ErgoGroup

E-vote 2011
Security Architecture
Electronic counting of paper votes
V 1.1

Change history

Date	Version	Description	Author
26.11.2010	0.1	Initial	
15.12.2010	0.5	First draft version for review	
20.01.2011	1.0	First complete version	
11.03.2011	1.1	Some minor updates.	

Contents

1. Introduction 4

2. Conceptual design 4

2.1 Security domains and interfaces 4
2.2 User profile and description 5
2.3 Authentication 5
2.4 Access control 6
2.5 Key Security Scenarios 6

3. Logical design 7

3.1 Application architecture 7

4. Physical design 7

4.1 Desktop environment and local network environment 8
4.2 Wide area networking environment 8
4.3 Solution topology 8

5. Self-protection in eCounting 10

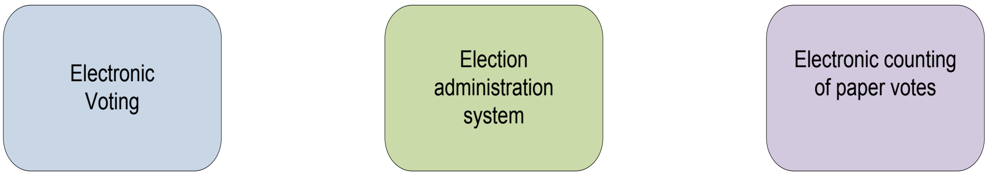
6. Domain isolation in eCounting 10

7. Non-bypassibility of security functionality in eCounting 10

1. Introduction

This document presents the security architecture of the election systems which is part of the E-vote 2011 project. By *security architecture*, we mean the conceptual, logical, and physical design which is used to protect the systems and the information they protect from compromise.

The E-Vote 2011solution consists of three different but interacting systems:


Electronic Voting
Election administration system
Electronic counting of paper votes

Each system can operate in its own environment, but require interaction to satisfy common requirements such as configuration, authentication/authorization, logging and reporting. The overall security architecture is described in the document “Security Architecture - General Overview”.

To support counting of paper ballots, the system for electronic counting of paper votes is installed in municipal counting centres (estimated 150 centres). It contains modules for scanning and verifying ballots, in addition to local administrative functions.

2. Conceptual design

Conceptual Design is the view of the security solution *from the user point of view*. It seeks to define the characteristics of information access and authentication that are part of the user experience.

2.1 Security domains and interfaces

The Paper Voting Domain includes two separate security domain as illustrated below.

