White paper
Swiss Post e-voting Infrastructure Explained

November 2016

Post CH Ltd
Use only for private, non-commercial audit purposes

Contents

1. Introduction

1.1 Purpose of the document

Swiss Post believes that transparency is vital in order to gain the confidence of the voters and cantons when it comes to electronic voting. This document describes the e-voting infrastructure with all implemented security aspects.

2. E-voting software

The core e-voting software used at Swiss Post was developed by Scytl in Barcelona in cooperation with Swiss Post. The second-generation voting protocol uses the features of individual verifiability and is end-to-end encrypted. More detailed information on the software can be found in the white paper "Swiss Post Online Voting Protocol Explained".

The software itself already fulfils strict security requirements and is completely encrypted, from vote casting through to analysis. The infrastructure is designed to be catastrophe-proof and can reliably prevent unauthorized internal and external access.

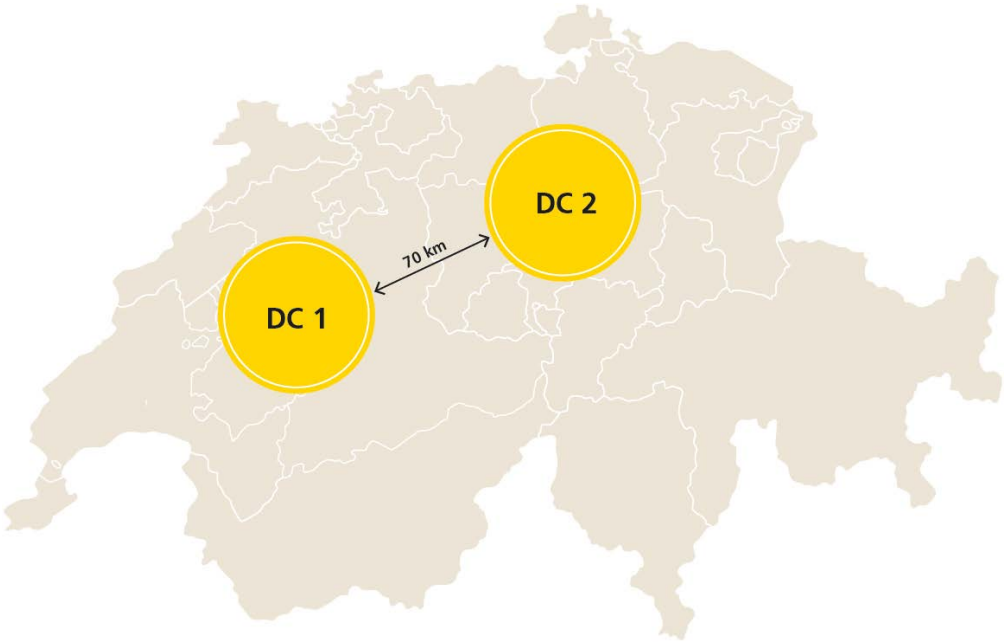
3. IT infrastructure

3.1 Data centers & BCM

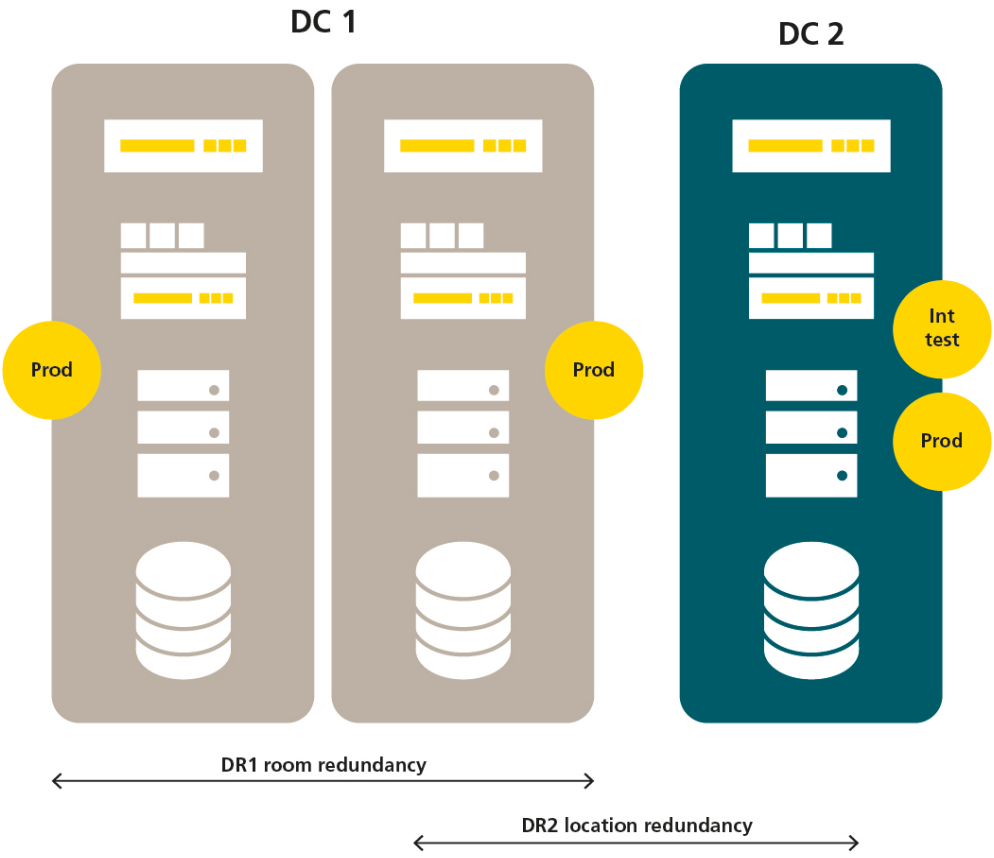
Swiss Post has two geographically separated data centers. Our data centers are distinguished by the following features:

Features

- FINMA-compliant, TÜV Dual Site Level 3-certified
- The operator is ISO 27001 and ISO 22301-certified
- Full redundancies for critical supply systems
- No single point of failure
- Strongly authenticated access control
- Uninterruptible power supply



All e-voting systems are situated in both data centers to provide geo-redundancy. If the primary data center fails, the other data center takes over the services. In addition to geo-redundancy, room redundancy is also guaranteed within a data center. This guarantees business continuity.

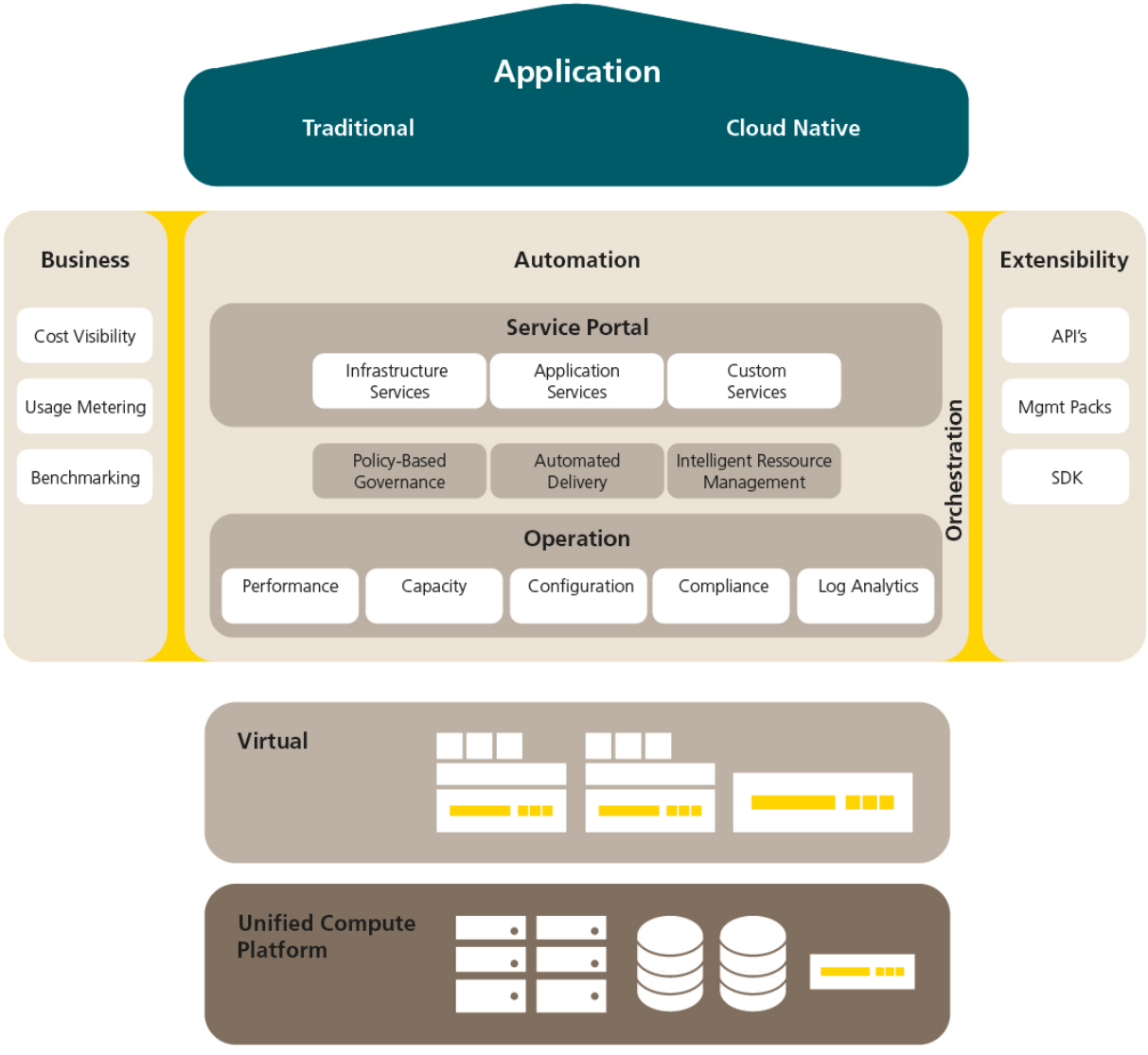


3.2 Application infrastructure

3.2.1 E-voting SDDC

Swiss Post's e-voting service is completely virtualized (apart from the reverse proxy and database infrastructure). The virtualization platform mirrors the Swiss Post software-defined data center (SDDC).

The system comprises a computer, network and storage infrastructure, all of which is included in a box (data center in a box). Such systems can be set up and expanded on a modular basis.

