via the system architecture. On-line communications will be mutually authenticated using SSL certificates, and information will be digitally signed where appropriate. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 6.1

The Tenderer confirms that this requirement will be met. The components in the E-voting and Election Settlement Module having direct access to a secure execution environment in an HSM will be able to verify the code directly. Other components will rely on integrity checking provided by a remote HSM. See also Appendix 3, "Trusted execution environment" for more information.

Elaboration of Requirement OS 6.2

The Tenderer confirms that this requirement will be met. With help of a secure execution environment provided by HSM technology, the Auditing Application will be able to remotely attest the state of the E-voting Collection Server. See also Appendix 3, “Trusted execution environment” for more information.

Elaboration of Requirement OS 7.1

The Tenderer confirms that this requirement will be met. The roles in the system will be defined according to Use Case 0.1 Definition of roles, and managed in the Election Preparation Module. For off-line components, the role system of the underlying operating system will be used. However, a script defining the users and roles on these components will be generated based on the users and roles managed in the Election Preparation Module. See also Appendix 3, “User roles”, for more information.

Elaboration of Requirement OS 7.2

The Tenderer confirms that this requirement will be met. The roles in the system will be defined according to Use Case 0.1 Definition of roles, and managed in the Election Preparation Module. For off-line components, the role system of the underlying operating system will be used. However, a script defining the users and roles on these components will be generated based on the users and roles managed in the Election Preparation Module. See also Appendix 3, “User roles”, for more information.

Elaboration of Requirement OS 7.3

The Tenderer confirms that this requirement will be met. The roles in the system will be defined according to Use Case 0.1 Definition of roles, and managed in the Election Preparation Module. For off-line components, the role system of the underlying operating system will be used. However, a script defining the users and roles on these components will be generated based on the users and roles managed in the Election Preparation Module. See also Appendix 3, “User roles”, for more information.

Elaboration of Requirement OS 7.6

The Tenderer confirms that this requirement will be met by the system. In fact, outside the E-voting Client Application, which runs only locally on the voter's PC, there is no such stage where a vote is not completely anonymous. The most sensitive processes are anonymization and tabulation where the integrity of the votes has to be preserved. These processes are executed on air-gapped computers, with at least two election officials authenticated. Trusted execution technology is used to run the algorithms so that only audited code will be executed.

Elaboration of Requirement OS 7.7

The Tenderer confirms that this requirement will be met via the system architecture. The key management components are capable to perform N-out-of-M authentication protocols. See also Appendix 3, "Components" for more information.

Elaboration of Requirement OS 7.8

The Tenderer confirms that this requirement will be met via the system architecture. No HSM will be installed in an uncontrolled environment. HSMs used in controlled environments shall be at least FIPS 140-2 Level 3 certified. See also Appendix 3, "Components" for more information.

Elaboration of Requirement OS 7.9

The Tenderer confirms that this requirement can be met as an option: a cryptographic algorithm can be implemented to generate the private keys in different HSMs, and merge them right before the encryption.

However, the Tenderer wants to point out that the requirement will already be met functionally in the base solution. Private keys will be generated in HSMs certified on FIPS 140-2 level 3 and Common Criteria EAL4+. The keys generated in the HSMs will be based on random number generation based on hardware, and approved by FIPS. The private keys generated this way will be protected through an AES encryption key shared across a secret sharing algorithm based on smart cards. The keys are protected within the FIPS 140-2 level 3 boundaries, so they will never leave the HSM tamper boundary.

Elaboration of Requirement OS 7.11

The Tenderer confirms that this requirement will be met. The access to authentication data will be protected, and it will be possible to check its integrity through the Auditing Application.

Elaboration of Requirement OS 7.14

The Tenderer confirms that this requirement will be met. Wherever a separation of duties is necessary, different roles mapping to the different duties can be created, and these roles will give access to different functionalities or services. In addition, some of the functionalities or services can be made mutually exclusive ensuring no overlap of duties. Different users within the group of election officers can then be assigned to these different roles. All this can be done according to Use Case 0.1 Definition of roles. See also Appendix 3, "User Roles" for more information.

