

E-vote 2011 System Architecture eCounting of pVotes

V 1.0

“Source Code, High Level Architecture Documentation and Common Criteria Documentation Copyright (C) 2010-2011 and ownership belongs to The Norwegian Ministry of Local Government and Regional Development and EDB ErgoGroup 67 AS (“Licensor”)

The Norwegian Ministry of Local Government and Regional Development has the right to use, modify (whether by itself or by the use of contractors) and copy the software for the sole purposes of performing Norwegian Public Sector Elections, including to install and run the code on the necessary number of locations centrally and in any number of counties and municipalities, and to allow access to the solution from anywhere in the world by persons who have the right to participate in Norwegian national or local elections. This also applies to elections to the Longyearbyen Community Council at Svalbard and any possible future public elections in Norway arranged by the Election Authorities.

EDB Ergo Group 67 AS (or whom it appoints) has the right, inside and outside of Norway to use, copy, modify and enhance the materials, as well as a right of licensing and transfer, internally and externally, either by itself or with the assistance of a third party, as part of the further development and customization of its own standard solutions or delivered together with its own standard solutions.

The Norwegian Ministry of Local Government and Regional Development and EDB ErgoGroup AS hereby grant to you (any third party) the right to copy, modify, inspect, compile, debug and run the software for the sole purpose of testing, reviewing or evaluating the code or the system solely for non-commercial purposes. Any other use of the source code (or parts of it) for any other purpose (including but not limited to any commercial purposes) by any third party is subject to EDB ErgoGroup 67 AS’ prior written approval.”

E-vote 2011	Version: 1.1
eCounting of pVotes	Date: 26.05.2010

Change history

Date	Version	Description	Author
11.11.2010	0.1	Initial	
08.12.2010	1.0	Verified the document with the current solution	
25.05.2011	1.1	Added virtual environment	

E-vote 2011	Version: 1.1
eCounting of pVotes	Date: 26.05.2010

Contents

1. Electronic counting of paper votes (Scanning)	4
1.1 Architectural goal and scope	5
1.2 Essential use cases	5
1.3 Logical flow	6
1.4 Interfaces between subsystems	7
1.5 Process overview	7
1.6 Implementation overview	8
1.7 Virtual environment	9
1.8 VMware ESXi	10

E-vote 2011	Version: 1.1
eCounting of pVotes	Date: 26.05.2010

1. Electronic counting of paper votes (Scanning)

The eCounting of pVotes system facilitating the different tasks required for digitalizing paper ballots and producing text data from the images. The identified tasks are:

- Digitalize paper ballots and produce Tiff image files
- OCR the Tiff image files and extract relevant data
- Validate the text data in cases where the OCR is uncertain
- Summarize the validated data, and produce data representing the counts
- Electronically signing of data and transferring to the central election system

The eCounting of pVotes system (eCounting) consist of:

- four MS Windows applications
 - pVoteAdmin for administration, signing, and transfer
 - Scan for scanning and interpretation of paper ballots. Based on ReadSoft Scan.
 - Verify for manually verification of OCR text from tiff images of the ballots. Based on ReadSoft Verify.
 - Transfer for transferring the data from completely processed forms in the FORMS database to the pVote database. Based on ReadSoft Transfer.
- two databases:
 - pVote - a custom MS SQL database for managing election data
 - FORM - a standard MS SQL ReadSoft database for managing OCR scanned images of forms
- a shared file system
- a Internet connected workstation or server with access to the central election administrative system (Admin)

To log in to any of the system components (applications), the user must provide a valid token previously downloaded from Admin. Predefined user roles are created and users are restricted to perform actions specified in the token.

As part of the installation process, a set of ballot templates provided by KRD will be used to configure the underlying ReadSoft software. Before use of the eCounting of pVote system, the election configuration will be downloaded from the Admin system. The signed configuration files will be read by pVoteAdmin on startup.

