E-vote 2011

Appendix 6: Customer Technical Platform

Project: E-vote 2011

Change log

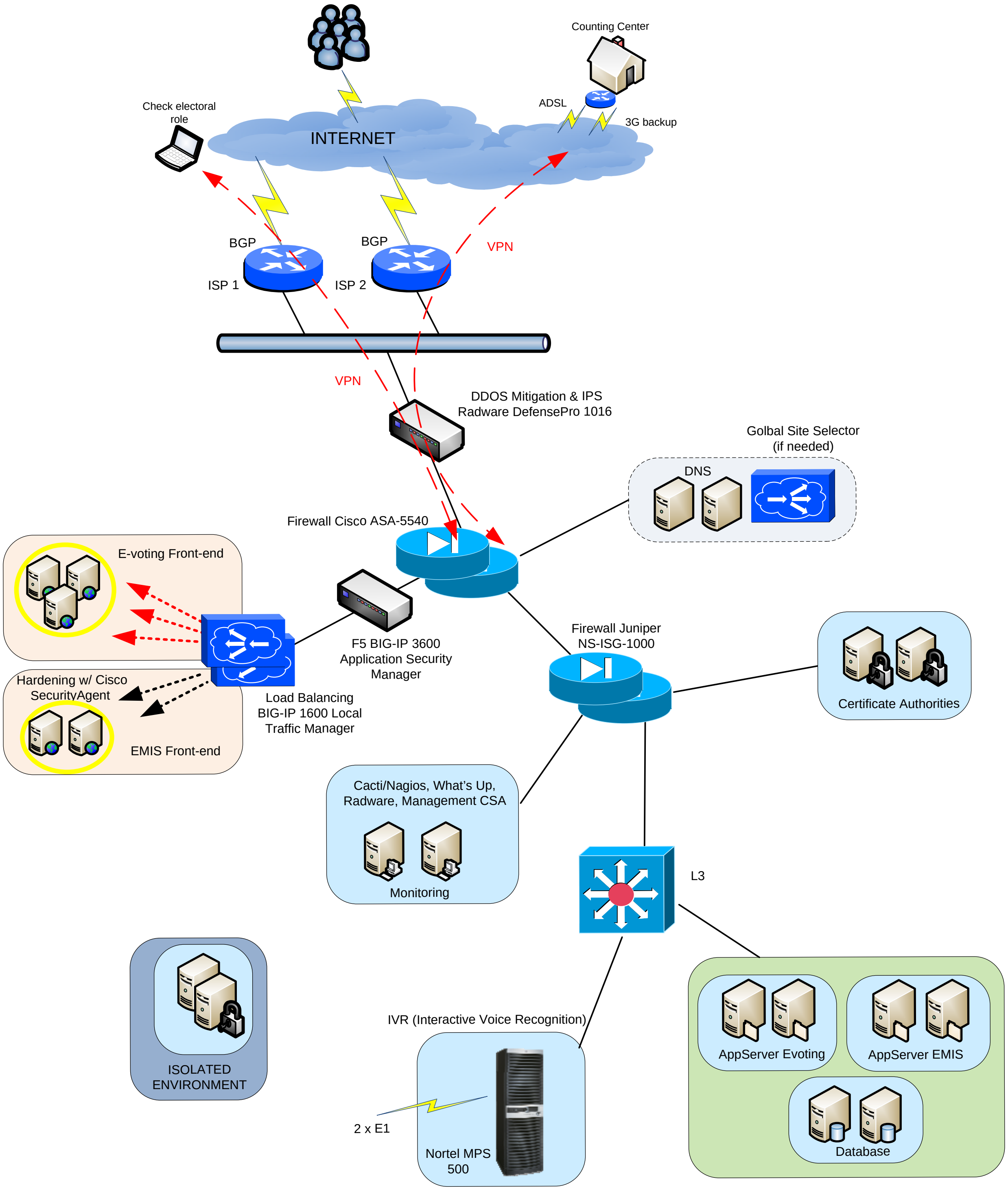
Version	Date	Author	Description/changes
0.1	26.10.09		First version

CONTENT

1. Technical Platform – 2011 Pilots

1.1. Technical Platform Overview

The following figure presents the detailed diagram of the whole election platform.