Elaboration of Requirement OS 7.17

The Tenderer confirms that requiring two-factor authentication for administrators, operators and auditors will be possible. It should be decided later exactly which method should be used.

Elaboration of Requirement OS 8.1

The Tenderer confirms that e-votes that have been acknowledged will not be lost or altered under any circumstance. This can be ensured using synchronized E-vote Stores, integrity checking in the E-vote Stores, and public cryptography.

The E-vote Stores protect their database integrity through the trusted execution environment. To bypass this mechanism, an attacker would have to modify the contents of that environment. If several co-operating election officials have compromised the trusted execution environment, it will be discovered by the auditors when they execute the remote attestation protocol. This mechanism protects both against the alteration and the deletion of ballots. See Appendix 3, “Trusted Execution Environment” for more information.

Elaboration of Requirement OS 8.4

The Tenderer confirms that it will not be possible to alter, delete or add vote records undetected during transfer in the network or between system modules or components. This will be done through technical and cryptographic measures

E-Vote

- In order to alter a vote, an attacker would have to break the digital signature scheme.
- In order to add a vote on someone else’s behalf, an attacker would have to break the digital signature scheme.
- As soon as it has been stored in the E-vote store, the deletion of a vote will be registered by the auditing system and the integrity checks in the E-vote Stores.

Counting of P-Votes

- Cross checks will be made to ensure the total number of ballots issued, the number of images scanned and the number of votes extracted and counted all tally.
- Key securable objects such as the vote table within the e-Count database will be configured as write-only
- The e-Count is performed on an air-gapped network ensuring highly restricted and controlled access.

Elaboration of Requirement OS 8.5

The Tenderer confirms that the Election System will maintain the confidentiality of the votes and keep them sealed until the counting process. Only the Tabulation Application will be able to decrypt the e-votes, and the decryption key will be shared such that at least N out of M election officials must be present. See also Appendix 3, "Security aspects" for more information.

Elaboration of Requirement OS 8.6

The Tenderer confirms that this requirement will be met. All sources of sensitive information will be authenticated. Digital signatures will be used to protect integrity. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 8.7

The Tenderer confirms that this requirement will be met through cryptographic measures. When a voter has voted, a check-code will be sent to the voter over SMS. The message will be cryptographically connected to the ballot. If an attacker has modified the ballot, then the check-code will differ from the check-code corresponding to the voter's party and/or candidate choice on his polling card. In that case, the voter should notify the election officials. If some of the voters verify the check-codes, then systematic manipulation by an attacker can be ruled out. See also Appendix 3, "Cryptographic protocol" for more information.

Elaboration of Requirement OS 8.9

The Tenderer confirms that the Election System will detect and report any unauthorized changes to a vote.

E-Vote
When a voter has voted, a check-code will be sent to the voter over SMS. The message will be cryptographically connected to the ballot. If an attacker has modified the ballot, then the check-code will differ from the check-code corresponding to the voter's party and/or candidate choice on his polling card. In that case, the voter should notify the election officials. If some of the voters verify the check-codes, then systematic manipulation by an attacker can be ruled out.

In addition, if changes are made to e-votes stored in the E-vote Store, or begin processed further down the Election System, changes will be detected by the Auditing Module.

P-Vote/e-Count
Access to the separate, air-gapped e-count network is highly restricted and controlled. Updates made officially to votes through the adjudication process are audited and the process is displayed openly on double screen terminals ensuring the process is constantly under scrutiny. Additionally the paper and image copy of the ballot will always remain as a verifiable record of the vote cast.

See also Appendix 3, “Cryptographic protocol” and “Security Aspects” for more information.

Elaboration of Requirement OS 8.10

The Tenderer confirms that this requirement will be met. When a voter has voted, a check-code will be sent to the voter over SMS. The message will be cryptographically connected to the ballot, and should be checked against codes printed on the voter’s polling card. The SMS message will not be digitally signed, as there is no standard way of doing it and no support for verification in mobile phones. The E-voting Server will also digitally sign its reply to the E-voting Client Application as an additional measure.

