ErgoGroup

E-vote 2011
Security Architecture
General Overview
V 1.1

Change history

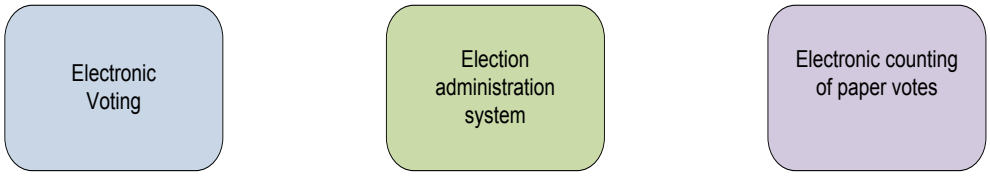
Date	Version	Description	Author
18.11.2010	0.1	Initial	
07.12.2010	0.5	Complete version for review	
03.03.2011	1.0	Minor updates after revview	
11.03.2011	1.1	QA	

Contents

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:



Each system can operate in its own environment, but require interaction to satisfy common requirements for configuration, authentication, reporting, auditing, and key management. The security architecture documentation is divided in one document for each of these systems.

Definitions:

E-vote 2011	The project
E-voting client	Subsystem for casting votes electronically
E-voting system (eVoting)	The subsystem handling eVoting. (Includes E-voting client, backend functions for storing votes, and functions for tallying votes i.e. counting of eVotes).
Election administration system (Admin)	Subsystem for configuring and managing elections
List proposals	Part of the Admin system
Electoral Roll	Part of the Admin system
Election configuration	Part of the Admin system
Counting registration	Part of the Admin system
Settlement	Part of the Admin system
eCounting of pVotes system (Scanning)	Subsystem for counting of paper ballots
Reporting	Horizontal reporting functionality
Log & Audit	Horizontal log and audit functionality

2. Overall 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 Main security domains and the interfaces between them

The security objectives for the election solution describe the security domains to be secured. The three election systems are contained in different security domains as illustrated below.