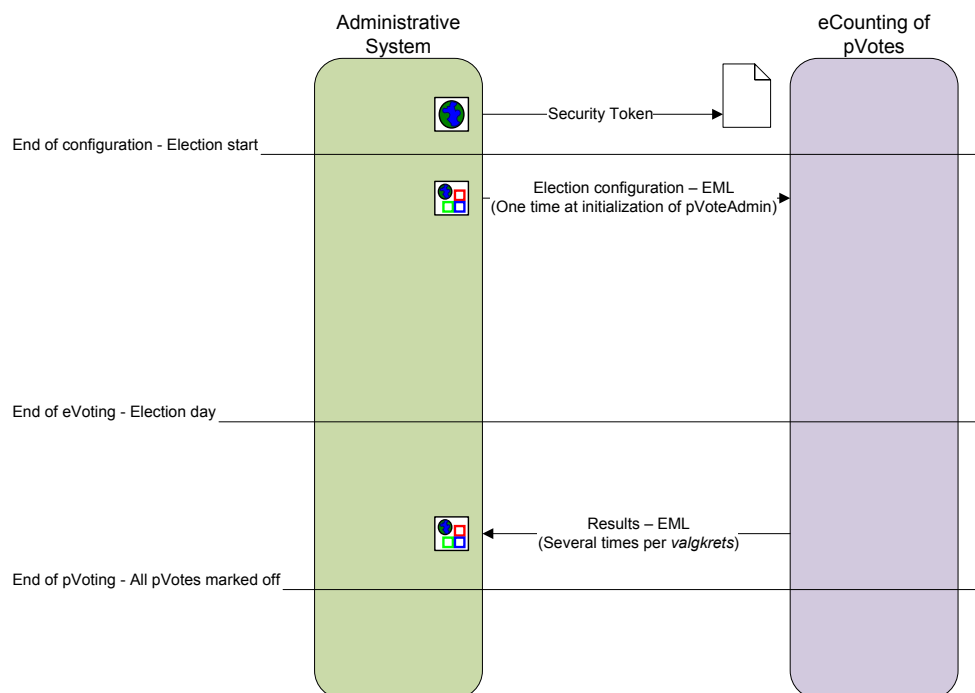


Figure 1 DFD eCounting of pVotes context level view

E-vote 2011	Version: 1.1
eCounting of pVotes	Date: 26.05.2010

1.1 Architectural goal and scope

The system is built around the following conditions:

- Ballot papers are distributed and sent to location (Municipality, County etc) for counting.
- Software is configured at each location initially.
- Database Configuration like Location name, unique Number etc.
- Scanner Configuration which is compatible with ReadSoft Software.
- Software has to be configured based on Ballot papers list which to be scanned processed which are distributed for each location.
- Counting
- Draft Counting
- Scanning
- Final Counting
- Scanning
- Verification of results from earlier phases of counting (scanning)
- The Output after verification is to transfer the results from database to EML format.

The design is given by the restrictions and design of the ReadSoft application programming interface. The ReadSoft software consists of modules which we attach our programming using DLLs. This is commercial software developed in Microsoft .Net. The system is to a large degree built around extensions to this software as follows:

- Management functions such as database maintenance and export of logs
- Scanning
- Read barcodes
- Handling unrecognized ballots
- Handle exceptions such as scanner missing paper, connectivity failure, etc.
- Verification of scanned data
- Ballot handling (discard, approve, search, duplicate elimination)
- Transfer of counts to administrative system (EML)

1.2 Essential use cases

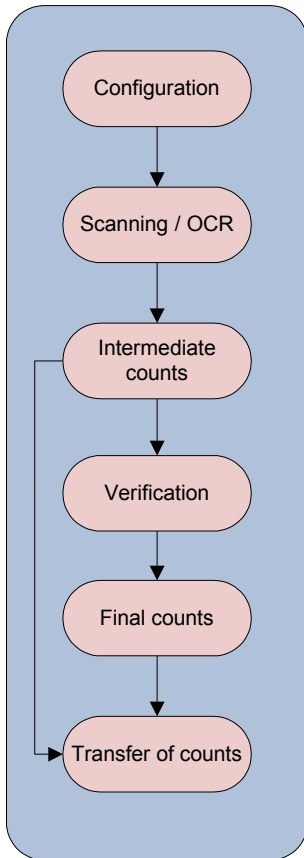
Use Case 3.3 Electronic counting of p-votes