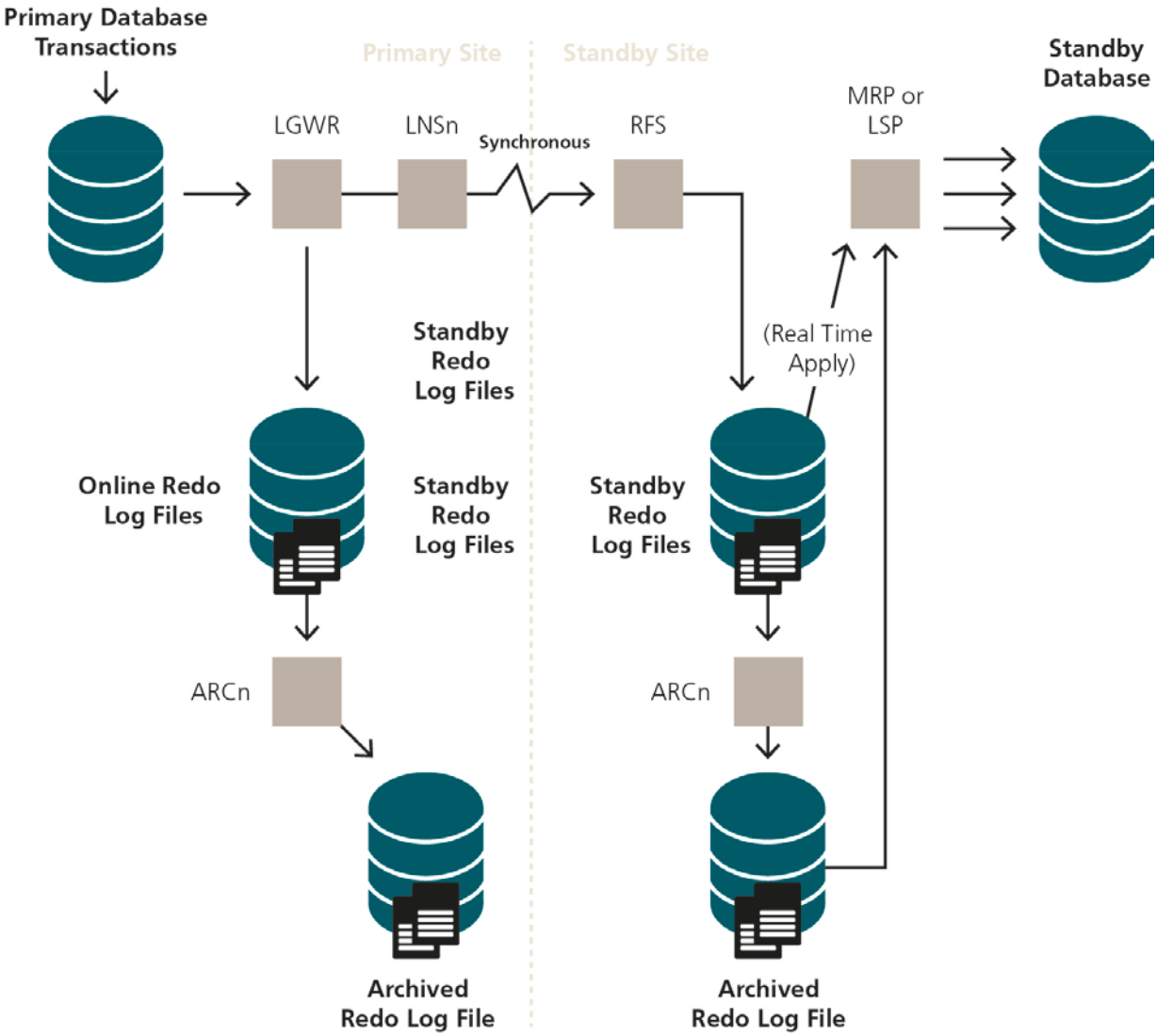


3.3 Database infrastructure

The e-voting database infrastructure comprises three productive and two integrative dedicated systems.

3.3.1 Triple mirroring and zero data loss

The ballot box, which is encrypted and signed, is located in the database. Data must always be consistent and may at no time be lost. Data is therefore triple-mirrored (saved synchronously three times).