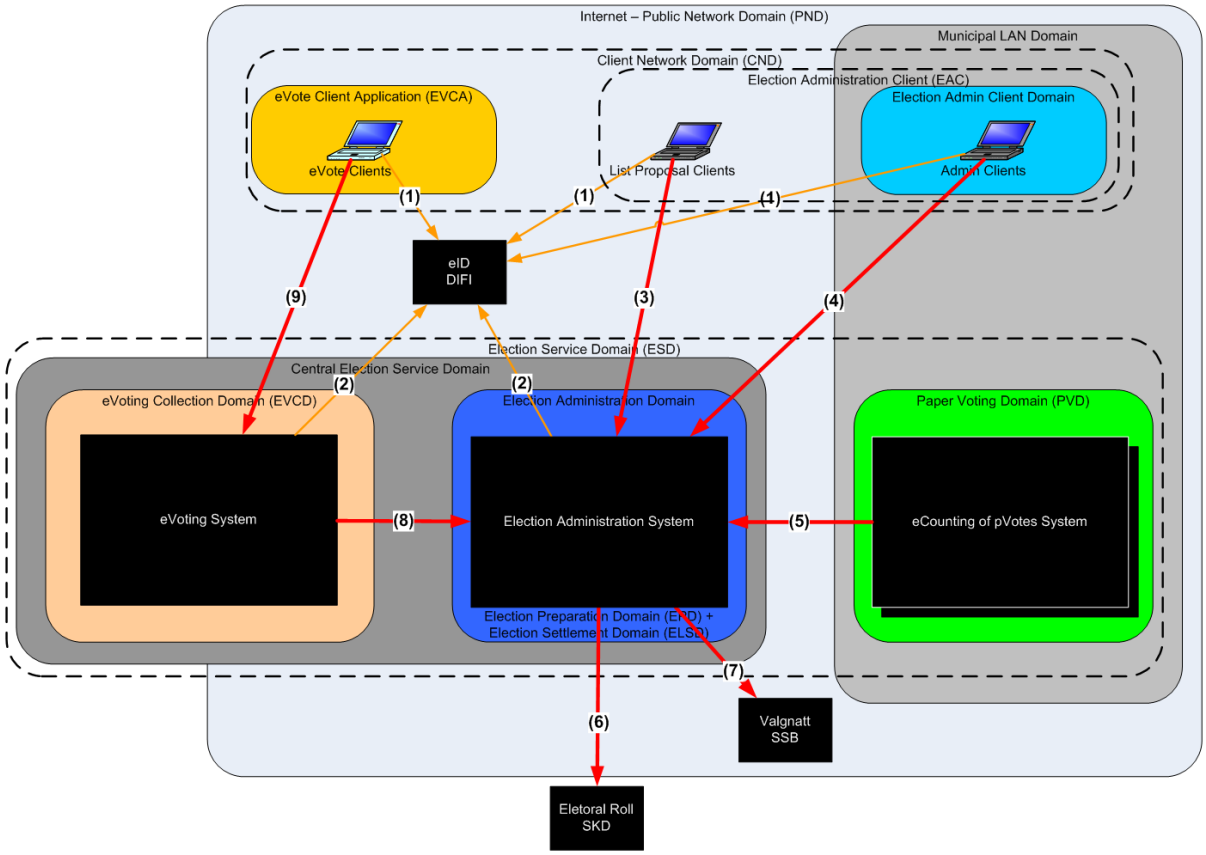


Figure 1: The Election Domain (ED)

- **Election Domain (ED)** contains all the Election and Voting Services that are necessary to prepare and complete an election.
- **Internet - Public Network Domain (PND)** contains that part of the communications infrastructure which is not under the control of the Election Service operators and clients.
- The **Central Election Service Domain** contains that part of the communications and processing infrastructure which will be under the Government's control. It is used to host the election preparation services, the e-voting collection services, as well as the election settlement services. The original tender defines an *Election Service Domain (ESD)* which also included the Paper Voting Domain under municipal control.
- The **Election Administration Domain** contains all the services required to prepare an election (called the *Election Preparation Domain (EPD)* in the original tender) and the election settlement processes (called the *Election Settlement Domain (ELSD)* in the original tender). Election preparation provides abilities both for paper-voting and for electronic voting. In Settlement, the results of both paper-votes and e-votes are merged into the final election results, seats are distributed and the election results are computed for publication. This domain is part of the *Central Election Service Domain* and is described in detail in a separate document [Ref. "Security Architecture - Election Administration System"].
- The **Paper Voting Domain (PVD)** contains all systems to scan, verify, and count paper ballots. This domain is part of the *Municipal LAN Domain* and is described in detail in a separate document [Ref. "Security Architecture - Electronic counting of paper votes"].
- The **e-Voting Collection Domain (EVCD)** contains the IT infrastructure to host the electronic ballot

collection process. The EVCD are physically separate from the EPD and ELSD to facilitate the anonymity of the ballot. This domain is part of the *Central Election Service Domain* and is described in detail in a separate document [Ref. "Security Architecture - Electronic Voting"].

- The original tender defines the *Client Network Domain (CND)* as that element of the infrastructure under client control, which is used to support access to the Election Service. As part of CND the *Election Administration Client (EAC)* was defined to contain clients for election preparation and administration. As the solution does not contain any mechanism to implement any common client domains, these terms are purely conceptual and included just as a reference.
- The **Election Administration Client Domain** contains the clients used for election preparation and administration. The **List Proposals Clients** are client used by party representatives to access the public part of election administration. Both kinds of clients are described in detail together with the election administration system.
- **E-Voting Client Application (EVCA)** is that element of the client network that is supplied by the election service and used to access the public E-voting services in EVCD. The e-voting client is described in detail together with the rest of the e-voting system.

The required interactions between the systems are done through the following interfaces (numbered in the figure above):