Elaboration of Requirement OS 8.12

The Tenderer confirms that the anonymization of the e-votes and the tabulation will be done in parts of the Election System that is air-gapped. See also Appendix 3, "Components" for more information.

Elaboration of Requirement OS 8.13

The Tenderer confirms that this requirement will be met. The vote-casting annotation will be made into the Electoral Roll right after the vote has been stored in the E-vote Stores.

Elaboration of Requirement OS 8.14

The Tenderer confirms that the sources of the data containing the electoral roll and the lists of candidates will be authenticated. All sensitive communication between the Election System and the outside world will be authenticated. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 8.15

The Tenderer confirms that it will be possible to verify the integrity of the data transferred between system modules and components. Data that could be tampered with by an attacker will be digitally signed. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 8.16

The Tenderer confirms that this requirement will be met. All sensitive communication between the Election System and the outside world will be authenticated. Data that could be tampered with by an attacker will be digitally signed. See also Appendix 3, "Communication policies" for more information.

Elaboration of Requirement OS 8.17

The Tenderer confirms that no functions will exist that allow election officers to reset the Election System to its initial state after the polling phase has begun. This requirement will be met through the system architecture, and certain operations will be available in certain stages of election process.

Elaboration of Requirement OS 8.18

The Tenderer confirms that votes stored or communicated outside controlled environments will be encrypted. E-vote will be either encrypted or anonymized at all times, except in the E-voting Client Application before encryption. See also Appendix 3, "Security aspects" for more information.

Elaboration of Requirement OS 8.19

The Tenderer confirms that it will be ensured that the Election System presents an authentic ballot to the voter. Even though a Trojan on the voter's client computer can alter the ballot on the screen in the E-voting Client Application, any of its activity will be detected by the cryptographic voting protocol that ensures the vote's integrity. See also Appendix 3, "Cryptographic protocol" for more information.

Elaboration of Requirement OS 9.1

The Tenderer confirms that this requirement will be met. All of the components, except for the E-vote Stores will be easily replaceable in case of failure. For that reason there will always be two synchronized E-vote Stores in the system at all times. In case of failure in one module a replication procedure can be started.

The Auditing Application has functionality to perform a self-check protocol to ensure that all system components are functioning as intended.

The high-availability features in system architecture support the use of organizational measures and high-availability hardware:

- All server components must have RAID controllers.

- All server components must have doubled power supply units.
- Authentic back-up configurations must exist at all times.
- Private keys must be backed up or redundant HSMs must be installed.
- Different Internet Service Providers should be used to connect the E-voting Collection Server to the internet

Elaboration of Requirement OS 9.2

The Tenderer confirms that the system architecture will not impede the quick restoration of the e-voting services in the case of a system restart. It should be noted though that some operations, e.g. such as the activation of keys stored in a HSM, must be carried out by election officials before election can continue. See also Appendix 3, "Availability" for more information.

Elaboration of Requirement OS 9.4

The Tenderer confirms that this requirement will be met. The Auditing Application has functionality to execute self-check protocol to ensure that all system components are functioning as intended. See also Appendix 3, "Availability" for more information.

Elaboration of Requirement OS 9.5

The Tenderer confirms that this requirement will be met. There will be an optional configurable parameter that allows to set sensible maximum to the number of votes allowed per voter.

Elaboration of Requirement OS 10.1

The Tenderer confirms that the authenticity, availability and integrity of the voters' registers and lists of candidates will be maintained. The Election Preparation Module will control all election data from its submission by the relevant group or party, throughout the various approval stages and final sign-off until its onward transmission to printers and the E-voting component. The same applies to the voters' registers store in the E-roll. Data can be viewed and changes made only by appropriately authorised individuals and all interested parties will be notified as changes in status occur. All changes will be fully tracked and audited. As data remains within the Election Preparation Module and E-roll throughout its lifespan, the authenticity, availability and integrity of voters' registers and lists of candidates is maintained.