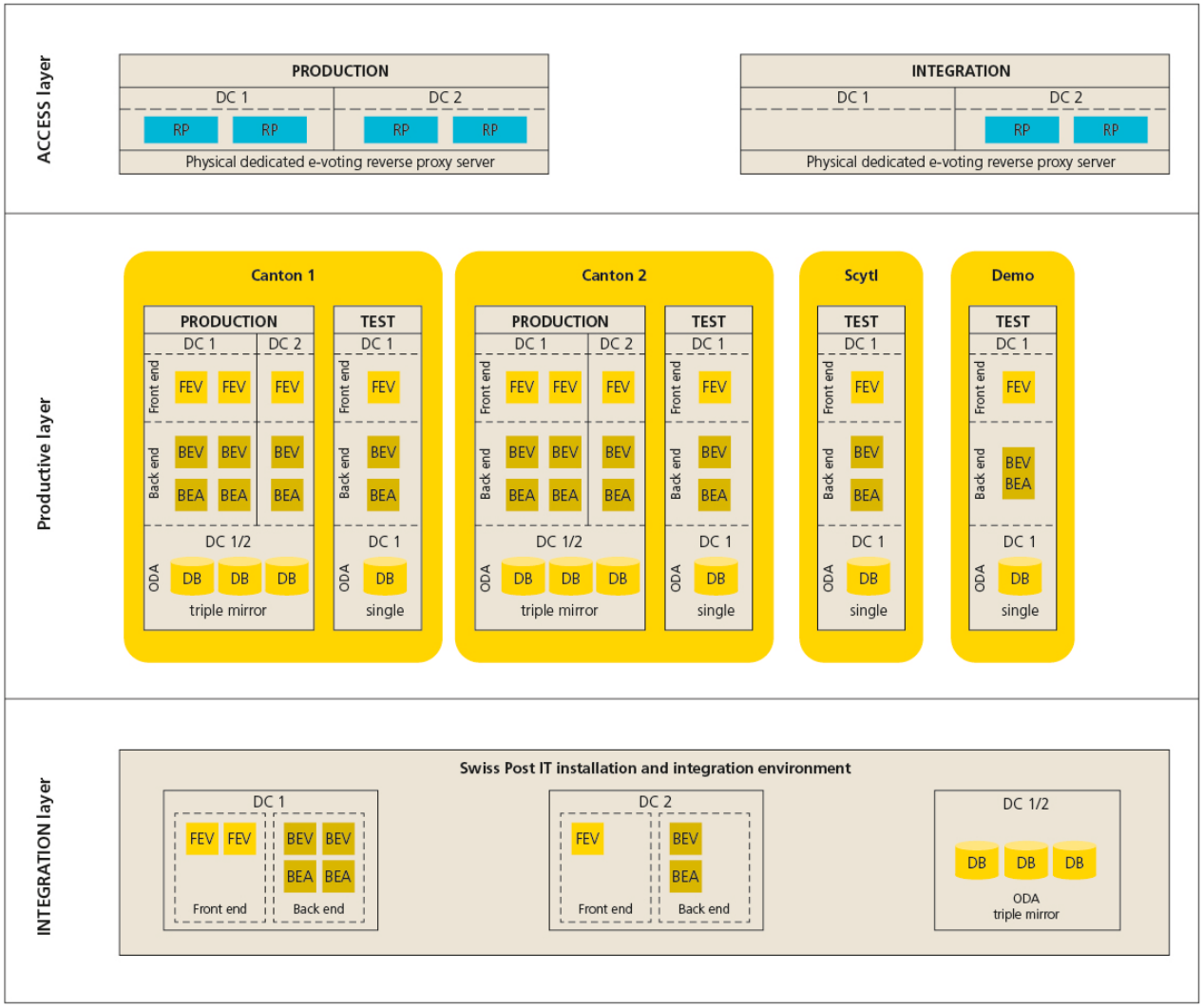


3.4 E-voting infrastructure

3.4.1 Separated infrastructure

Each canton has its own e-voting environment that is logically completely separated from other cantons' environments.

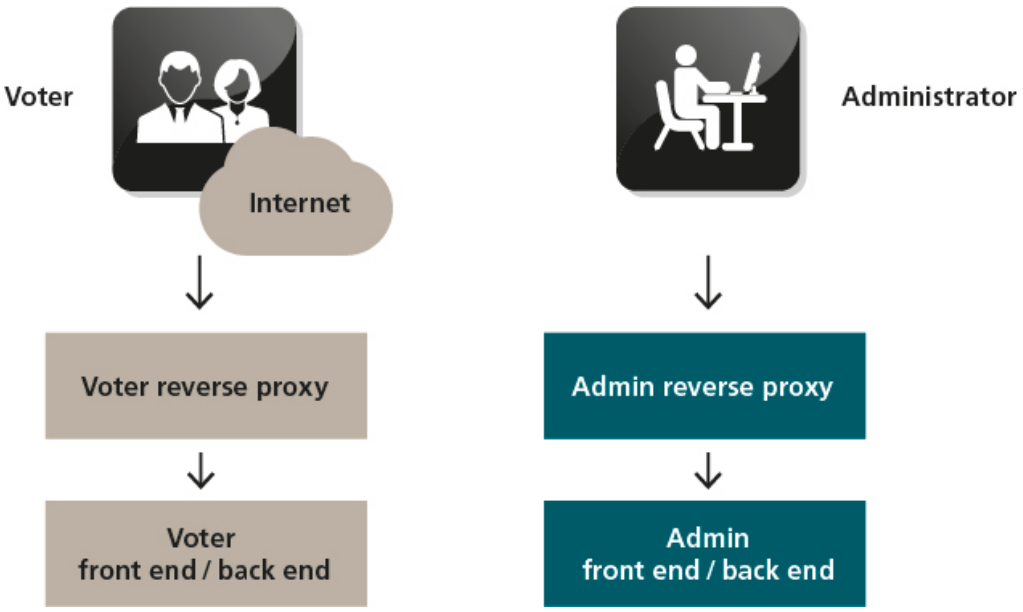
In addition to the separation of cantons, there is a dedicated access layer (reverse proxy infrastructure) that has been set up for voters and cantonal administrators.



The e-voting setup for each canton comprises two separate parts: the public voter part and the admin part. Both are completely separate; interconnections are not permitted and prevented by firewalls. The admin part is used to create an election with the SDM (secure data manager). The election is set up in the voter application via a specially secured channel. The voter part is used for the actual election for voters.

Both the public voter part and the admin part comprise several layered servers in various network areas/layers separated by firewalls.

- Access layer: reverse proxy
- Application layer: front-end server (application server, static file host)
- Application layer: back-end server (application server, application logic)
- Database layer: database (storage location of encrypted ballot papers in the encrypted ballot box)



The reverse proxy layer exists in two variants:

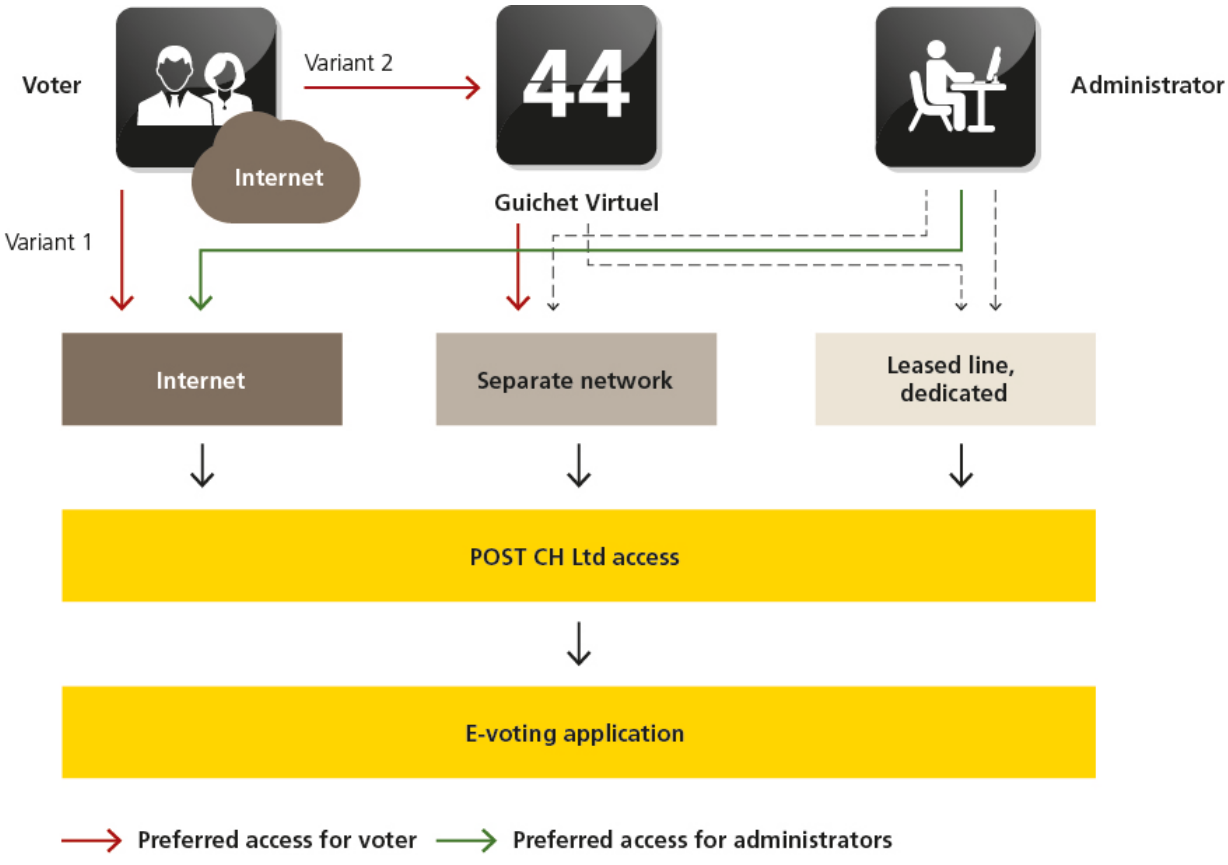
- **Variant: Swiss Post IT reverse proxy (model 1)**
  In the reverse proxy variant, the voter's browser or canton's secure data manager (SDM) accesses the reverse proxy infrastructure. The reverse proxy infrastructure performs a security test and, in the case of the SDM, performs authentication. The request is then forwarded to the front-end server in Swiss Post's canton layer/application layer.

- **Variant: Canton reverse proxy (model 2)**
  The canton provides the access layer for voters itself. From the canton's systems, the requests directly reach Swiss Post's canton layer/application layer via a separate network. The SDM devices use the same channel as in model 1. Model 2 allows a cantonal portal (e.g. Guichet Virtuel) to be connected securely to Swiss Post's e-voting infrastructure.

3.4.2 Access points for cantons

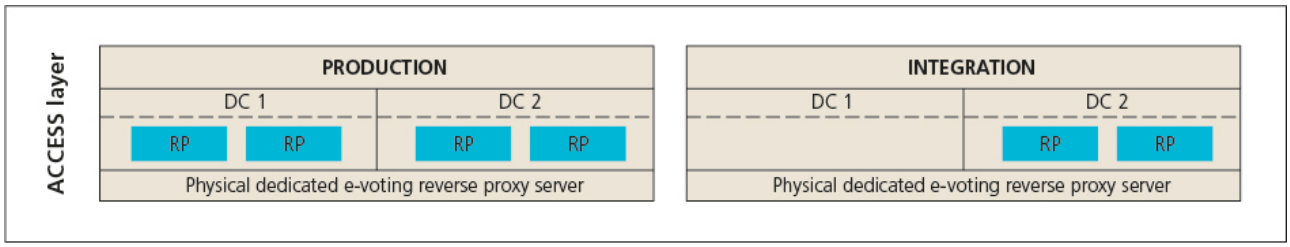
As described above, there are two access points for cantons. If the canton has its own infrastructure and portal, voters of the relevant canton can vote using this portal.
Cantons without their own portal may use Swiss Post's voter portal for their voters.

The following graphic illustrates the access points.



