Whitepaper

Übersicht über die Infrastruktur des E-Votings der Schweizerischen Post

November, 2016

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

The property of the cryptographic mechanisms and protocols described in this document is protected by their owners.

Use only for private, non-commercial audit purposes

© Copyright 2016 – Post CH AG, Bern, Switzerland

November, 2016

Inhaltsverzeichnis

1. Einleitung

1.1 Zweck des Dokuments

Die Schweizerische Post ist der Meinung, dass Transparenz zentral ist, um das Vertrauen der Bürgerinnen und Bürger sowie der Kantone für die elektronische Stimmabgabe zu gewinnen. Das vorliegende Dokument beschreibt die E-Voting Infrastruktur mit allen implementierten Sicherheitsaspekten.

2. E-Voting Software

Die E-Voting-Kern-Software, die bei der Schweizerischen Post eingesetzt wird, wurde von der Firma Scytl in Barcelona in Zusammenarbeit mit der Post entwickelt. Das dafür eingesetzte Stimmabgabeprotokoll der 2. Generation besitzt eine individuelle Verifizierbarkeit und ist End-to-End-verschlüsselt. Detailliertere Informationen zur Software können dem Whitepaper «Swiss-Post Online Voting Protocol Explained» entnommen werden.

Die Software selber erfüllt bereits hohe Anforderungen an die Sicherheit und ist von der Stimmabgabe bis zur Auswertung vollständig verschlüsselt. Die Infrastruktur ist katastrophensicher aufgebaut und kann nicht autorisierte Zugriffe von aussen wie von innen verlässlich abwehren.

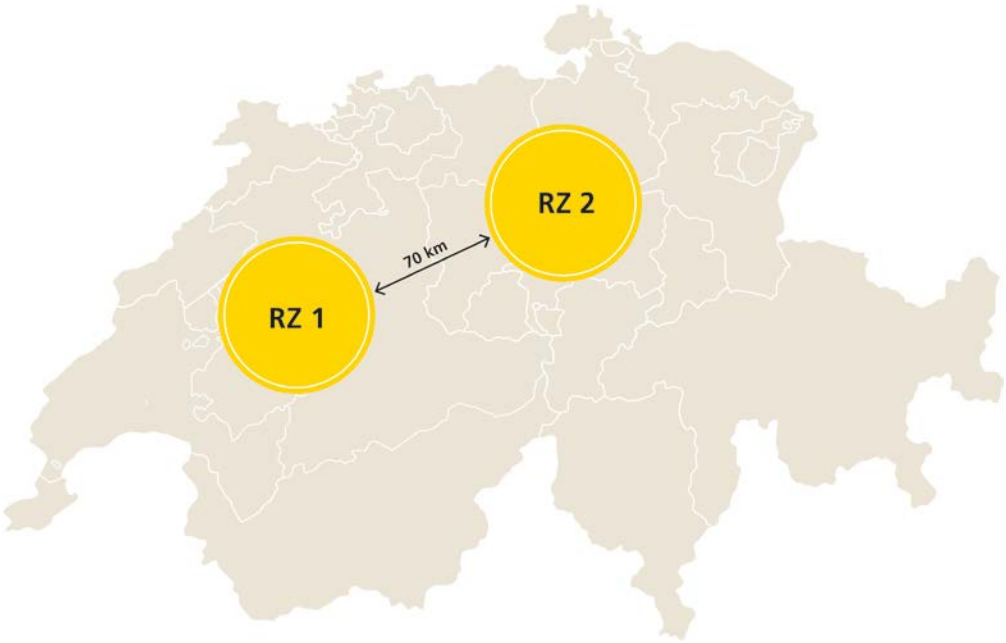
3. IT-Infrastruktur

3.1 Rechenzentren & BCM

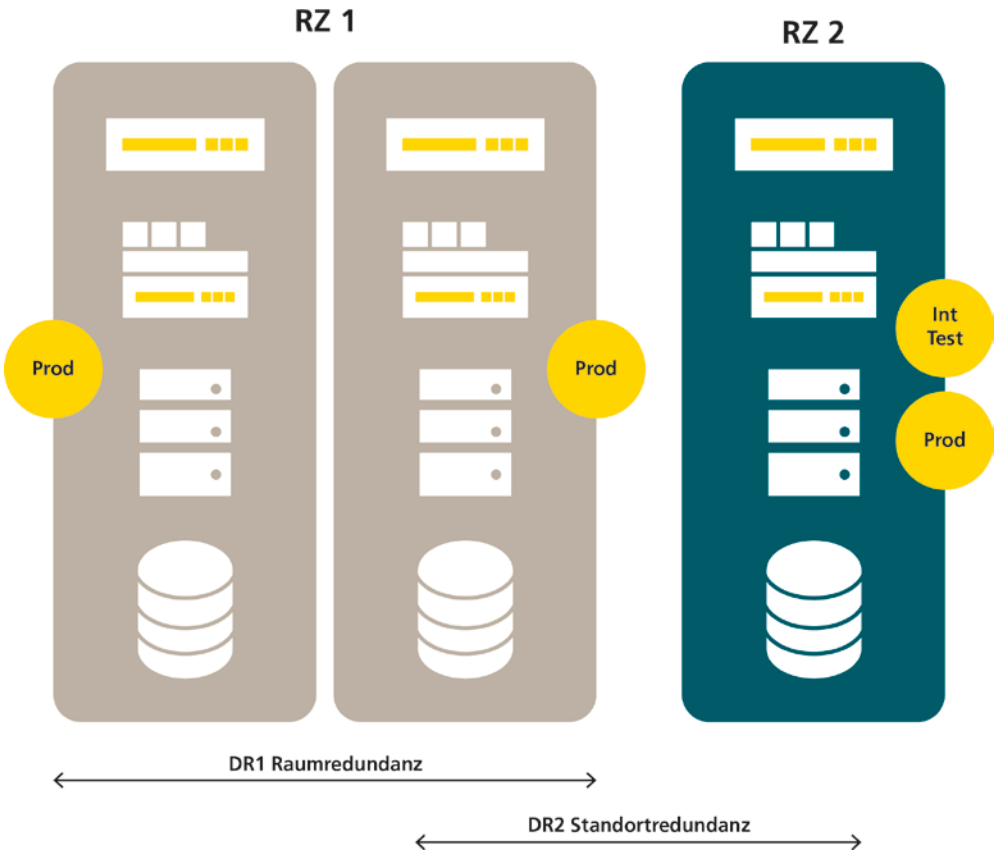
Die Schweizerische Post verfügt über zwei geografisch getrennte Rechenzentren. Die folgenden Merkmale zeichnen unsere Rechenzentren aus:

Merkmale

- FINMA-konform, TÜV-«Dual Site Level 3»-zertifiziert
- Der Betreiber ist ISO-27001- und ISO-22301-zertifiziert
- Vollständige Redundanzen kritischer Versorgungssysteme
- No single Point of Failure
- Stark authentifizierte Zutrittskontrolle
- Unterbruchsfreie Stromversorgung



Alle E-Voting Systeme sind in beiden Rechenzentren standortredundant vorhanden. Fällt das primäre Rechenzentrum aus, übernimmt das andere Rechenzentrum die Dienste. Neben der Standortredundanz wird innerhalb eines Rechenzentrums eine entsprechende Raumredundanz gewährleistet. Somit ist Business Continuity jederzeit gewährleistet.

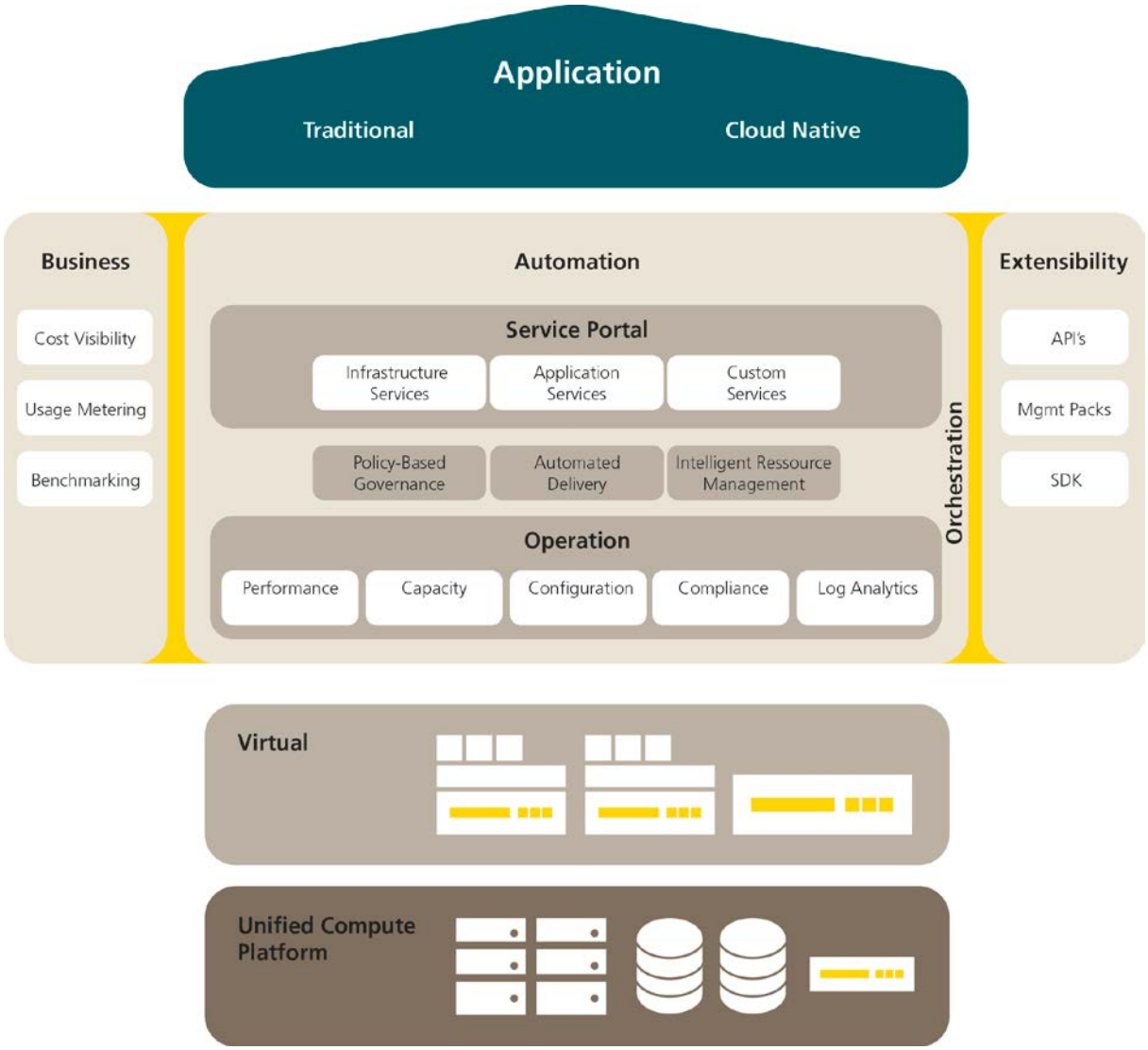