- Select election
- Scan ballots
- Read ballots
- Store results
- Present results
- Verify results

Parts of the use case is handled by the administrative system:

- Interface to upload counts in EML
- Comparison and approval of results

1.3 Logical flow



Configuration

EML election configuration is imported and the system is configured. In addition, ReadSoft configuration is performed

Scanning

Scanning of ballots is performed by feeding ballots into a scanner connected to a work station. The software will store the images and perform OCR

Intermediate counts

Counts are produced based on the OCR interpretation of the votes
When scanning is completed an intermediate count is produced and can be transferred

Verification

Verification of ballots and changes/discarding of ballots is performed to generate the final data

Final counts

Final counts are based on verified data and is prepared for transfer

Transfer of counts

EML with counts is produced, signed and transferred

1.4 Interfaces between subsystems

The eCounting of pVotes system has interfaces to the central election administration system.

Receive from administrative system:

- Encrypted and signed security token downloaded from a web interface¹
- Election configuration and language translations in EML through a web service

Publish to administrative system:

- Counts of votes in EML through a web service¹

Byypass smartcard will be used to personally sign the count EML files before they are transferred to the Central Administrative System.

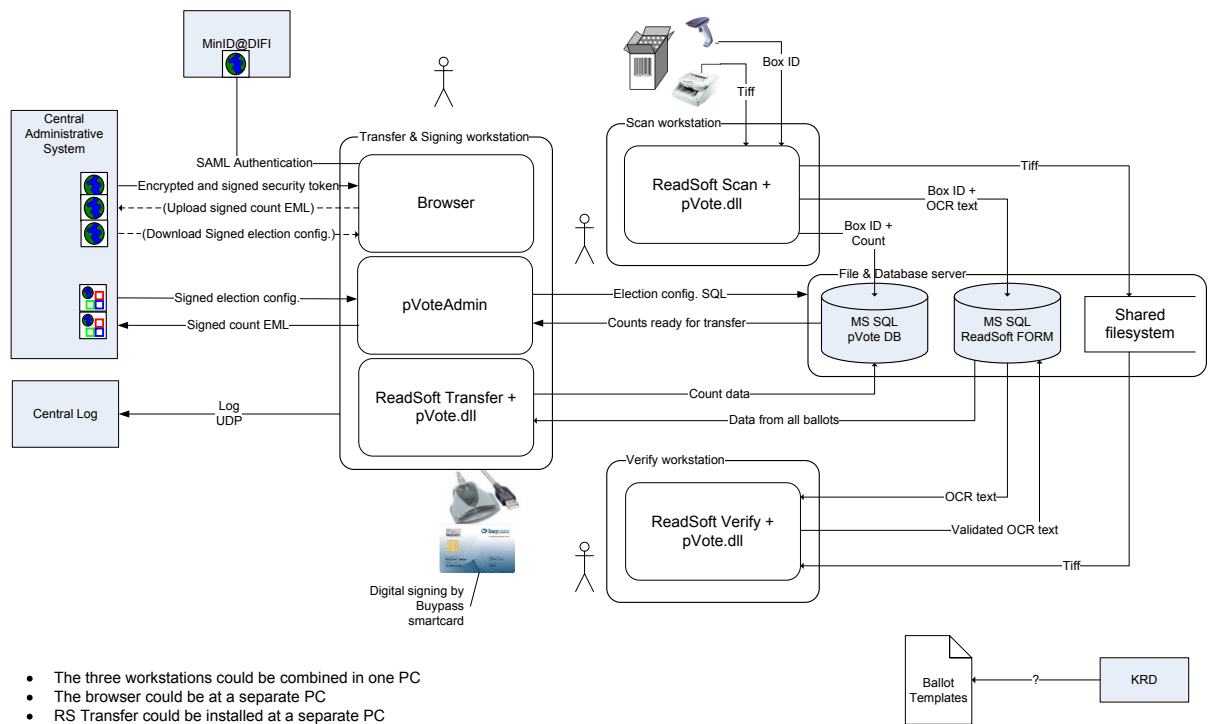


Figure 2 DFD eCounting of pVotes High level view

How the paper ballot templates will be distributed from KRD, and how (and when) will they be used in by ReadSoft Manager to configure the ReadSoft software, has to be decided.