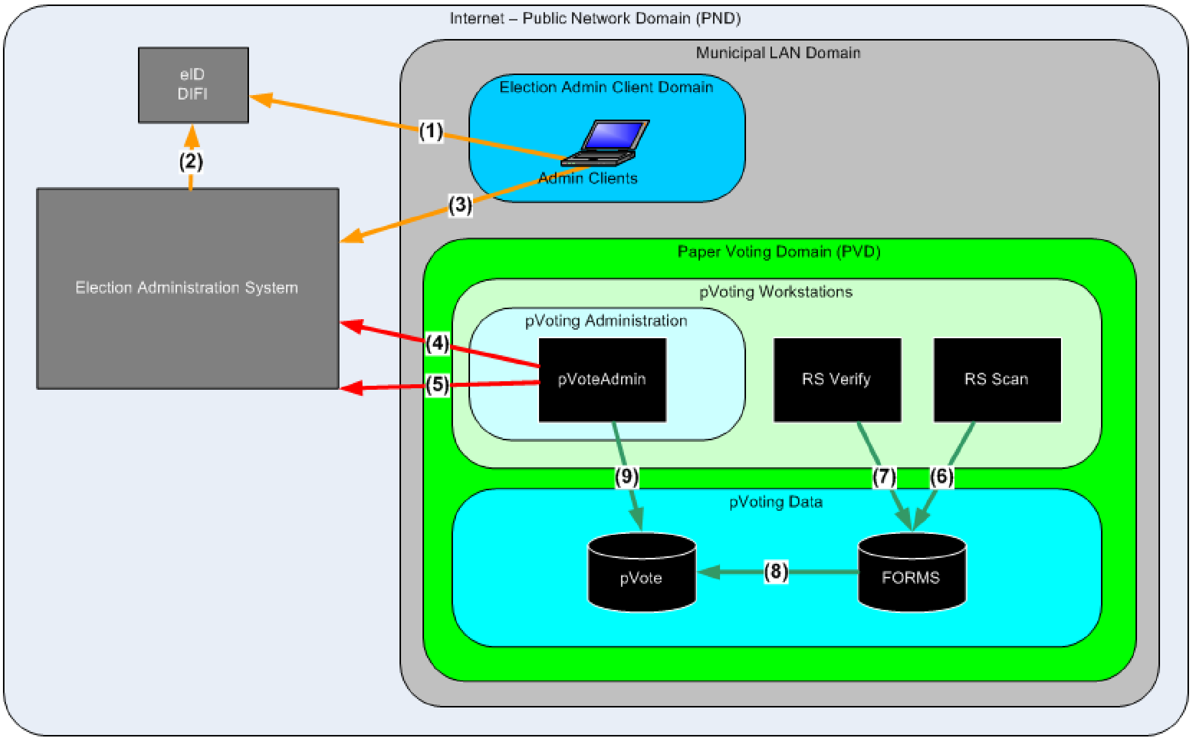


Figure 1: Paper Voting Domain

- The **pVoting Workstations** domain includes workstations for the three different functions in the eCounting of pVotes system; Administration, Scanning, and Verification
- The **pVoting Administration** domain contains the workstation for Administration of the eCounting of pVotes system. The system in this domain is the only one of the systems in the paper voting domain which needs external connection. Before use of any of the pVoting applications, the user has to download a 'security token' from the Central Election Administration System. The PC running the Admin client could be the same PC running the pVoteAdmin.
- The **pVoting Data domain** contains two databases and a file system shared between the pVoting applications at one site.

The interfaces to the system and between the subsystems are (numbered in the figure above):

1. User authentication. Web interface over HTTPS. Possible redirected from election service.
2. Verify user authentication. Web service over mutual authenticated connection.
3. Web interface for election administration over mutual authenticated HTTPS connection. When logged on the Admin system, the user could download the *security token* which is needed to use the pVoting applications.
4. **Get election configuration** in EML (XML) format over a mutual authenticated HTTPS connection. The configuration EML files are digitally signed by the Election Administration system.
5. **Send ballot count results** in EML (XML) format over a mutual authenticated HTTPS connection. The counting EML files are digitally signed by an election official using her Buypass smart card while she is logged on in the pVoteAdmin application.
6. Internal database connection from the RS Scan application.
7. Internal database connection from the RS Verify application.
8. Transfer of ready verified scanned ballots from the RS FORMS database to the pVote database. The process is performed by the RS Transfer service.
9. Internal database connection from the pVoteAdmin application.
10. **Send audit - and system logs to the central log database** from all pVoting systems through rsyslog service (UDP/514).The audit log data is immutabilized before it is sent.

2.2 User profile and description

There are a three user roles defined in the central election administration system (Admin) which are used by the pVote applications. New users must be created in Admin. The assigned user role is checked when the different pVote applications are started. Only user with the right user role will be allowed to use these applications.

User role	General use
Scanneadministrator	User in pVoting domain. User of pVoteAdmin and RS Manager.
Scanneoperatør	User in pVoting domain. User of RS Scan.
Scanningkontrollør / Verifiserer	User in pVoting domain. User of RS Verify.

2.3 Authentication

The authentication for the pVoting domain is *indirectly* based on ID-porten as described in the document "Security Architecture - General Overview".

Operators in the pVoting a domain must log on to the Admin system and download a security token file before they can use their application. The token file contains the user-id, assigned role, and expiration time. The token is signed by the Admin application private key. When users chose to download their token, they have to pick a personal password. The Admin system uses the given password to generate a symmetric key which is used to encrypt the token file.