3.2 Applikationsinfrastruktur

3.2.1 E-Voting SDDC

Der E-Voting Service der Schweizerischen Post ist (ausser der Reverse-Proxy- und der Datenbank-Infrastruk-tur) vollständig virtualisiert. Die Virtualisierungsplattform widerspiegelt das Software Defined DataCenter SDDC der Schweizerischen Post.

Das System besteht aus einer Computer-, Netzwerk- und Storage-Infrastruktur, welche gemeinsam in einer Box (Datacenter in a Box) bereitgestellt wird. Solche Systeme können modular auf- und ausgebaut werden.

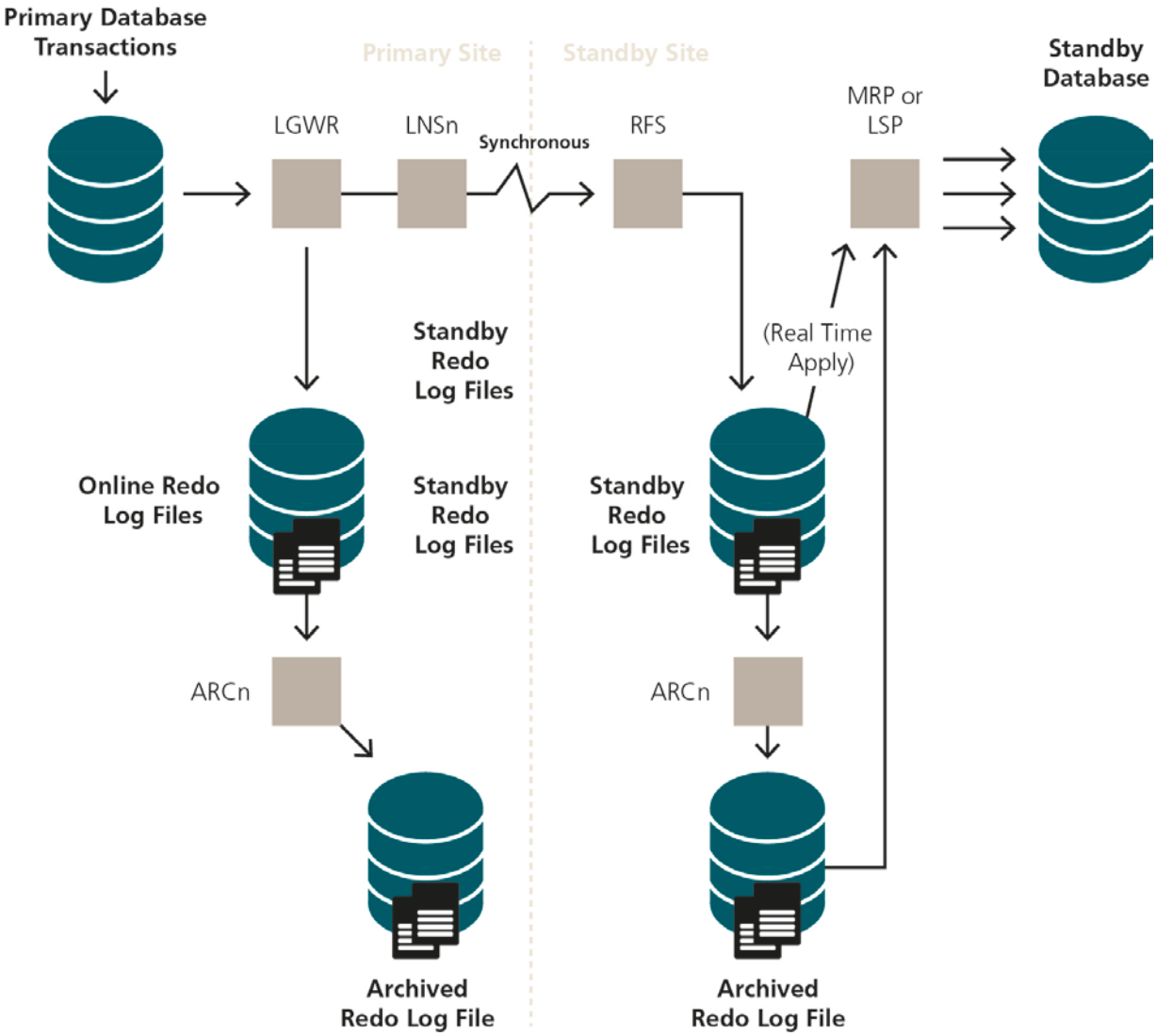


3.3 Datenbankinfrastruktur

Die E-Voting Datenbankinfrastruktur besteht aus drei produktiven und zwei integrativen, dedizierten Systemen.