Elaboration of Requirement OS 11.5

The Tenderer confirms that the components of the Election System that will be exposed to the PND will be properly protected against hacking, malicious software of any kind and DNS attacks. It will be achieved through a combination of organizational, physical and technological security measures. Remote electronic access to the servers is minimized, so that only absolutely necessary services are provided over the network. In particular, remote administration of servers will not be allowed. The servers are located behind firewalls. The number of external services that used by servers will be minimized. Private (virtual) channels are established for external services if possible. The servers are also deployed on the secure server platforms. Physical access to the servers is limited using physical and organizational security measures.

Elaboration of Requirement OS 13.2

The Tenderer confirms that this requirement will be met via the Auditing Module. The Auditing Application will have functionality to execute a self-check protocol to ensure that all system components are functioning as intended.

Elaboration of Requirement OS 13.3

The Tenderer confirms that this requirement will be met via the Auditing Module. Each component will track its operations, and access control to the audit logs will be role based. Most important events will be connected securely by digital time-stamping.

Elaboration of Requirement OS 13.4

The Tenderer confirms that an Auditing Module will be designed and implemented as a part of the Election System, and all components will send relevant audit records to the Auditing Module for secure storage. See also the functional description of the Auditing Module in Appendix 3 for more information.

Elaboration of Requirement OS 13.5

The Tenderer confirms that this requirement will be met. The Auditing Server in the Auditing Module will provide a service to store audit records centrally, in addition to the local storage in each component of the Election System. The Auditing Application will provide facilities for monitoring and verification, including the generation of audit reports. See also the functional description of the Auditing Module in Appendix 3 for more information.

Elaboration of Requirement OS 13.6

The Tenderer confirms that the Auditing Module will be open and comprehensive:

- Open: the time-stamping methods used for auditing will all be well-known and previously published. See included article "Time-Stamping with Binary Linking Schemes" for more information. The solution itself will be open source. The software includes functionality to publish data that can be used by third parties to verify that the log has not been tampered with.
- Comprehensive: all system components shall be included in the auditing process.

The Auditing Module will also actively report on potential issues and threats. A set of normal scenarios will have to be defined, and any deviation from those scenarios will be reported immediately.

Elaboration of Requirement OS 13.8

The Tenderer confirms that this requirement will be met via the Auditing Module. All relevant information relating to the voting procedures will be logged securely using the digital time-stamping system.

Elaboration of Requirement OS 13.9

The Tenderer confirms that this requirement will be met. Each step in the lifecycle of a ballot is securely logged using the Auditing Module. This log can be later analyzed against the state of the components to see whether there are any inconsistencies or not.

Elaboration of Requirement OS 13.10

The Tenderer confirms that this requirement will be met. Each step in the lifecycle of a ballot is securely logged using the Auditing Module. This log can be later analyzed against the state of the components to see whether there are any inconsistencies or not.

Elaboration of Requirement OS 13.11

The Tenderer confirms that this requirement will be met. The Auditing Module will not be exposed to the internet. It is possible to verify the integrity of the Auditing Module at all times, so that if anything is modified, it can immediately be detected.

Elaboration of Requirement OS 13.13

The Tenderer confirms that this requirement will be met. All server-side components will execute a self-check on the data integrity after a reboot.

Elaboration of Requirement OS 14.1

The Tenderer confirms that this requirement will be met. The election servers will be installed from authorized and audited software disks and configured with the election data from Election Preparation Module under the supervision of auditing personnel. The resulting configuration will be integrity checked, and the data loaded into trusted execution environment will be digitally signed. The Auditing Application can be used to ensure that the state of the system has not been modified.

Elaboration of Requirement OS 14.4

The Tenderer confirms that this requirement will be met. It will be possible to check the components of the Election System against their baseline and identify any changes. If the baseline itself is audited and the functionality approved, then it follows that the component being examined will act according to its specification.

6. Elaboration of External Interface Requirements

Elaboration of Requirement EIS4

The Tenderer confirms that the system will interface with a common authentication infrastructure, as detailed in Use Case 9.1 Authentication. As a minimum requirement, the common authentication infrastructure must support SAML 2.0. It should be noted though that if the solution has to fall back on the Altinn portal, the use of digital signatures will be impossible. The consequence of this would be that it wouldn't be possible to implement large parts of the voting protocol outlined in Appendix 3.