1. **User authentication**. Web interface over HTTPS. Possible redirected from election service. Described in the section "Authentication in general" below.
2. **Verify user authentication**. Web service over mutual authenticated connection. Described in the section "Authentication in general" below.
3. **Public web interface for list proposals** over HTTPS. Described together with the election administration system.
4. **Web interface for election administration** over mutual authenticated HTTPS connection. Described together with the election administration system.
5. **Interfaces for the Paper Voting Domain**. The following interfaces is used:
    a. 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.
    b. Deliver ballot count results in EML (XML) format over a mutual authenticated HTTPS connection. The counting EML files are digitally signed by the responsible system operator at the scanning site.
    c. Deliver copy of local log events through rsyslog service (UDP/514). The audit log data is immutabilized before it is sent.
6. **Get initially load and daily updates of the electoral roll** from Skattedirektoratet (SKD).
7. **Send preliminary and final reports of election result**s to Statistisk Sentralbyrå (SSB).
8. **Interfaces for the eVoting Collection Domain**. The following interfaces is used:
    a. Get election configuration in EML (XML) format from a mutual authenticated HTTPS connection. The configuration EML files are digitally signed by the Election Administration system.
    b. Deliver eVoting count results in EML (XML) format over a mutual authenticated HTTPS connection. The counting EML files from eVoting are digitally signed by the Counting module.
    c. Deliver copy of local log events through the same rsyslog service as 5c (UDP/514). The audit log data is immutabilized before it is sent.
    d. Check if a voter is eligible to cast a vote in an election with a web service over a mutual authenticated HTTPS connection.
    e. Get a record based file for the whole electoral roll with mark-offs from a web service over a mutual authenticated HTTPS connection. The electoral roll copy is used to check the final electronic ballots and to filter out all voters which have cast a paper vote from the final electronic count.
9. **Public web interface for electronic voting** over HTTPS. Described together with the electronic voting system.

More detailed information on the interfaces could be found in System Architecture documents [Ref. "System Architecture - Interfaces].

2.2 Main user groups

The three systems have several different user groups which are described in more detail under each. The main user groups are:

1. **Election administrators/officials** setup, configures, and administers elections before, during, and after the election. The tasks are done in a web application from client PCs which are under municipal control and have a special purpose SSL client certificate installed.
2. **Political party officials** use a public web application to send in list proposals with candidates for the different parties before the election.
3. **Eligible voters** cast their electronic vote in a public web application. Only eligible voters in the election roll could cast their vote.
4. **Operators in pVoting** scan paper ballots, verify them, count them, and report the results with PC applications installed in municipal local network at counting centrals.
5. **Operators in eVoting** setup and configure the election and report the counting results from the electronic voting.

2.3 Authentication in general

The national personal identification number ("fødselsnummer" in Norwegian) is used as user identification in all applications.

Users of the Admin (including public list proposal) and eVoting web applications authenticate themselves through the national electronic ID service ("MinID" at "ID-porten"). This is in principle a single-sign-on system for many government services, but the configuration does not allow single-sign on towards the election systems.

Operators in the pVoting and eVoting domains authenticate themselves with a token file generated and down-loaded from the Admin web application. The token includes user identification and permissions (user role). The token is digitally signed by the Admin system and encrypted with a key generated from a user provided pass-word.

Call to web services are authenticated (only by the infrastructure) based on the calling IP address and provided SSL client certificate.

Authentication with ID-porten adheres to the SAML version 2.0 (SAMLv2) standard. SAML is the "Security Assertion Markup Language", and defines standards for exchanging information about identity and authentication state within a Circle of Trust.

SAMLv2 includes the concepts of single sign-on (SSO) and single log-out (SLO). SLO implies that logging out of a single service provider will log the user out of all service providers in the Circle of Trust on which they have sessions.

The SAMLv2 specification supports a "service provider first" approach, in which the user first attempts to access the service provides resource. ID-porten uses this approach for Single Sign On.

Following is a description of how the Admin and eVoting web applications redirects a user to ID-porten so she can authenticate there, and then come authenticated back:

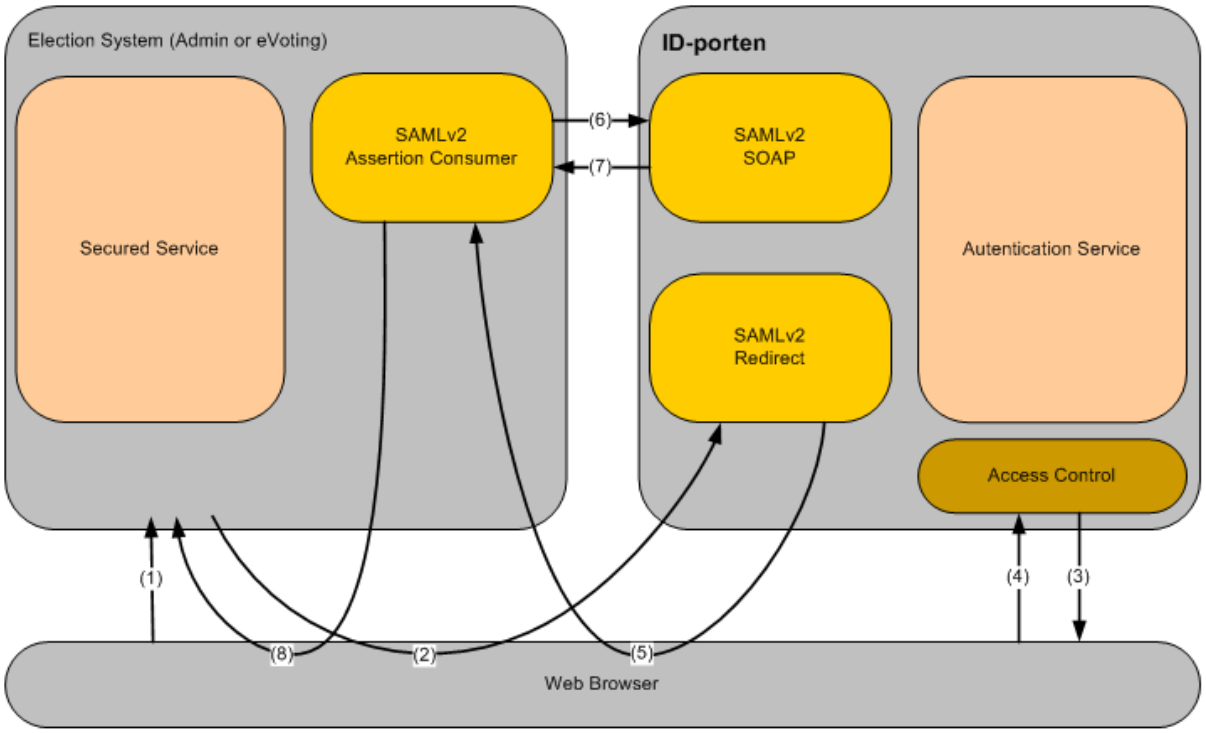


Figure 2: Authentication process with ID-porten

The steps involved are as follows:

1. The user tries to access the election web site via the browser
2. The user gets redirected to ID-porten since she doesn't have a session with the election web site
3. ID-porten asks the user to authenticate
4. The user authenticates with MinID by entering her credential (Social security number, PIN, and password)
5. The authenticated user returns to the election web site with a SAMLv2 artifact
6. The election system enclose the artifact in a SOAP request directly to ID-porten
7. ID-porten responds to the SOAP request with the assertion document the artifact refers to, and which contains information about the user
8. The election system establish a user session based on the information received about the user and gives access to the site the user tried to reach in step 1.

If the user already has an active session in ID-porten, as a result of a recent authentication, the user goes directly from step 2 to step 5 (step 3 and 4 is not necessary). This gives Single Sign On. More detailed description of ID-porten could be found in implementation guides from Difi.

2.4 Authorisation and access control in general

Only predefined users could log on to the Admin web application. Users and user roles are defined in the Admin system. Users with special roles (e.g. "Systemansvarlig" and "Valghendelseansvarlig") have permission to create, edit, and delete roles and users in the Admin web application. Access to pages, entities, and tasks in the Admin application is secured by a role based access control (RBAC) system. A more detailed description of the RBAC system could be found in the "Security Architecture - Election Administration System" document.

When political party officials want to submit a list proposal, they need a user created for them. Only users in the role "Listeforslagsstiller" have access to functionality in the public list proposal web application.

Web services in the Admin system access other services as a user belonging to the user role "Web Service".

In the application for electronic voting, users are not created up front in the system. Everyone with MinID could log on to the application, but only eligible voters in the election roll could cast their vote.

It is not defined any local users in the eCounting of pVotes domain. Operators on these systems need to log on to the Admin web application to generate and download a security token file which must be present when starting a pVoting application. The token state which permissions (role) the user has. Only users with the right permissions are allowed to start the different applications.

3. Overall 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 architecture of each of the three systems is described in more detail in separate documents.