Counting Center
ADSL
3G backup
Check electoral role
INTERNET
BGP
BGP
ISP 1
ISP 2
VPN
VPN
DDOS Mitigation & IPS
Radware DefensePro 1016
Golbal Site Selector
(if needed)
DNS
Firewall Cisco ASA-5540
E-voting Front-end
F5 BIG-IP 3600
Application Security
Manager
Firewall Juniper
NS-ISG-1000
Certificate Authorities
Hardening w/ Cisco
SecurityAgent
Load Balancing
BIG-IP 1600 Local
Traffic Manager
EMIS Front-end
Cacti/Nagios, What's Up,
Radware, Management CSA
Monitoring
L3
ISOLATED
ENVIRONMENT
IVR (Interactive Voice Recognition)
2 x E1
Nortel MPS
500
AppServer Evoting
AppServer EMIS
Database

1.1.1. Access Router

The datacenter will have two different WAN connections for redundancy reasons.

The routers will share via BGP a block of 16 public IP addresses. If the main access to Internet fails the secondary router will propagate those IP addresses.

It is recommended that both routers belong to different Service Providers. Different technology would be desirable on each ISP (fiber, copper).

The estimated bandwidth is approximately 30 Mbps.

1.1.2. DOS/DDOS/IPS Mitigation Hardware

To prevent a DDOS/DOS attack on the election system infrastructure and network, a DOS/DDOS mitigation hardware shall be implemented on the external part of the network to detect and block connections with relatively high volume of network traffic coming from a single source machine directed towards the election system and prevent the attack from reaching the internal part of the network.

To protect the whole election system from malicious and anomalous behavior, an IPS shall be implemented. The IPS shall be able to detect and block all types of attacks and attack signatures launched against any of the devices inside the election system.

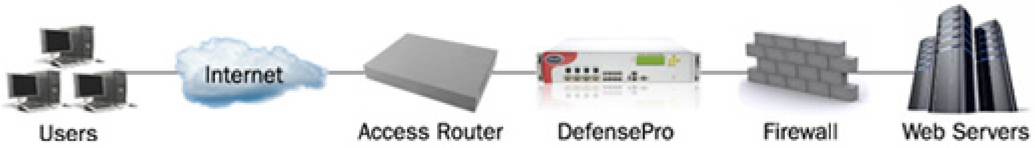
This device is installed between the router and the perimeter firewall. Many Internet Service Providers allows the installation of this device in-front of the access router (ISP network). This is something we need to negotiate with the ISP to prevent possible DOS/DDOS attacks from reaching the core network of the election system.

Radware’s award-wining DefensePro is a real-time Intrusion Prevention System (IPS) and DoS protection device that maintains your business continuity by protecting your application infrastructure against existing and emerging network based threats that can’t be detected by a traditional IPS such as: network & application resource misuse, malware spreading, authentication defeat and information theft. DefensePro features full protection from traditional vulnerability-based attacks through proactive signature updates that prevent already known attacks including worms, Trojans, Bots, SSL-based attacks and VoIP attacks.

Unlike market alternatives that rely on static signatures, DefensePro provides unique behavioral-based and automatically generated real-time signatures to prevent non-vulnerability-based and zero-minute attacks. These attacks include: network & application floods, HTTP page floods, malware propagation, Web application hacking, brute force attacks aiming to defeat authentication schemes, and more. And, DefensePro does this all without blocking legitimate users' traffic and without need of human intervention.

With multiple segments protection in a single unit, a pay-as-you-grow license upgrade approach, and ease of management with ‘hands-off’ security features such as no-configuration and self-tuning, DefensePro is the industry’s leading IPS for best functionality, maximum affordability and ease of management.

DefensePro protects revenue-generating Web-enabled services. Online businesses rely on Web applications to generate their revenues. DefensePro coexists with other security tools such as firewalls, Web application firewalls (WAFs) and even signature-based IPSs, which are incapable of fending off high-volume DoS/DDoS flood attacks and application-flood attacks.



DefensePro is the industry’s first solution to provide unparalleled security by offering adaptive, behavior-based protection capabilities at client, application server and network levels. It immediately identifies and mitigates a wide range of network attacks (including non-vulnerability threats and zero-minute attacks) by automatically generating real-time signatures. The real-time signature "engine" is an adaptive multi-dimension decision engine that deploys fuzzy logic technology for accurate attack detection and mitigation without blocking legitimate user traffic.