When the token is presented to a pVote application, the user has to input her password again. The pVote applications use the same algorithm to generate a symmetric key which is used to decrypt the file.

The pVote applications check:

- the user provided password correctly decrypt the token file to prove the file is not stolen
- the digital signature of the Admin application to prove the user was properly authenticated and none of the information in the token has been tampered with since it was generated
- the expiration time to prove the token is still valid

2.4 Access control

The pVote applications only check the user role when they start. The applications are limited and specialised. If a user is allowed to run an application, she could use all functionality provided by the application.

Each pVote application has its own database user with limited permissions

.

2.5 Key Security Scenarios

Here is a description of some key security scenarios.

2.5.1 Configuration

Election configuration is imported from the central election administration system (Admin) over a mutual authenticated HTTPS connection. The operator, using the application pVoteAdmin, selects an available election event and downloads the latest version of the configuration files. The pVoteAdmin application uses the appended digital signature to check the authenticity and integrity of the files before the operator chose to configure the system.

2.5.2 Verification of ballot scan

After scanning of the ballots, a special workflow handles the queue of 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. The operator's decisions are recorded in the audit log and the scan image of the ballot in question will later be transferred together with the counting results.

2.5.3 Signing and transfer of counting results

After all ballots from one election district is scanned and verified, the counting data is transferred from the ReadSoft FORMS to the pVote database and the counting result is marked as ready for reporting. 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.The operator, using the application pVoteAdmin, selects the results she want to report, digitally signs it, and upload it over a mutual authenticated HTTPS connection to the central election administration system (Admin).

Buypass smartcard will be used to personally sign the count EML files before they are transferred to Admin. When the user in pVoteAdmin chose to sign, she will be prompted for her PIN by the Buypass software.

2.5.4 Audit log

There are two kinds of logs collected from the electronic counting of paper votes system:

- Application logs will registering important events for application monitoring
- Infrastructure logs will register logs for every security event in the servers and infrastructure components

The application events "*Application start/stop*" and "*User login/access control*" are logged from all pVote applications. In addition the following application specific events are logged:

Application	Event
pVoteAdmin	*Configuration verification*: When the election configuration is selected, downloaded from Admin, and verified against the digital signature.
pVoteAdmin	*System configuration*: When the downloaded election configuration is used to configure the electronic counting of paper votes system.
pVoteAdmin	*Send count result*: When the ballot count is approved, signed, and uploaded to the central election administration system.

RS Manager	*Scan configuration*: When the ReadSoft Manager application is used to configure the ReadSoft FORMS database and the ReadSoft part of the scanning system.
RS Scan	*Election district begins/ends*: When the scanning of one election district (consisting of potential several ballot boxes) begins/ends.
RS Scan	*Ballot box begins/ends*: When the scanning of one ballot box begins/ends.
RS Verify	*Ballot accept/reject*: When the operator process one ballot from the queue of questionable ballots and approve or discard it with a reason.

All logs are stored locally and copied to the central log system through the RSYSLOG protocol.

All the logs are protected through the “Immutable Logs” mechanism, which is ensuring the integrity of the log information. Application logs are generated in a secure way (immutabilized) locally by the “immutabilizator module” when the log files are processed by the RSYSLOG protocol. While infrastructure system logs are stored in standard form locally and immutabilized centrally after they are transferred.

3. Logical design

Logical Design is the view of the security solution *from the design team’s point of view*. It seeks to define as far as possible technology-neutral design which meets the needs of the users.

3.1 Application architecture

The electronic counting of paper votes system (eCounting) consists of five rich client applications working together on two shared databases. Four of the applications; Manager, Scan, Verify, and Transfer, are build on the corresponding applications from ReadSoft. All the ReadSoft applications work on the ReadSoft FORMS database. The Transfer application transfer ready verified scanned ballots from FORMS to the pVoting database. The pVoteAdmin application works on the pVote database.