3.3.1 Triple Mirroring und «zero data loss»

Die Wahlurne befindet sich verschlüsselt und signiert auf der Datenbank. Die Daten müssen stets konsistent sein und es dürfen zu keiner Zeit Daten verloren gehen. Die Daten werden daher dreifach und synchron «triple mirroring» gespeichert.

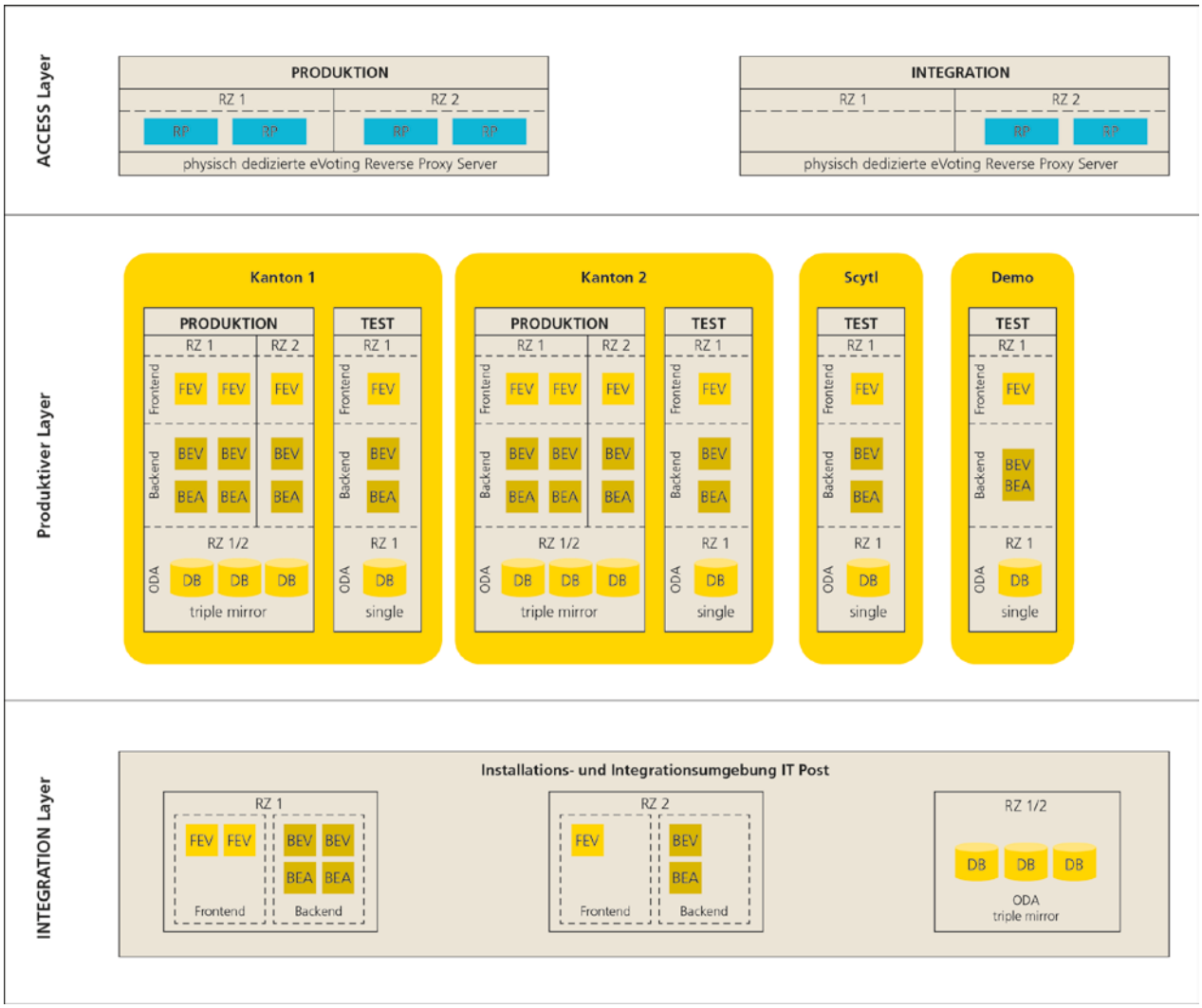


3.4 E-Voting Infrastruktur

3.4.1 Getrennte Infrastruktur

Jeder Kanton verfügt über eine eigene E-Voting Umgebung, die logisch komplett von den Umgebungen der anderen Kantone getrennt ist.