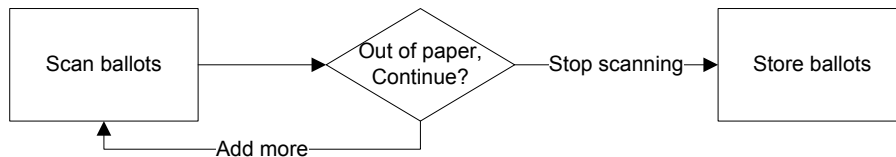
1.5 Process overview

Scanning

During scanning of ballots from a new ballot box, the system requests data from a bar code reader. The bar code contains information regarding municipality, location and ballot box number.

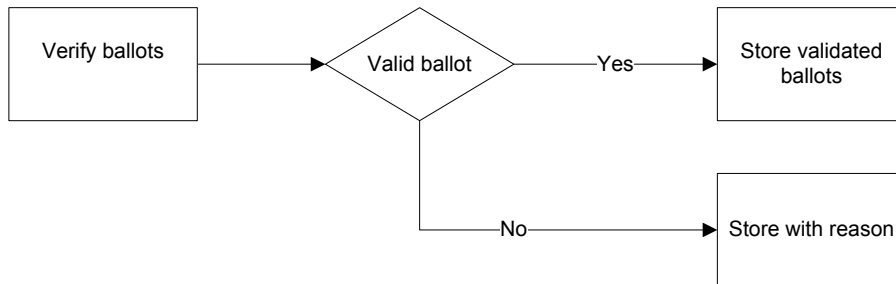
When the scanner runs out of paper, the user adds more paper from the ballot box, or if the box is empty, ends the scanning process by selecting stop on the screen. The ballots are stored automatically.

¹ One requirement is that the eCounting system must be able to function without external network connectivity during the Election Day. As a consequence the system must be able to export the personally digitally signed counts to files which manually could be uploaded by a web interface to Admin from a separate workstation with external network connectivity. For the same reason, there exists a web interface for manual download of the signed configuration files.



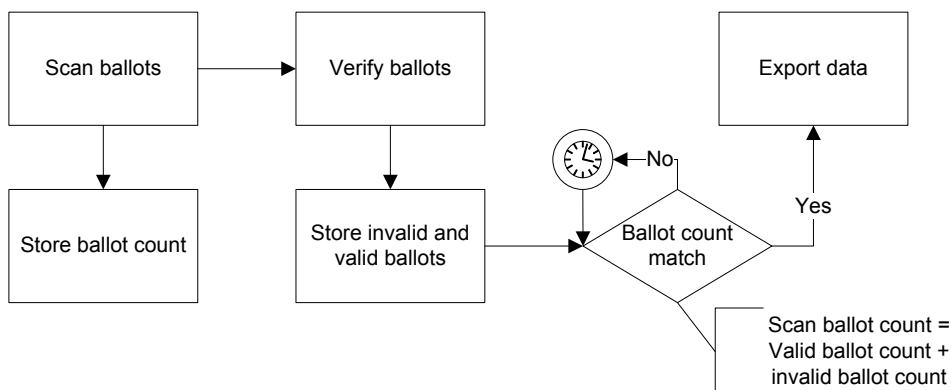
Verification

Ballots are validated by entering uncertain numbers and markings. A special workflow or queue handles the ballots that are considered invalid as regards to election legislation or unrecognized by the system. In this queue the user can discard ballots with a reason or approve ballots if the ballot is considered valid.



Export of data

Whether or not a ballot box is ready for export is decided by comparing the number of ballots scanned, and the number of valid and invalid ballots. When the counts match, the ballot box is ready for export. The data needs to be signed by a validated user before the data is transferred to the central election system.