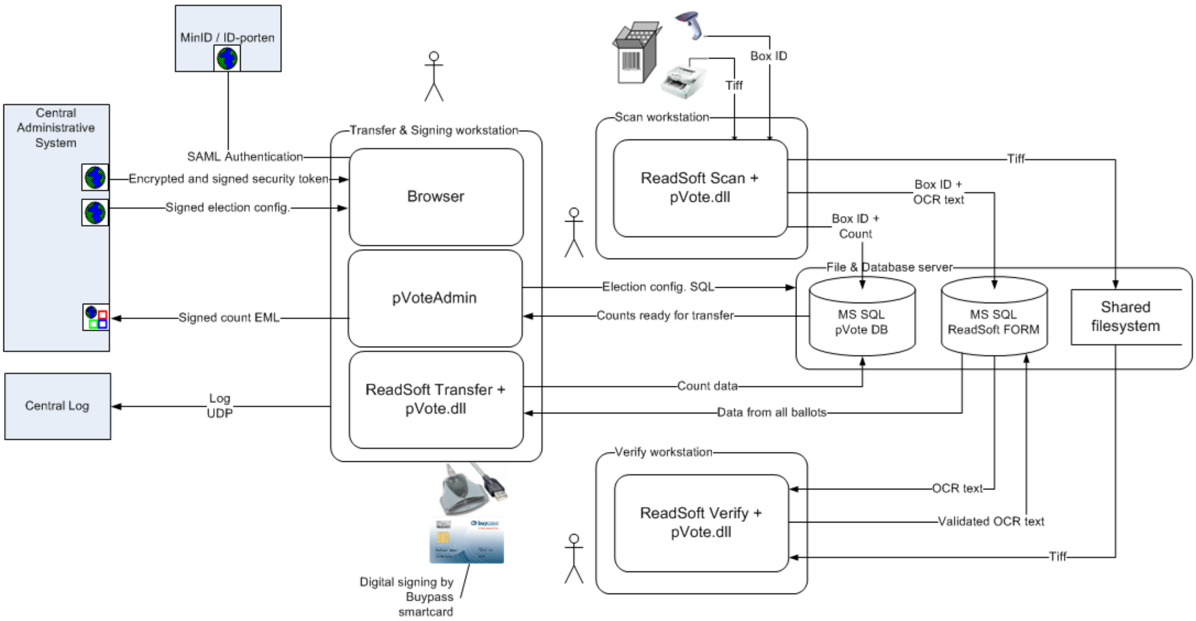


Figure 2: Electronic counting of paper votes - Logical design

4. Physical design

Physical Design is the view of the security solution from the developer’s point of view. It seeks to define the configuration of the physical components used to implement the technology solution and to provide a process for operation and support of the system.

4.1 Desktop environment and local network environment

The PCs used to run the pVote applications at the scanning site are under municipal administration and - security policy.

The PCs running pVoteAdmin have a connected smartcard reader and have installed a Buypass Crypto Service Provider to perform digitally signing with a Buypass smartcard.

The PCs running the Scan application have a connected bar code reader and a paper ballot scanner.

4.2 Wide area networking environment

The PCs running the pVoteAdmin application and the PCs used to log on to the central election administration (Admin) web application need https connection to the Admin system. All the machines in the Paper Voting Domain need rsyslog connection to the central log collector and NTP connection to a reliable time source.

No services in the Paper Voting Domain should be available from the outside.

4.3 Solution topology

The electronic counting of paper votes system (eCounting) is deployed at several counting centres all over Norway during the election.