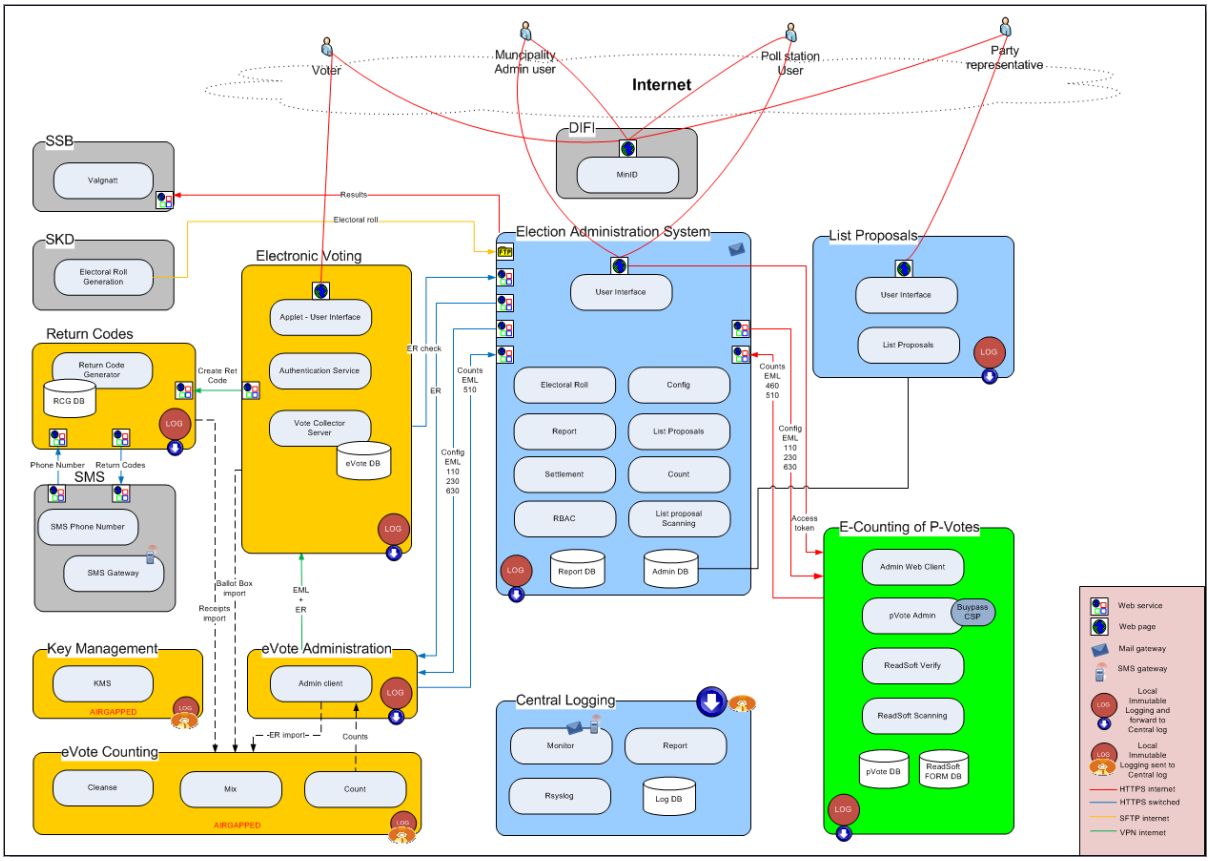


Figure 3: Overall logical design

3.2 Logging, auditing, and monitoring

Logs are collected in all three systems locally and a copy is sent to a central log and audit system. Logs are collected from both application events and infrastructure events. To prevent tampering with the log data, the log files are "immutabilized" by continuously appending hashes (HMAC) of previous log entries. Application logs are immutabilized locally before they are sent to the central system. Standard infrastructure logs are immutabilized in the central system.

Below is an overview of the log and audit solution. Details about which events get logged are in separate documents for each system.