Insite Centralized Management and Reporting

Radware’s Insite provides the management interface for all APSolute products, including DefensePro. With features that enable centralized device configuration, monitoring and reporting, Insite management solution increases visibility and control of network security (provides real-time detailed information on attack attempts, including the type and severity of those attacks).

DefensePro IPS & Behavioaral Protection Model

We suggest DefensePro 1016, which has a performance up to 1 Gbps of inspection.
This model is designed for the protection of medium-sized data centers deployed by large enterprises, eCommerce and service providers.
The Radware’s Insite management interface will be installed in a server (monitoring module of the datacenter).

1.1.3. Perimeter security

To protect the perimeter of the election system, Indra shall implement the following security measures:

DMZ Networks: A DeMilitarized Zone (DMZ) network shall be implemented where all publicly available servers (e-vote web servers, DNS server, EMIS front-end servers) are to be located and protected.

External Network Firewall: for ports and services filtering, to ensure that only those defined and allowed ports and services and allowed to pass through the external network. For the polling stations and count centers, a VPN connection shall be implemented. Tunnel closing and opening shall be done on this device.

The chosen firewall is a Cisco ASA-5540 (active/passive pair). This firewall has enough performance to handle all the traffic, including the IPSEC tunnels of the counting centers and the remote access (the computers checking the electoral role).

Internal Network Firewall: The internal firewall shall be implemented to protect the internal servers (Application servers, Database servers) located in the internal part of the network that is directly communicating with the servers located in the DMZ. This firewall shall ensure that only the defined and authorized ports, services and frontend machines are allowed access to the internal servers.
To avoid human errors on the configuration, the internal firewall will be from other vendor, such as Juniper ISG-1000 (active/passive pair).

Indra is open to changes if the customer is more confident with other firewall vendors

Application firewall: to ensure that only authorized http methods are executed on the application level and hazardous methods are blocked. It employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration prevents the possibility of application level attacks such as XSS, SQL injection, CSRF, Link injection caused by badly coded source codes.

F5-BIG-ASM-3600-4G. BIG-IP Application Security Manager (ASM) delivers comprehensive protection for web applications. BIG-IP ASM can help your organization quickly pass a security audit without requiring changes to the application code. It employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration makes implementation and maintenance easier

BIG-IP Application Security Manager is the fastest application delivery security product on the market and includes an integrated XML firewall. It combines application optimization and acceleration technologies such as RAM cache, compression, SSL offload, TCP optimization, and other performance advantages of F5's TMOS architecture. This offloads the servers, improves the user experience, and consolidates the footprint in the datacenter for easier management.

With BIG-IP Application Security Manager, application delivery security is easy to implement and manage. It includes specific, built-in validated application security policies for common applications as well as an automatic policy-building engine that can quickly adapt to application updates. BIG-IP ASM helps you rapidly and virtually patch web application vulnerabilities without involving your application development team. This helps you maintain compliance with government and industry regulations such as PCI and HIPAA.

VPN Connection: A VPN connection shall be implemented to all PCs located in polling stations to provide an end-to-end secure communication.

SSL Channel: For e-voting in an uncontrolled environment a secure communication channel shall be implemented using SSL 256 bit key encryption to protect the data traversing between the voter and the election system to prevent data hijacking, intercepting and modifying

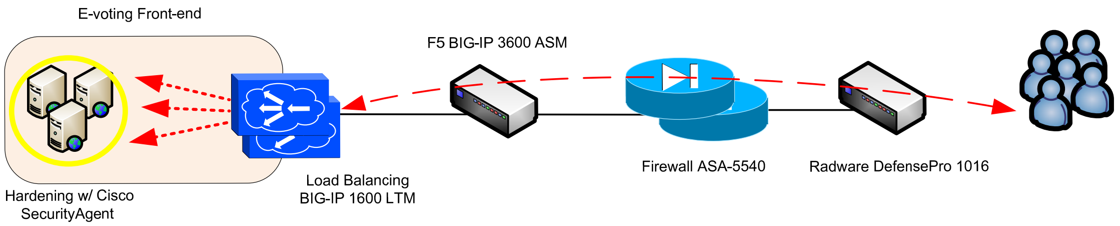
Server, Routers and Switches Hardening
The proposed solution shall include a server hardening that will involve the creation of a baseline for the security on all election system platforms including the PCs to be used on polling stations (controlled environment). As it is understood, that the default configurations of the election platforms are not

designed with security as the primary focus, but rather, it is designed for communication and functionality only. To effectively protect the platforms, a solid and sophisticated security baseline for all types of platforms in the election system shall be implemented, that includes removing unnecessary services and filtering TCP and UDP ports.