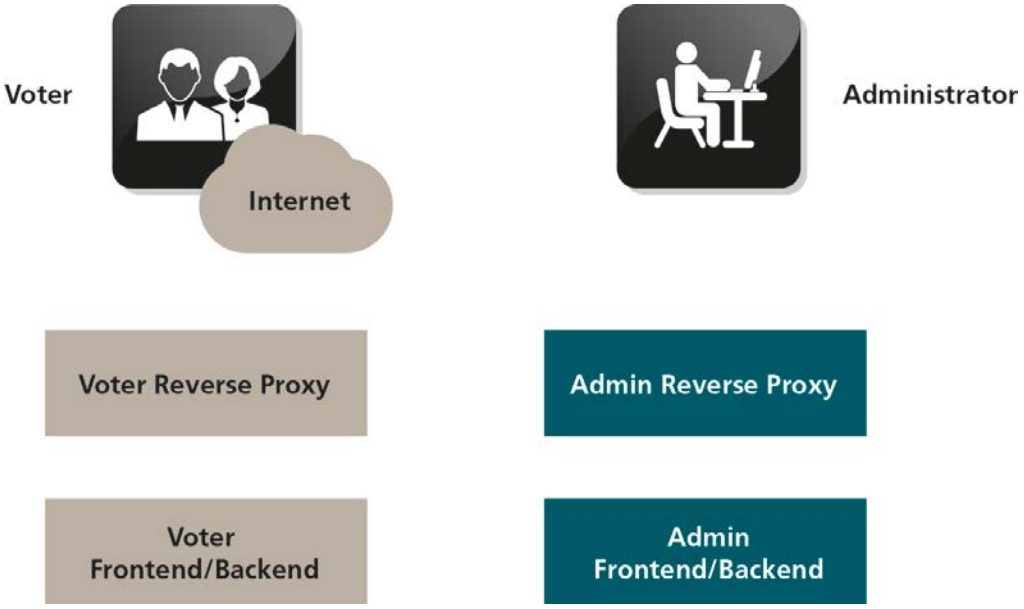
Neben der Kantonstrennung gibt es einen dedizierten Access Layer (Reverse-Proxy-Infrastruktur), der für Stimmbürgerinnen und Stimmbürger sowie für Kantonsadministratoren aufgebaut worden ist.



Der E-Voting Setup pro Kanton umfasst zwei getrennte Teile. Den öffentlichen Voter-Teil sowie den Admin-Teil. Die beiden Ausprägungen sind komplett getrennt, Querverbindungen sind nicht zugelassen und durch Firewalls verunmöglicht. Der Admin-Teil wird verwendet, um mit dem SDM (Secure Data Manager) eine Wahl zu kreieren. Die Wahl wird via einen speziell gesicherten Kanal auf der Voter-Applikation eingerichtet. Der Voter-Teil wird für den effektiven Urnengang für die Stimmbürger oder Stimmbürgerinnen verwendet.

Sowohl der öffentliche Voter-Teil wie auch der Admin-Teil bestehen aus mehreren hintereinander gestaffelten Servern in unterschiedlichen, durch Firewalls getrennten Netzwerk Areas / Layers:

- Access Layer: Reverse Proxy
- Application Layer: Frontend Server (Applikationsserver, Host von statischen Files)
- Application Layer: Backend Server (Applikationsserver, Applikationslogik)
- Database Layer: Datenbank (Speicherort der verschlüsselten Wahlzettel in der verschlüsselten Urne)



Die Reverse-Proxy-Schicht existiert in zwei Varianten:

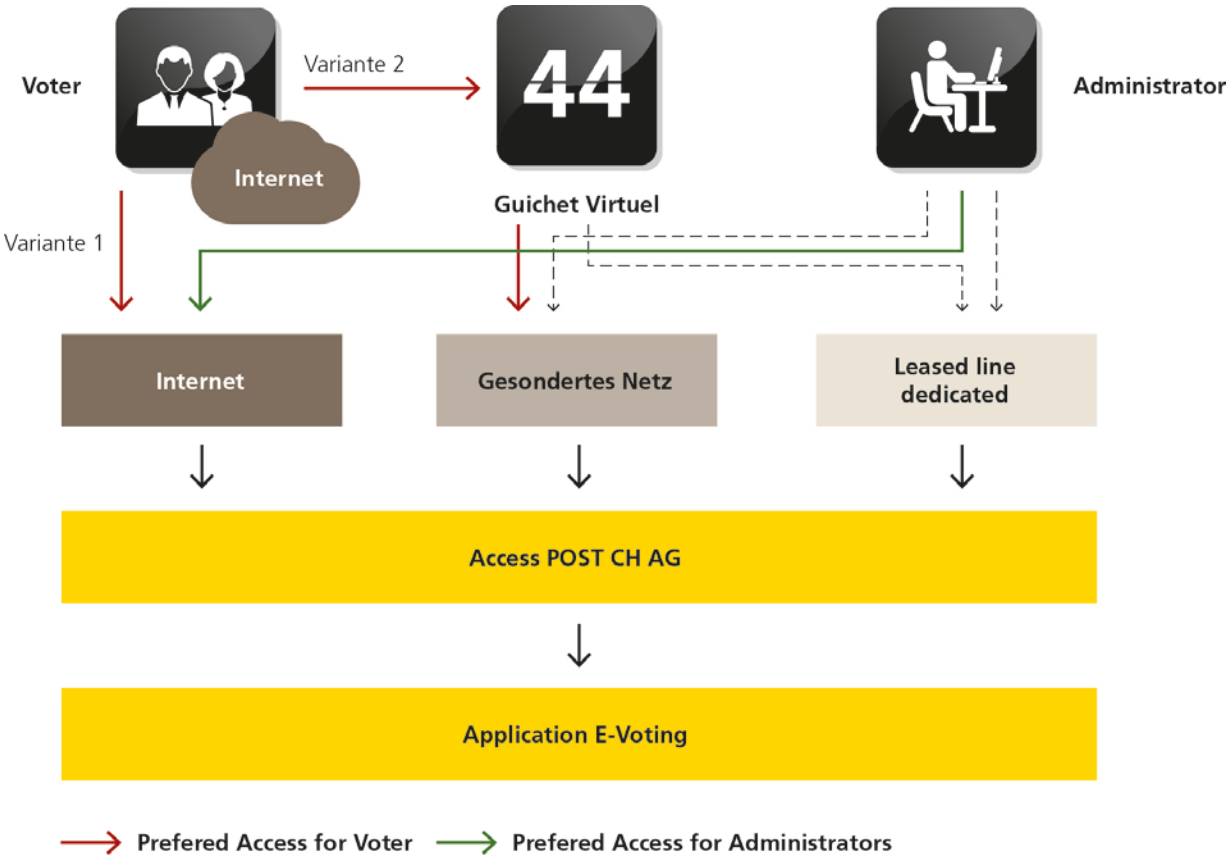
- **Variante: Reverse Proxy bei Post IT (Modell 1)**
  In der Variante Reverse Proxy greift der Browser des Stimmbürgers oder der Stimmbürgerin respektive der Secure Data Manager (SDM) des Kantons auf die Reverse-Proxy-Infrastruktur zu. Die Reverse-Proxy-Infrastruktur führt eine Sicherheitsüberprüfung und im Fall des SDM bereits eine Authentifizierung durch. In einem zweiten Schritt wird die Anfrage an die Frontend-Server im Kantons-Layer / Application Layer der Post weitergereicht.