3.5 E-voting access layer

3.5.1 Reverse proxy infrastructure



Swiss Post's reverse proxies run on physical hardware. For each data center, there are two physical productive servers and a total of four servers for the e-voting environment. Reverse proxy functionality is ensured through multiple instances of the reverse proxy software for each server. For each hardware server, there is a voter reverse proxy, a voter SDM reverse proxy and an admin reverse proxy per canton. The instances are logically separated. They run on a highly secure operating system as different users with different certificates and separate IP addresses on specially robust servers.

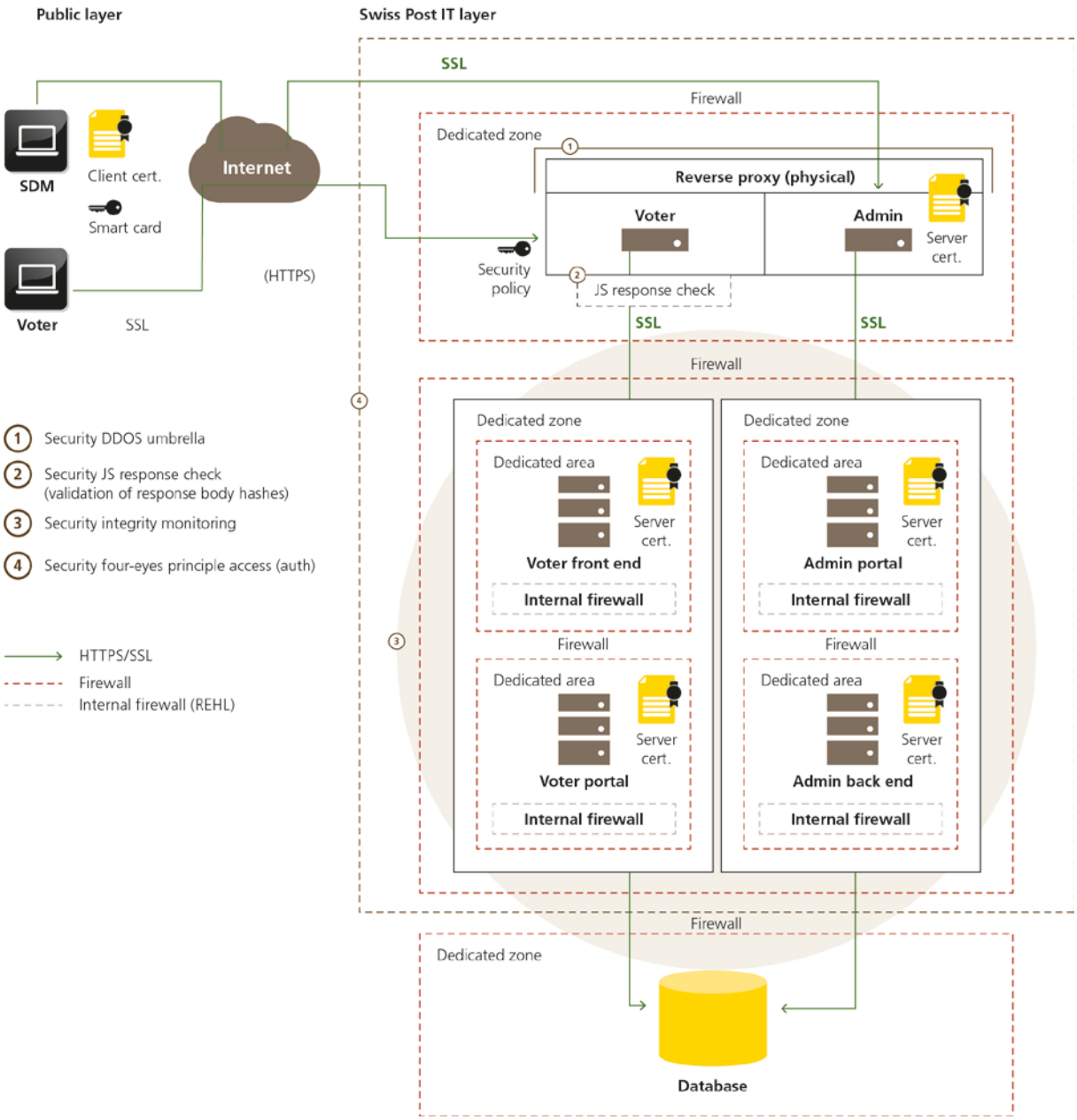
For access via the voter SDM and the admin reverse proxy, connections are authorized using a client certificate.