Security hardening features shall also be applied on switches and routers to prevent possible attacks that could compromise the election system network

In addition, a Cisco security agent shall be in place to execute and manage the hardening tasks on all frontend servers (webservers).

Webservers will have a Cisco Security Agent installed to prevent manipulation on the server itself.



Cisco Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

Cisco Security Agent provides numerous network security benefits including:

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware
- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities
- "Always Vigilant" Security - Your system is always protected, even when users are not connected to the corporate network or lack the latest patches

1.1.4. Monitoring

Monitoring the availability and usage of network and computing resources plays an important role in the voting process. To be able to manage networks components and computing resources proactively it is vital to have a comprehensive monitoring system in place.

Monitoring system shall be implemented to monitor the services and features of the election system including the implemented security mechanisms to ensure that all systems are working properly. Any failure detected shall be reported in real-time. Election personnel shall monitor and check the functionalities of the election system and ensure that prompt action is executed once an alarm is received

Two servers will be checking the services on servers, storing events and collecting statistics.The tools installed will be:

- Cacti or Nagios. Checking applications, services and networking statistics.
- What's Up.
- Syslogs
- Radware Insite security. Manage and store security DDOS and IPS attacks.
- Cisco Security Agent Management. Manage and store events on front-end servers

1.1.5. Data security:

Isolated environment server
To protect the confidentiality of data and maintain its integrity, the election system will deploy a totally secure and hardened isolated environment server. This server will not be in any way connected to any other network logically or physically. The isolated server will serve the following operations:

- The generation of public/private keys that will be used to decrypt/encrypt the e-votes.
- VoterID generation
- Unique party code generation for every voter and calculation of hash value equivalent for every party code
- The decryption and counting of e-votes after the election process

As this server is isolated logically and physically, the risks of data compromise logically would be impossible.

Data encryption
The election system shall implement an asymmetric algorithm using RSA 2048 bit key encryption to encrypt the votes. After generating the public and private key, the private key shall be encrypted using symmetric algorithm and shall be divided into several parts using secret sharing algorithm and providing each authorized election officers its own unique part of the key where parts or all of them are needed in order to reconstruct the key. In this case, we considered that counting on all authorized officers to combine together the secret keys might be impractical and therefore a threshold scheme shall be used where some of the secret key parts will be sufficient enough to reconstruct the key and execute the decryption process

Voter unique party code
To protect the integrity of the vote, a unique party code shall be generated for every voter. A voter shall be provided a unique party code that corresponds to the voter and is unique to every other voter. If in case the voter's terminal has been compromised and infected, and the attacker has successfully manipulated the vote and change the party code to another party code, it will be detected by the election system and the voter shall be asked to review the party code provided in the voter's card. A hash calculation mechanism that validates every unique party code provided to every voter will ensure that no manipulated voted can be recorded and accepted at any time.

Encryption algorithms
To ensure the security, integrity and confidentiality of all election data, the following encryption algorithms shall be implemented:

- RSA 2048: This encryption shall be implemented to encrypt the recorded e-votes
- AES 256 bit: This encryption shall be used to encrypt the private key of the generated RSA private key
- SHA2 algorithm: This algorithm shall be implemented to calculate the hash value of every party code to be provided to every voter

1.1.6. Application security

Source code fortification: To prevent application related security threats such as SQL injection, Blind SQL injection, Cross-site-scripting, Phishing, Cross-site-request-forgery, Link injection, etc, the election system shall implement a source code fortification process prior to deployment. A rigorous testing of all source codes will be executed to identify and resolve badly coded source codes as well as those that contain hazardous characters. Additional measures such as filtering user inputs will also be implemented to prevent an attacker to input malicious parameters that could possible compromise the election application system. In addition, this process shall address all application threats mentioned in Open Web Application Security Project (OWASP) and Web Application Security Consortium (WASC).