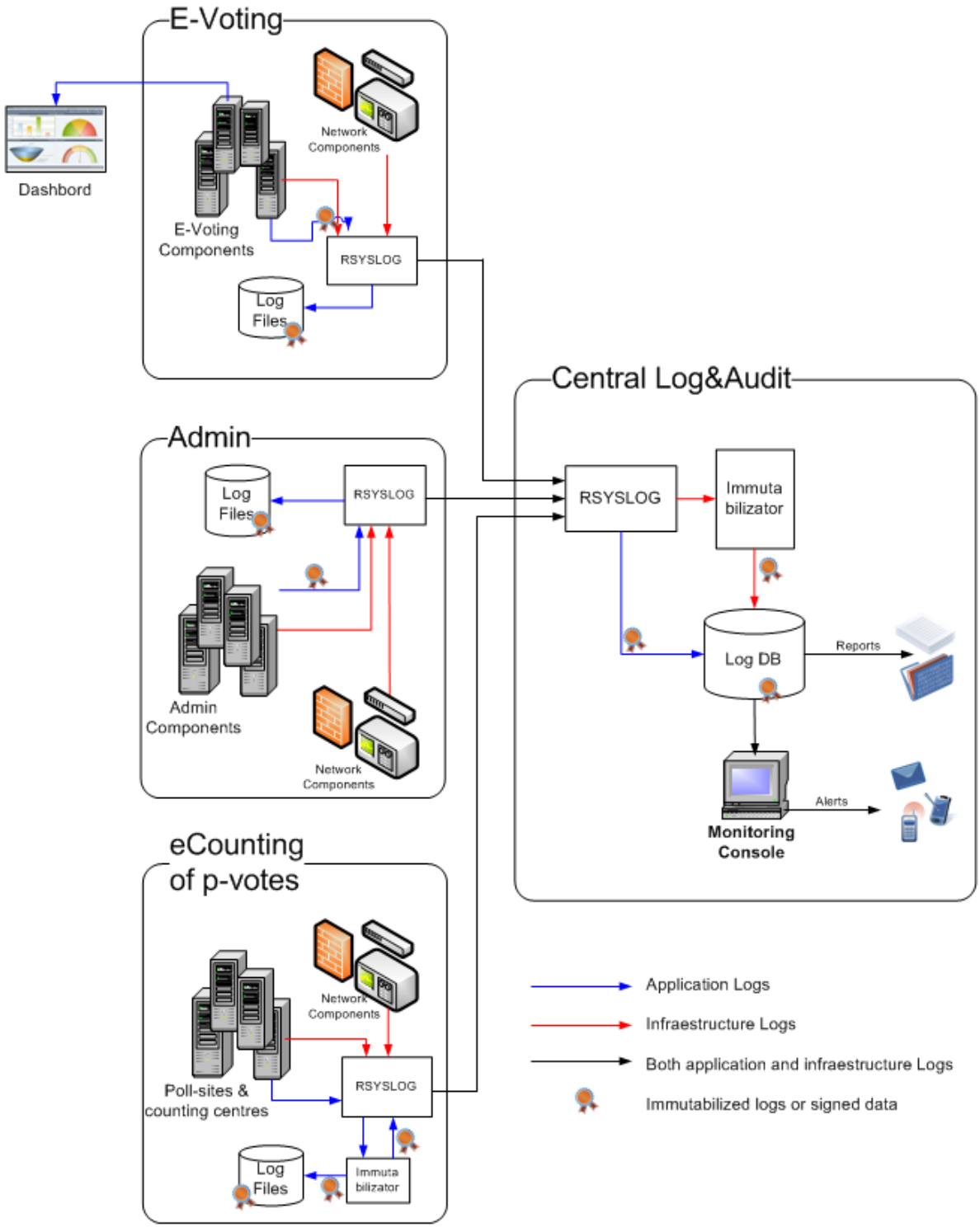


Figure 4: Log and audit - Logical design

4. Overall 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

We have no influence on the clients used by the electronic voters and political parties' representatives. They could use any supported web browser on any platform.

The municipal Admin client, the poll station client, and the Admin client at the scanning site are under municipal administration and - security policy. To access the Admin system, the user needs a standard web browser and an installed SSL client certificate.

Each system for electronic counting of paper votes consists of one file - and database server, three desktop Windows applications, a smart card reader, and at least one ballot scanner. The systems will be installed temporary in municipal LANs during elections. The installations will be run under municipal administration and - security policy.

4.2 Local area network environment

The systems for electronic voting and election administration are deployed at Brønnøysund service provider. The two systems are run in separate environments.

The systems for electronic counting of paper votes are deployed at several municipal LANs with Internet connection.

4.3 Wide area networking environment

The web applications for electronic voting and election administration are accessed from Internet. SSL server certificate are installed for each system and all connection is by HTTPS. All Admin clients (except for list proposals) have installed SSL client certificates. All connections from these clients are by mutual authenticated HTTPS.

4.4 Network components

The internet facing web servers are protected by firewalls. The firewall rules accept only HTTP traffic to these servers. Traffic to election administration system (except public list proposal) is only allowed from municipal owned IP addresses.