3.5.2 Security policy

An open-source security policy is used on the reverse proxies.
This is a module that offers protection from attacks. The module operates two different security policies. The voting reverse proxy must be accessible to international clients. Access can therefore not be authenticated using a client certificate. For this reason, a bespoke policy has also been developed for the voter reverse proxy that exclusively permits a narrow, pre-defined server access list.

4. E-voting security

Scytl's e-voting software already provides comprehensive security for the election and ballot boxes using a second-generation voting protocol, individual verifiability and end-to-end encryption. Swiss Post ensures the transport of encrypted ballot papers and encrypted ballot boxes. This transport is secured on Swiss Post's systems using additional security measures. The following diagram presents a summary of the security-relevant aspects implemented for Swiss Post's e-voting solution.



4.1 Security measures

4.1.1 Access layer/reverse proxies

A large proportion of security measures are concentrated on the access layer with its reverse proxies and are described in chapter 3.5 on the e-voting access layer. Essentially, this involves implementing mandatory access control both on the operating system and application levels.
In addition to these security measures, additional measures have been implemented to make e-voting as secure as possible. These are described below.

4.1.2 Firewalls, zones and areas

The zone and area concept separates the servers from each other within the network. This means that the access layer, voter front end, voter portal, admin portal, admin back end and database are in different networks and do not see each other. Each zone and each area are protected by firewalls. The connection takes place using regulated and defined firewall rules. The traffic allowed through a firewall and traffic not permitted through a firewall is defined in the firewall policy. The access layer is physically separated from the rest of the e-voting infrastructure.

4.1.3 SDM access

The SDM (secure data manager) with which the election is set up and with which the election results are collected is connected to the admin reverse proxy and the voter SDM reverse proxy. There is a certificate on the SDM. This is validated by the reverse proxies and used for authentication. This means that only this client can retrieve the different voting admin URLs. The SDM client is always used according to the multiple-control principle and is safely stored when not in use.

4.1.4 High-security operating system

The infrastructure is built on an open-source, high-security operating system that supports the access control mechanism. All e-voting platform servers (reverse proxies and e-voting servers) use this operating system.

This high-security operating system means that an e-voting server process runs in a separate context and is fully encapsulated. This means that a process can only use the system's designated resources. All other resources are not available to it (mandatory access control).

4.1.5 Firewall (IP table)

In addition to Swiss Post's own physical network firewall, firewall software is used on the entire e-voting platform and at operating system level. Only access to the necessary system management ports and from defined web server IP addresses is allowed.

4.1.6 Mutual authentication at SSL/TLS level

The various servers' communication is encrypted. They always authenticate each other using certificates. This ensures full end-to-end encryption (from data entry to vote counting) for e-voting.

4.1.7 Integrity monitoring

For e-voting, Swiss Post uses an open-source solution on the entire platform for operating system integrity monitoring and as an IDS (intrusion detection system).

4.1.8 JS response check

The reverse proxy validates the JavaScript files that are sent to a client (voter). This means that the reverse proxy checks files' hashes in the HTTPS response body that are delivered by the back-end systems. In the event of a deviation from the configured hash value, it prevents the delivery of a possibly manipulated file. This represents a control measure that ensures the correct JavaScript-based encryption of ballots on the client.

4.1.9 Four-eyes principle

The four-eyes principle controls administrative access to the entire e-voting infrastructure. When a system administrator wants to access an e-voting component, they require a token number that they receive from another person from another department after their identity and reasons for access have been checked. This token number is only valid once and becomes invalid once the administrator logs out.

4.1.10 E-voting monitoring

The infrastructure components are monitored in accordance with a standardized and ISO-certified process. Alarming takes place as per defined thresholds by SMS and/or e-mail alerts.

In addition to this monitoring, voter monitoring has been developed for e-voting. The e-voting application generates specific logs with events that can be assigned to individual phases in the voting process. This allows submitted, completely anonymized votes in an election to be observed in real time as well as be searched, filtered and statistically and graphically analysed. This monitoring is primarily used to verify that the electronic vote casting procedure is carried out properly. Critical situations or anomalies during an election trigger an alert that is sent by SMS to the defined entities.

4.1.11 E-voting deployment process

The deployment process describes the manner in which a new release from the software supplier will be applied to the e-voting platform. It is important to note that the supplied release is checked for integrity using a checksum and deployment will be only possible using the four-eyes principle. Each deployment is recorded in Swiss Post's change management tool, tracked, and tested and approved following deployment completion.

Post CH Ltd
Development & Innovation
Wankdorfallee 4
3030 Berne

swisspost.ch/e-voting
e-voting@swisspost.ch