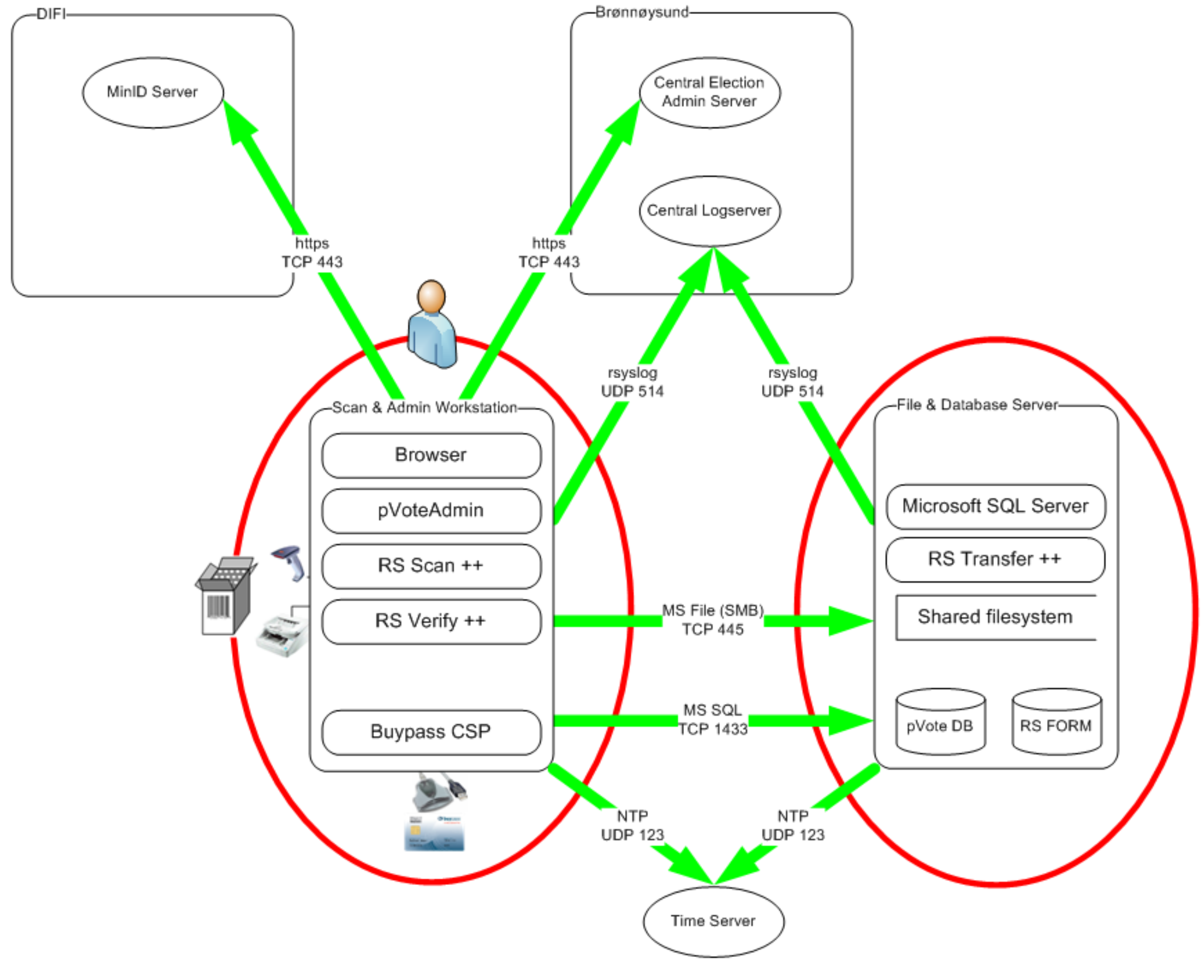


Figure 3: Operational environment for eCounting

Some of the larger counting centres need more than one scanning workstation. These sites distribute the different applications as follows.