Application firewall: to ensure that only authorized http methods are executed on the application level and hazardous methods are blocked. It employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration prevents the possibility of application level attacks such as XSS, SQL injection, CSRF, Link injection caused by badly coded source codes.

Application server hardening: A hardening process shall be implemented on the application server level. The hardening process shall involve the creation of a baseline for the security on all election application system. To effectively protect the application on the application server level, a solid and sophisticated security baseline for all application servers in the election system shall be implemented, that includes removing unnecessary services, disabling of default user, guest and admin accounts and to ensure that all accounts requires authentication and a strong password to access the application server

1.1.7. Logical access control

The proposed solution shall implement access controls to restrict access to election systems to authorized personnel only.

Role-Based Access Control and Separation of Duties: To control access to the election system and to prevent one person to hold a role to execute critical tasks, the election system shall implement Role-based access control. In RBC, the assignment of permission to perform a particular operation in the election system is meaningful, because the operations are granular with meaning within the election application. RBAC has been shown to be particularly well suited to separation of duties (SOD) requirements, which ensure that two or more people must be involved in authorizing critical operations. An underlying principle of SOD is that no individual shall be able to execute a breach of security through dual privilege. By extension, no person may hold a role that exercises election systems related tasks over another.

The same principle of access control applied to the election application shall be implemented to all other devices in the election infrastructure. Default systems administrator accounts shall not be used on a day-to-day operation instead a user account with configured rights and permission according to its role and tasks in the election system shall be provided, and no more, no less.

1.1.8. Physical security

In consideration of the existence of physical security threats that could compromise election data and the election system as a whole, Indra proposes a robust physical security implementation to prevent events or catastrophic events that could occur if a physical security breach is realized. This solution shall apply to any contractor or sub-contractor that will provide the co-location services for the election system.

- Physical security access control

  A physical security access control shall be implemented to restrict access to authorized personnel only. All access has to go through a procedure that involves approval from separate and authorized personnel. A description of the nature of the access shall be clearly defined and justified. An access control mechanism shall be installed on the entry point requiring the personnel to provide the applicable credential (Access card and PIN) needed before given access to the data center.

- Separation of duties

  Separate authorized personnel shall be required to analyze and review the access request and shall decide whether to approve or deny the request. These personnel must accompany the person inside the data center when possible and required and supervise all actions to be executed to ensure that only actions described in the access request are executed.

- Closed-Circuit TV (CCTV)

  A CCTV shall be implemented in all areas of the data center that will cover all areas of the data center to monitor entry and exit as well the activities of personnel inside the data center. A recording of the video shall be stored and kept for a certain span of time for future purposes.

- Logging mechanism

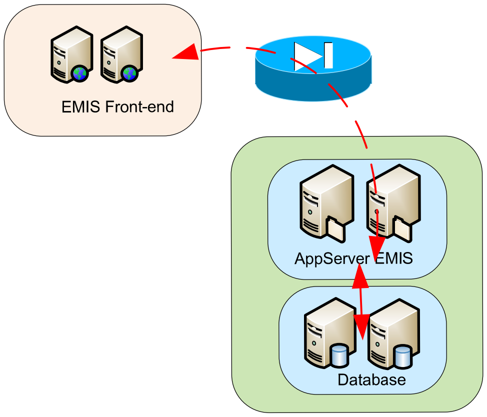
  A logging mechanism shall be implemented on all access to the data center. Indra proposes the combination of manual and automated logging procedures. Automated logging shall be done by the access control device while manual logging mechanism shall be implemented by the authorized personnel tasked to approve all data center access.

1.2. Election Administration Client. (EAC).

The election Administration clients are remote computer that need to connect to the EMIS portal in order to view/modify the election role before the election process.

1.3. Election Preparation Domain (EAD)

The election preparation domain is provided by the Application EMIS. These two servers gives the information needed to the webservers (front-end EMIS) and queries/store the information on the database servers.