Elaboration of Requirement EIS5

The Tenderer advises the Principal not to interface with Altinn for the submission of list proposals. Interfacing with Altinn for the submission of list proposals would have the following consequences for the pilot project:

- Interfacing with Altinn would mean that another component would be involved in the Election System. This will result in a higher complexity of the solution, and therefore also a higher risk in the project.
- Interfacing with Altinn would also incur an extra cost in addition to the implementation cost of the list proposals functionality itself.
- The Principal would not be able to take advantage of the digital pen or ICR technology for the list proposal functionality, offered as an option to this tender.
- There may also be more issues involving data integrity and auditing if the list proposal functionality would deployed outside the realm of the Election System.

The Tenderer also wants to point out that using Altinn for list proposals would introduce an extra interface to the user. From a usability perspective, this should be avoided.

The Tenderer has not estimated the extra cost of interfacing with Altinn for the submission of list proposals.

Elaboration of Requirement EIS6

The Tenderer confirms that the system will be able to import structured information on count results from systems delivered to municipalities by other vendors. The interface will be the same as the one used internally between the P-voting Servers and the Election Settlement Server, and based on EML Message 460 (Votes) and/or EML Message 510 (Count). The connection must be secured using SSL.

Elaboration of Requirement EIH1

The Tenderer confirms that the e-Count scanning solution will interface with all industry standard scanners. As the solution aims to support the widest variety of commercial off-the-shelf (COTS) scanning hardware TWAIN is the preferred interface due to its higher levels of availability. However, the scanning module will be designed in such a way that the ISIS protocol can be supported if required.

Elaboration of Requirement EIH2

The Tenderer confirms that the system will interface with printer suppliers for the production of polling cards, voting cards etc. The Election Preparation module will map all data received into a common specified format to permit easy integration with the print suppliers selected for the election.

The production of a standard data specification irrespective of the originating format maximizes the flexibility for choosing print suppliers and permits a comprehensive testing process to be completed during the selection process.

7. Elaboration of Documentation Requirements

Elaboration of Requirement D2

The Tenderer confirms that technical documentation will be delivered according to Chapter 9 Documentation in the Systems Requirements Specifications document.

The delivery will include technical documentation covering:

- Architecture and design (both sketches and text) explaining the different modules
- Database schemes for the system

- Coding standard(s) used for programming the different modules
- HTML documentation of classes, methods and code (generated with javadoc) for all Java code
- Dedicated documents describing the algorithms, interfaces and APIs of the system

One of the subcontractors, Norconsult, will receive the task of creating guidelines that should be followed and implemented in order to produce all the necessary system documentation in order to meet the certification requirements the KRD plans to be done after the 2011 elections.

The Tenderer acknowledges that good system documentation must be well structured, have a high readability, both in wording, images and drawings, and, of course, be easy to update and maintain. The appropriate formats for the documentation will be selected according to the concrete purposes and audiences of the documentation parts. Formats that can be considered range from simple text files over documents, spreadsheets, diagrams and figures to hypertext, wikis and other media.

Special care should be given to the documentation describing how the core modules can be downloaded, compiled and deployed. The delivery will also include scripts to build the core modules on the most common operating systems i.e. Windows, Linux, MAC and UNIX.

Elaboration of Requirement D3

The Tenderer confirms that documentation for installation and operations will be delivered according to Chapter 9 Documentation in the Systems Requirements Specifications document.

The system will be thoroughly documented on how to:

- Install (and update) the system
- Configure the system
- Operate and maintain the system
- Advice on operational procedures for back-up, monitoring activities, etc.

The installation and operations documentation will include step-by-step guidelines and low level documentation covering different topics.

Elaboration of Requirement D4

The Tenderer confirms that user documentation will be delivered according to Chapter 9 Documentation in the Systems Requirements Specifications document. The delivery will include documentation that can be used for the education of expert users and will include:

- Functional overview (both sketches and text) for the complete system
- More detailed information about the functionality of each module and application
- User guide for administrative officers and key personnel

In addition, the system will be shipped with end-user help for each of the applications (front-ends). These help files will be published both in HTML and PDF. It will be possible to access the HTML help texts from within the applications.