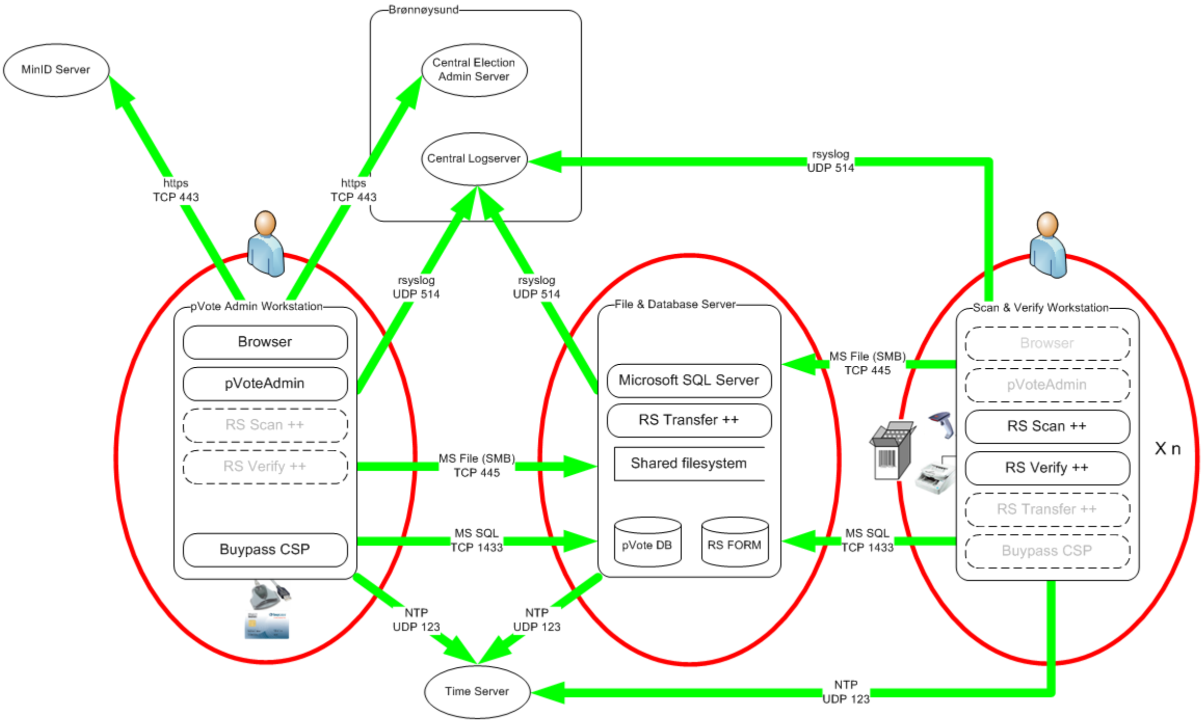


Figure 4: Operational environment for eCounting - Larger installations

It has been some discussion on how these environments should be configured and delivered all over the country in a secure and effective way. The delivering project has suggested developing a virtualized solution on one server with VMware ESXi. This is described in the document “Driftsmiljø for scanning av stemmesedler”.