1.4. Paper Voter Domain (PVD).

1.4.1. P-Votes Registration (Advance voters / Election Day) (PRD).

The polling station will have one or more computers checking the electoral role. This list of voters is located on a secure server in the datacenter, so we need to communicate those computers with the EMIS front-end servers in a secure way.

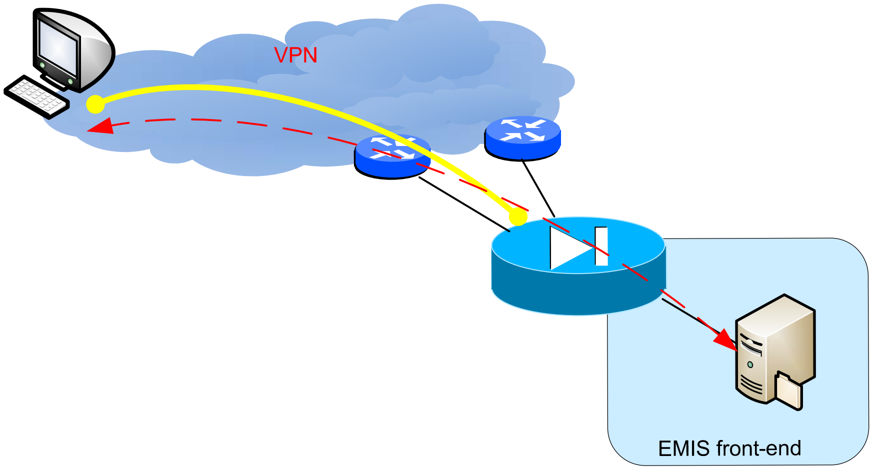
The EMIS front-end will not be published on Internet for security reasons. To access to this webservers each computer will have to establish a remote access VPN.

Each computer will have installed the Cisco VPN Client. The Cisco VPN Client is easy to configure on the client side and the security configuration can be pushed from the ASA firewall to the client when the tunnel is established (encryption, hashing…).

To connect to the datacenter is possible using the certificate on the smartcard, or using another certificate installed previously on the computer, or just providing a group/password credential.
Once the tunnel is stablished the computer will have access to the EMIS front-end. The webservers will ask for authentication to gain access to the application.

The security policy will be pushed to the computer from the firewall. No split tunneling will be configured. That means the computer will not be accessible from the Internet because all traffic will be redirected through the VPN. Any attempt to control this computer when connected to the EMIS front-end will be useless.

Once the traffic is decrypted, the firewall will only accept the allowed ports, discarding the rest of traffic.



1.4.2. E-counting

Once counting centers has the complete results, the information will then be send to the datacenter. A router Cisco 2801 will create a VPN (L2L) tunnel to connect both sides. The encryption can be changed as requested.

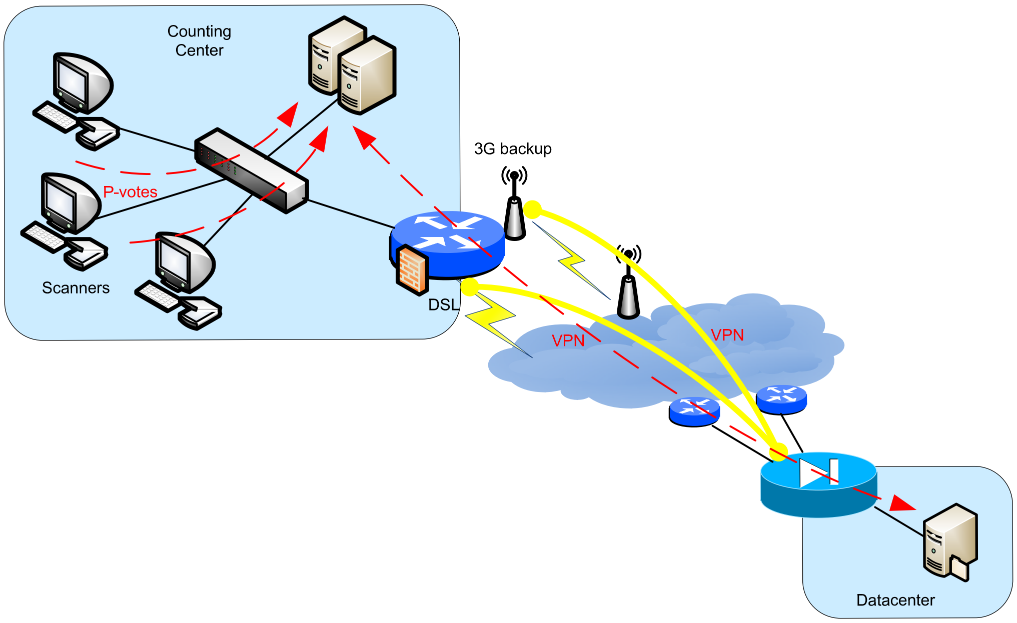
The router will have two HWICs to connect to Internet: one DSL interface card and one 3G interface card. Depending on the different kind of WAN lines of each counting center the interface card can be changed without problems.