The firewalls also accept log traffic from the E-voting environment and systems for E-counting of p-votes down to the central log servers.

Log events from the systems for E-counting of p-votes are sent over Internet (default port 514).

A load balancer is also deployed in front of the internet facing web servers. The Admin system (except public list proposals) is deployed in parallel servers for higher availability. The E-voting system is deployed in parallel servers for higher availability and load sharing.

Firewalls or other filtering devices are also deployed between the E-voting and Admin system, and between front end and backend of these systems.

4.5 Solution topology

The central part of the E-voting and Admin is deployed in two data centres at Brønnøysund. The system needed for handling the return codes for E-voting are deployed in two data centres at Directorate for Civil Protection and Emergency Planning (DSB). The offline (airgapped) systems used for cleansing and mixing of E-votes are placed in KRD’s own data centres.

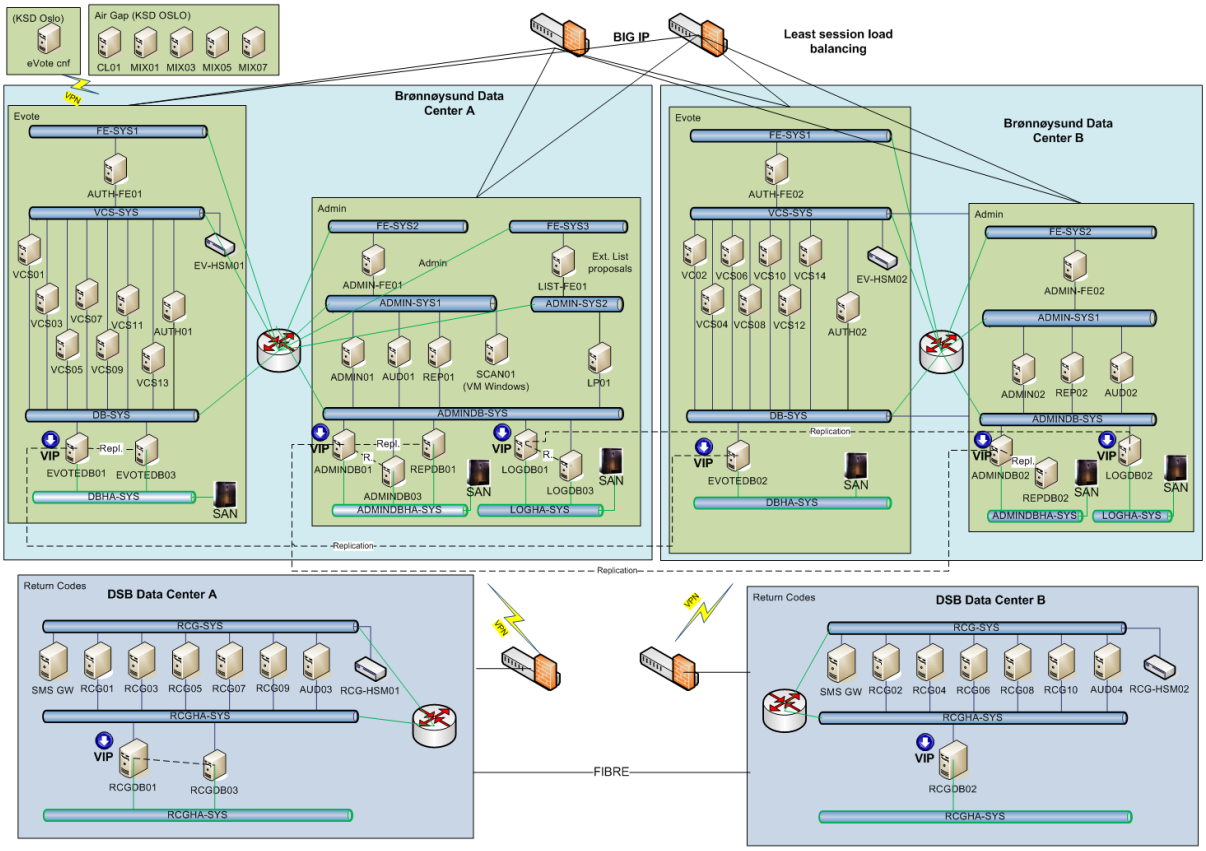


Figure 5: Operational environment