- **Variante: Reverse Proxy bei Kanton (Modell 2)**
  Der Kanton stellt die Access Layer für die Stimmbürger und Stimmbürgerinnen selbst zur Verfügung. Von den Systemen des Kantons gelangen die Anfragen über ein gesondertes Netz direkt in die Kantons-Layer / Application Layer der Post. Die SDM-Geräte benützen denselben Kanal wie beim Modell 1. Das Modell 2 ermöglicht es, ein Kantonsportal (z. B. Guichet Virtuel) sicher mit der E-Voting Infrastruktur der Post zu verbinden.

3.4.2 Zugangsmöglichkeiten für Kantone

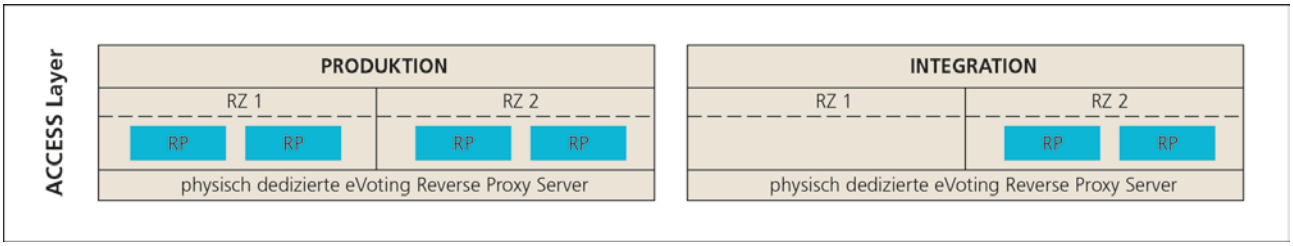
Wie oben beschrieben gibt es für Kantone zwei unterschiedliche Zugangsmöglichkeiten. Falls der Kanton über eine eigene Infrastruktur und ein eigenes Portal verfügt, können Stimmbürgerinnen und Stimmbürger des entsprechenden Kantons den Urnengang darüber abwickeln.
Kantone ohne eigenes Portal können für ihre Stimmbürgerinnen und Stimmbürger das Voter-Portal der Schweizerischen Post nutzen.

Die nachfolgende Grafik visualisiert die Zugangsmöglichkeiten.



3.5 E-Voting Access Layer

3.5.1 Reverse-Proxy-Infrastruktur



Die Reverse Proxies der Post laufen auf physikalischer Hardware. Pro Rechenzentrum existieren zwei physikalische produktive Server, total vier Server für die E-Voting Umgebung. Die Reverse-Proxy-Funktionalität wird pro Server durch mehrere Instanzen der Reverse Proxy Software sichergestellt. Pro Hardware Server existiert pro Kanton ein Voter Reverse Proxy, ein Voter-SDM Reverse Proxy und ein Admin Reverse Proxy. Die Instanzen sind logisch voneinander getrennt. Sie laufen als unterschiedliche User mit verschiedenen Zertifikaten und separaten IP-Adressen auf speziell gehärteten Servern unter einem hochsicherheits-Betriebssystem.