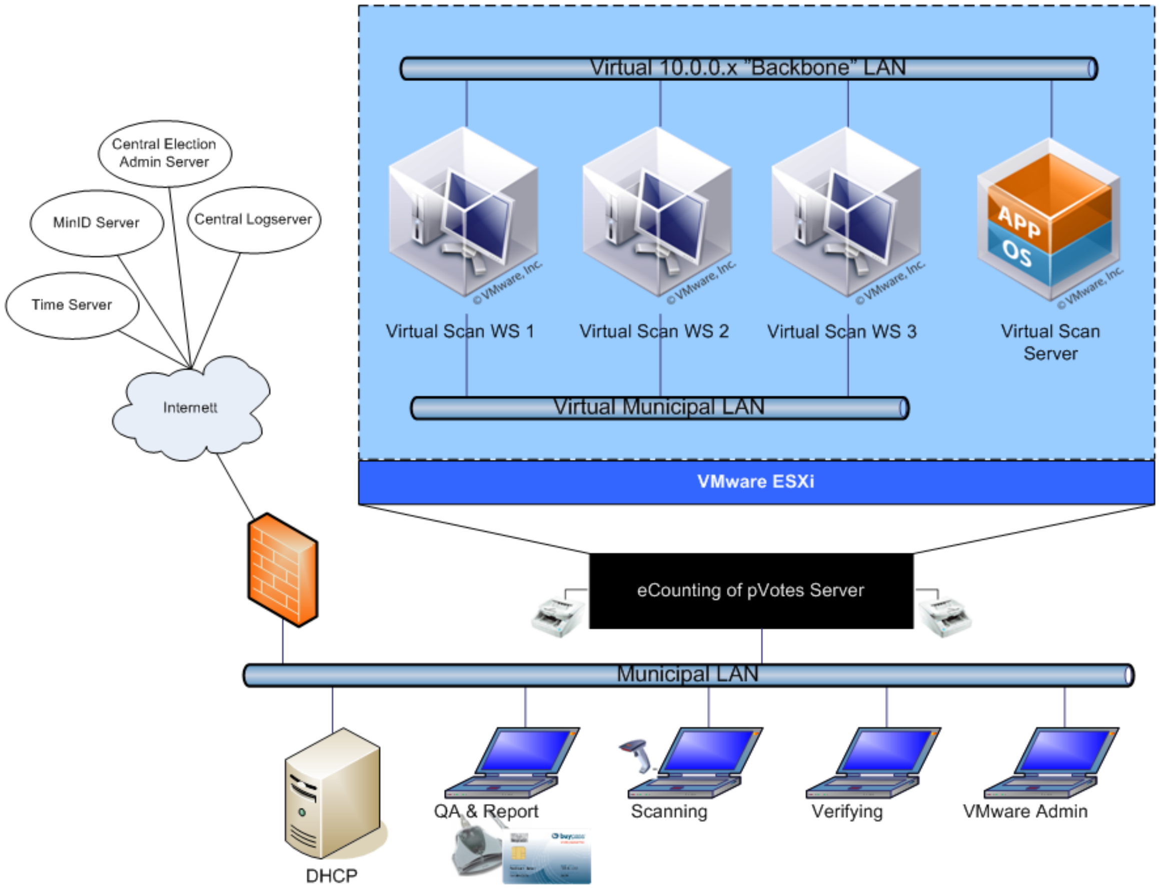


Figure 5: Production environment for eCounting virtualized

5. Self-protection in eCounting

This section sum up how the eCounting system protects itself from interference and tampering.

Only predefined authenticated users get access to the user interface of the system.

Possible threats against the security of the system are assessed and security controls are implemented as counter-measures. This threat model process is documented in the Redmine issue tracking system. Some of the security controls are mention below with reference to the corresponding issue number in Redmine.

To ensure that only system administrators could modify important parts of the system, the required security token contains the user identity and role (#3734) and the RBAC system restrict access to administrative functions (#3729).

All actions on behalf of a user in the eCounting applications require successfully identification and authentication of that user. To ensure this, all users are uniquely identified by their social security number (#3735) and all eCounting applications require a security token containing the user identity and role to be present. The eCounting systems are installed in an environment with some physical security (#2863).

Important events in the system are recorded in an audit log (#3728) which is secured from tampering (#2873). The systems use NTP (#3733) to enable correlation of the logs.

6. Domain isolation in eCounting

This section sum up how the security domains maintained by the eCounting system.

The Paper Voting Domain includes two separate security domain; the pVoting Workstations domain includes workstations for the three different functions and the pVoting Data domain contains two databases and a file system shared between the pVoting applications at one site.

The separation between the domains is implemented by separate VLANs and local firewalls on each (virtual) machine. The local firewalls on each machine restrict the connections to the necessary traffic.

7. Non-bypassibility of security functionality in eCounting

This section sum up how the eCounting system prevents bypass of the security functionality. The protection mechanisms should always be invoked to prevent that the applications can be used to access protected data or resources in an unauthorised way.

Several security controls are in place to ensure that the security functionality of the eCounting system could not be bypassed.

To ensure that the restriction on administrative functions could not be bypassed by attacking the clients, the eCounting workstations are hardened and have screen lock configured (#2856).

To ensure that the restriction on administrative functions could not be bypassed by malicious system administrators, direct system access in the production environment is restricted to a few people (#2863).

To ensure that the restriction on administrative functions could not be bypassed by malicious non-administrative users and voters, SQL injection attacks are prevented (#2869).