1.6 Implementation overview

The High Level Application Design follows a standard 3 layer set up:

- Presentation Layer (UI Framework) Layer.
- Business Logic Layer.
- Data Layer.

The ReadSoft -software is designed to digitize any kind of form data, extracting the text and markings using OCR and export of the data to a specified format.

To facilitate the extraction of data from election ballots a programmed plug-in called pVote has been developed. In addition to the plug-in, form definitions have been defined in ReadSoft to specify to the system what data needs to be extracted from the images.

The software is utilizing the 3-layer design as follows:

- **GUI-tier** handles dialog boxes and election specific windows.
- **Business logic-tier** handles election specific logic like checking the validity of numbers and marks, facilitating searching for candidates and rejecting invalid ballots.

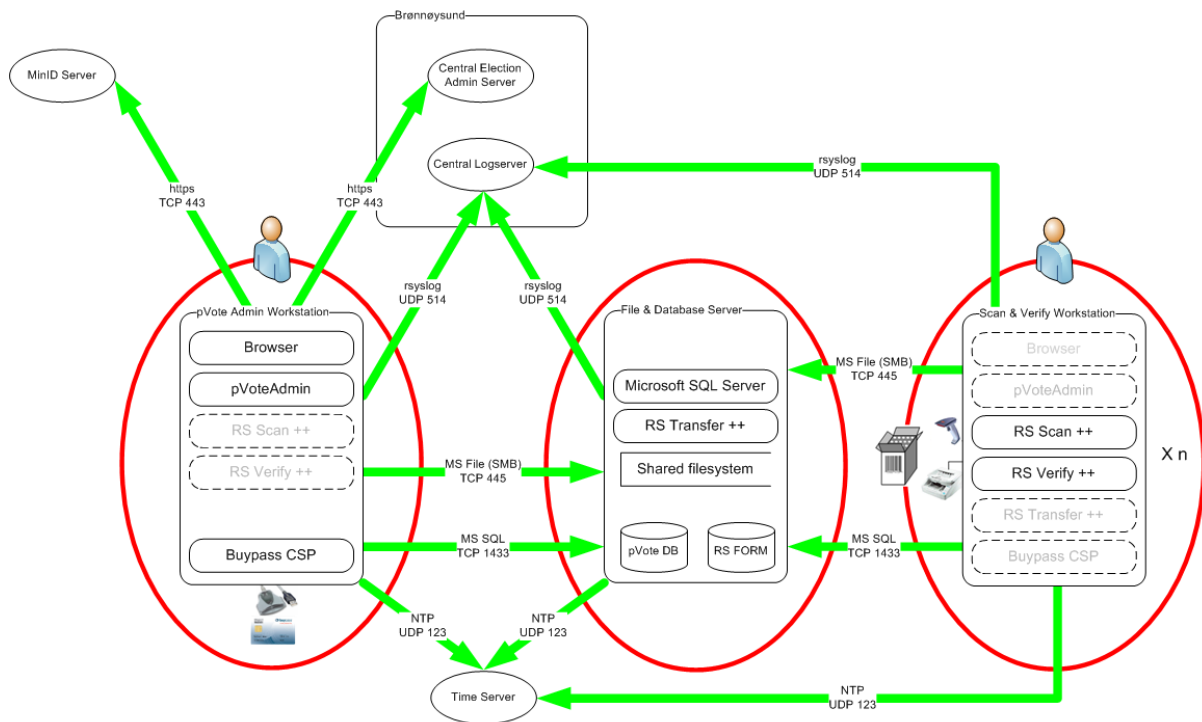
- **Data access-tier** handles communication with the database. All database specific functions are implemented in this tier, except queries and reading of connection strings, which are handled in the Business logic-tier.

The ReadSoft software is considered to be the host application and the pVote-plugin is the hosted application. The ReadSoft company has included this capability to enable third-party developers to extend the functionality of the standard product.

The developed modules are described in the design document for the subsystem.