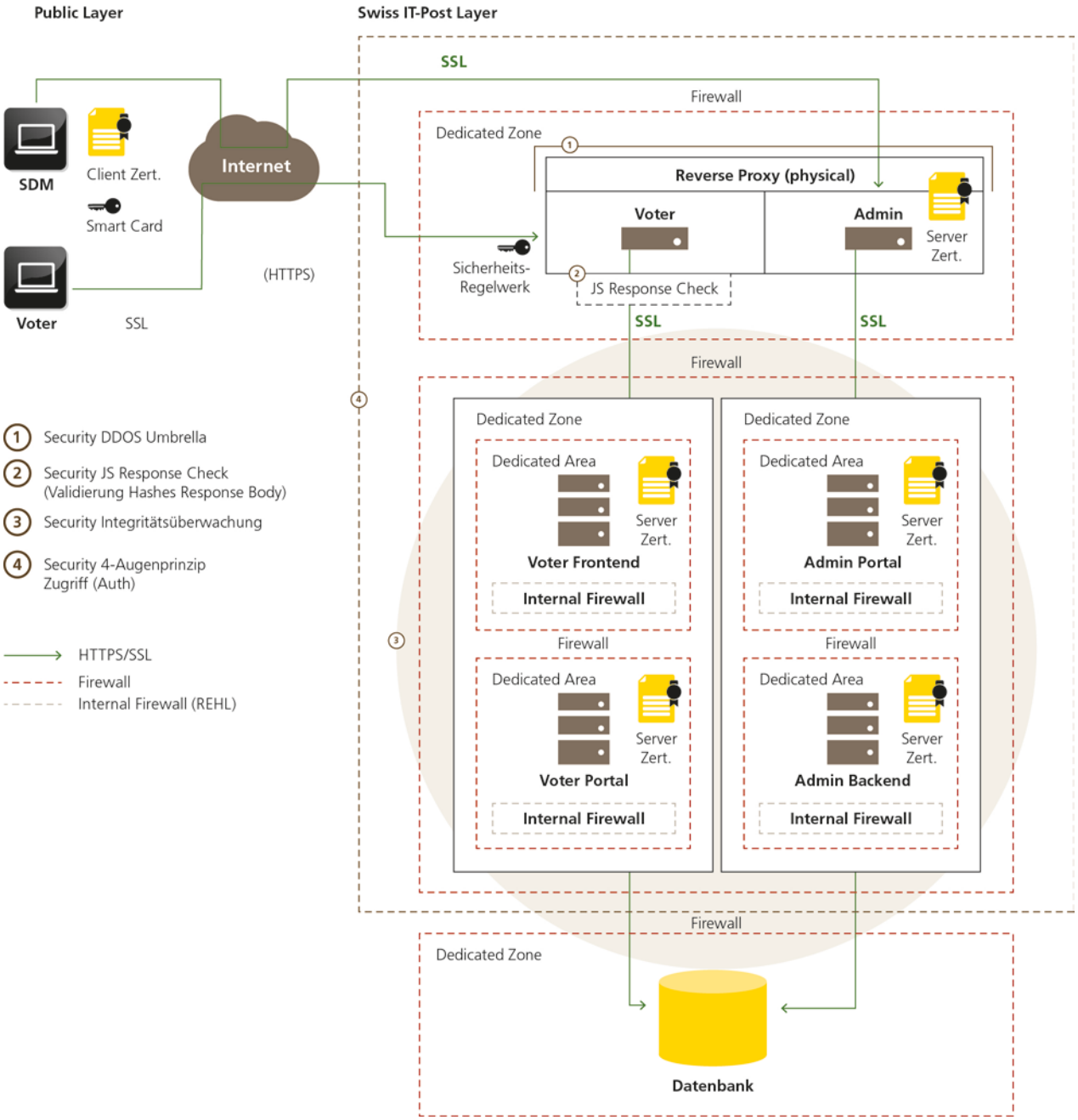
Für den Zugriff über den Voter-SDM und über den Admin Reverse Proxy werden die Verbindungen mittels Client-Zertifikat authentisiert.

3.5.2 Sicherheits-Regelwerk

Auf den Reverse Proxies wird ein Open-Source-Sicherheits-Regelwerk eingesetzt.
Dabei handelt es sich um ein Modul, das Schutz vor Angriffen bietet. Das Modul wird mit zwei verschiedenen Regelwerken betrieben.
Der Voting Reverse Proxy muss für weltweite Clients zugänglich sein. Der Zugang kann deshalb nicht mittels Client-Zertifikat authentisiert werden. Aus diesem Grund wurde für den Voter Reverse Proxy zusätzlich ein massgeschneidertes Regelwerk entwickelt, das ausschliesslich eine knappe, vordefinierte Liste von Zugriffen auf den Server zulässt.

4. E-Voting Sicherheit

Die E-Voting Software der Firma Scytl sichert die Wahl und die Wahlurne mittels des Stimmabgabeprotokolls der 2. Generation, der individuellen Verifizierbarkeit und der End-to-End-Verschlüsselung bereits umfassend. Die Post stellt den Transport der verschlüsselten Wahlzettel und der verschlüsselten Wahlurne sicher. Dieser Transport wird auf den Systemen der Post durch zusätzliche Sicherheitsmassnahmen gesichert. Die nachfolgende Darstellung zeigt übersichtlich die sicherheitsrelevanten Aspekte auf, die für die E-Voting Lösung der Post umgesetzt wurden.



4.1 Sicherheitsmassnahmen

4.1.1 Access Layer / Reverse Proxies

Ein grosser Teil der Sicherheitsmassnahmen konzentriert sich auf den Access Layer mit seinen Reverse Proxies und ist im Kapitel 3.5 E-Voting Access Layer detailliert beschrieben. Im Kern geht es darum, Mandatory Access Control sowohl auf Betriebssystem- wie auch Applikationsebene durchzusetzen. Neben diesen Sicherheitsmassnahmen wurden weitere Massnahmen implementiert, um den E-Voting Betrieb so sicher wie möglich zu machen. Sie werden im Folgenden beschrieben.

4.1.2 Firewalls, Zonen und Areas

Das Zonen- und Area-Konzept trennt die Server netzwerktechnisch voneinander. Das heisst, Access Layer, Voter Frontend, Voter-Portal, Admin-Portal, Admin Backend und die Datenbank sind in unterschiedlichen Netzen und sehen einander nicht. Jede Zone und jede Area sind durch Firewalls geschützt. Die Verbindung erfolgt mittels reglementierter und definierter Firewall-Rules. Im Firewall-Regelwerk wird definiert, welcher Verkehr durch eine Firewall erlaubt und welcher verboten ist. Der Access Layer ist physisch vom Rest der E-Voting Infrastruktur getrennt.