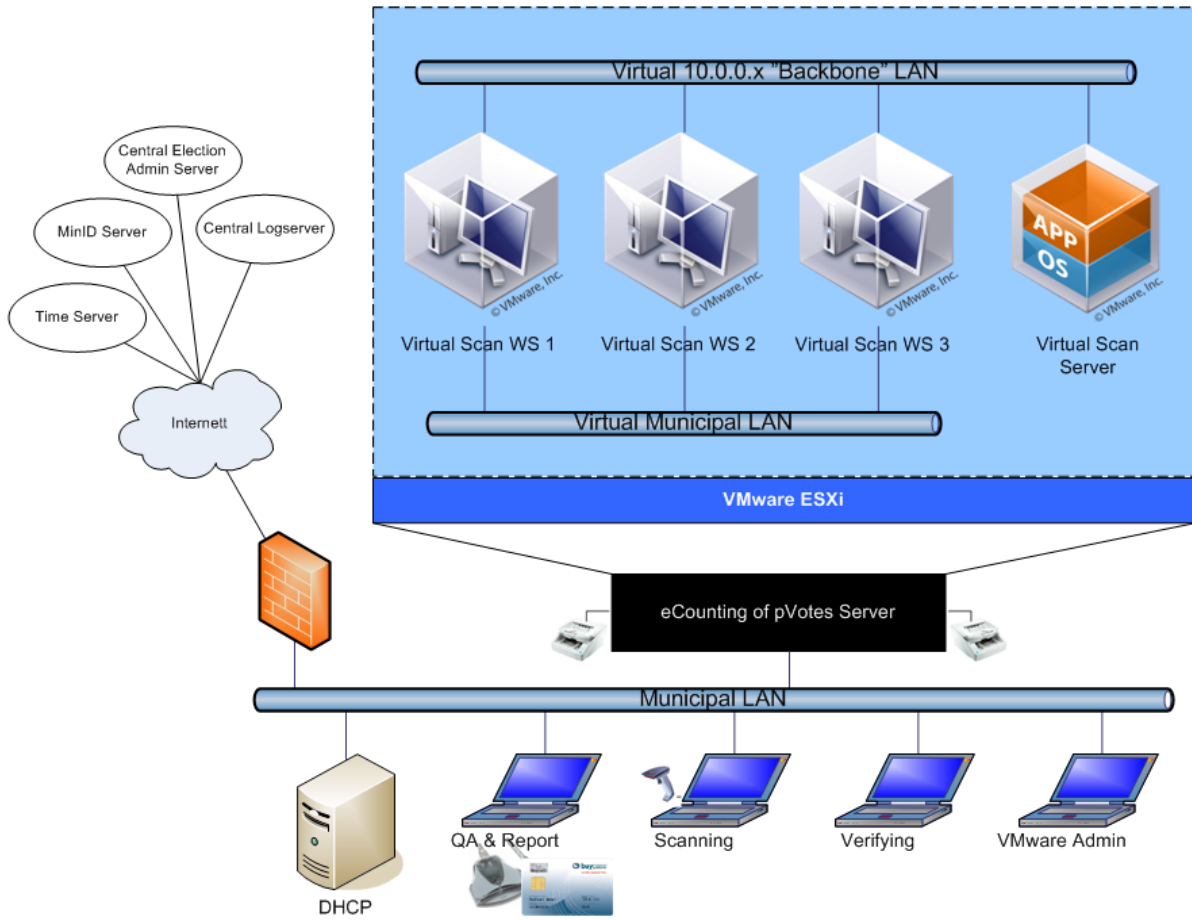
1.7 Virtual environment

To simplify the management of the eCounting environment, the system is delivered as a virtual server environment.



1.8 VMware ESXi

The counting environment is built around a local server in the counting center, running VMware ESXi.



The virtual machines are connected in its own private virtual network with access to the local virtual file- and database server. The virtual server can only be access from the virtual work stations. In addition, there is a small Active Directory instance for user management. In addition, any application that is started requires a security token, retrieved from the central administrative election system.

Scanners are physically connected to the local server, while scanners are connected to the virtual work stations. Counted results are signed by use of a Buypass smart card. One of the virtual servers have outward access to transfer counting results to the Central Administrative system through SSL with certificates.

The system logs all events and forwards this information to a central audit repository, in addition to local logs.