4.1.3 SDM-Zugang

Der SDM (Secure Data Manager), mit dem die Wahl aufgesetzt wird und die Wahlresultate abgeholt werden, verbindet sich mit dem Admin Reverse Proxy sowie mit dem Voter SDM Reverse Proxy. Auf dem SDM befindet sich ein Zertifikat. Dieses wird von den Reverse Proxies validiert und zur Authentifizierung herangezogen. Das heisst, dass nur dieser Client die verschiedenen Voting Admin URL aufrufen kann. Der SDM Client wird immer im Mehraugen-Prinzip verwendet und bei Nichtgebrauch sicher eingelagert.

4.1.4 Hochsicherheits-Betriebssystem

Die Infrastruktur ist auf einem Open Source hochsicherheits-Betriebssystem gebaut, das den Mechanismus der Zugriffskontrolle unterstützt. Alle Server der E-Voting Plattform (Reverse Proxies sowie die eVoting Server) haben dieses Betriebssystem im Einsatz.

Dieses hochsicherheits-Betriebssystem bedeutet, dass ein E-Voting Server Prozess in einem eigenen Kontext läuft und vollständig abgekapselt wird. Das heisst, der Prozess kann nur auf die vorgesehenen Ressourcen des Systems zugreifen. Alle anderen Ressourcen stehen ihm nicht zur Verfügung (Mandatory Access Control).

4.1.5 Firewall (IP-Table)

Als zusätzliche Zugriffs-Absicherung neben den posteigenen physischen Netzwerkfirewalls wird auf der gesamten E-Voting Plattform zusätzlich noch auf Betriebssystem-Ebene eine Firewallsoftware eingesetzt. Es werden nur die Zugriffe auf die notwendigen System Management Ports und von definierten Webserver-IP-Adressen zugelassen.

4.1.6 Mutual Authentication auf SSL/TLS-Ebene

Die verschiedenen Server kommunizieren verschlüsselt. Sie authentifizieren sich dazu immer gegenseitig mittels Zertifikaten.
Somit ist eine vollständige End-to-End-Verschlüsselung (von der Erfassung bis zur Auszählung der Stimmen) für E-Voting gewährleistet.

4.1.7 Integritätsüberwachung

Die Schweizerische Post setzt für E-Voting zur Integritätsüberwachung des Betriebssystems sowie als IDS (Intrusion Detection System) eine Open-Source-Lösung auf der gesamten Plattform ein.

4.1.8 JS Response Check

Der Reverse Proxy validiert die Java-Script-Dateien, die an einen Client (Wähler) gesendet werden. D.h., der Reverse Proxy überprüft die Hashes der Dateien im HTTPS Response Body, welche durch die Backend-Systeme ausgeliefert werden. Bei einer Abweichung vom konfigurierten Hash-Wert verweigert er die Auslieferung einer möglicherweise manipulierten Datei. Dies stellt eine Kontrollmassnahme dar, welche die korrekte Java-Script-basierte Verschlüsselung der Stimmzettel auf dem Client sicherstellt.

4.1.9 4-Augen-Prinzip

Das 4-Augen-Prinzip kontrolliert den administrativen Zugang zu der kompletten E-Voting Infrastruktur. Wenn ein System-Administrator Post auf eine E-Voting Komponente zugreifen will, braucht er eine Token-Nummer, die er nach Identitäts- und Begründungsprüfung von einer anderen Person aus einer anderen Fachabteilung erhält. Diese Token-Nummer ist nur einmal gültig und verfällt, sobald sich der Administrator wieder abmeldet.

4.1.10 E-Voting Monitoring

Die Infrastrukturkomponenten werden gemäss standardisiertem und ISO-zertifiziertem Prozess überwacht. Das Alarming erfolgt gemäss definierten Schwellenwerten per SMS und/oder E-Mail Alerts.

Neben dieser Überwachung wurde für E-Voting ein sogenanntes «Voter-Monitoring» aufgebaut. Die E-Voting Applikation generiert spezifische Logs mit Events, die sich einzelnen Phasen im Abstimmungsvorgang zuordnen lassen können. Somit können eingegangene, vollständig anonymisierte Stimmen bei einem Urnengang in Echtzeit beobachtet, durchsucht, gefiltert, statistisch analysiert und grafisch ausgewertet werden. Dieses Monitoring dient primär zur Kontrolle des ordentlichen Ablaufs der elektronischen Stimmabgabe. Kritische Zustände oder Anomalien während einem Urnengang lösen einen Alert aus, der per SMS an die definierten Stellen übermittelt wird.

4.1.11 E-Voting Deploymentprozess

Der Deploymentprozess beschreibt die Art und Weise, wie ein neuer Release des Softwarelieferanten auf die E-Voting Plattform aufgespielt wird. Hierbei ist zu beachten, dass der gelieferte Release mittels Checksumme auf Integrität geprüft wird und das Einspielen lediglich mit dem 4-Augen-Prinzip möglich ist. Jedes Deployment wird im Changemanagement-Tool der Post erfasst, getrackt und nach Vollendung des Deployments abgenommen.

Post CH AG
Entwicklung und Innovation
Wankdorfallee 4
3030 Bern

post.ch/e-voting
e-voting@post.ch