The router will have a security IOS to create the tunnels. Firewalling (CBAC) will also be configured on this routers to protect the counting center from Internet, but we recommend to configure ACLs only allowing ESP and NAT-Traversal (if needed) between the datacenter and the counting center.
All the information exchanged between both sides will be encrypted and the integrity of each packet will be checked.

If we have one DSL access, the Cisco 2801 will try to connect to the datacenter through the DSL interface, but if it fails the 3G interface connection will be used.

The desired situation will be to have static IP addresses. This is something to negotiate with the service providers. If there`s no possibility to have static IP addresses on the WAN we can configure on the router easyVPN.

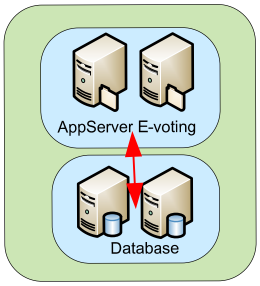
Finally the router will be secured and a security template will be applied: control plane, turn off services, ACLs…



Only the server of the counting center will have access to the datacenter. The firewalls will allow only desired ports after the decryption of the VPN.
There is a switch Cisco 2960 on the counting center. Security features will be applied on this switch: port secure, snooping, control plane, shutdown of empty ports…

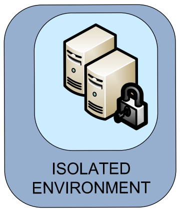
1.5. E-Voting Collection Domain (EVCD).

The E-voting collection domain is provided by the Application e-voting servers. These two servers shall store the information on the database servers



1.6. Election Setlement Domain (ELSD).

The Election Setlement Domain takes place in the isolated environment. This task is done by high processing performance severs.



2. Summary Table of Equipments

NETWORKING DEVICES

SWITHING

QTY	Reference	Descriptions
4	CISCO WS-C3750G-48TS-S	2 switches for the perimeter zone and MZ and 2 internal switches

FIREWALLING

QTY	Reference	Descriptions
2	CISCO ASA5540-BUN-K9	Active/passive perimeter firewall
2	JUNIPER NS-ISG-1000	Active/Passive internal firewall

DDOS Mitigation

QTY	Reference	Descriptions
1	Radware DefensePro 1016	DDOS Mitigation & IPS
1	Radware Insite Professional Security	Software to manage Radware devices and storage of attacks

HIPS - CSA

Number	Reference	Descriptions
1	Cisco Security Agents	Agent for Hardening the front-end servers. Management console

What's Up

QTY	Reference	Descriptions
1	What's Up Gold Standard - Up to 100 devices	Monitor Network Devices and Servers

Load Balancers

QTY	Reference	
2	F5-BIG-LTM-1600-4G-R	Internal Load Balancer for th webservers

Application Firewall

QTY	Reference	
1	F5-BIG-ASM-3600-4G-R	Application Firewall

NTP Appliance

QTY	Reference	
1	Symmetricon NTS-150	NTP server appliance

RACK

QTY	Reference	
3	DELL™ PowerEdge™ 4220 Rack (PE42201)	Racks, cables, connectivity and KVM switch

SERVERS

QTY	Reference	Descriptions
11	DELL PowerEdge R710 (SV3R710)	5 front-end Webservers + 2 servers to monitorization + 2 DNS servers + 2 Certificate Authorities
6	DELL PowerEdge 2970 (SV32971)	2 servers for the isolated environment + 2 application e-vote servers + 2 application EMIS servers
2	DELL PowerEdge R905 (PER9051)	2 servers for internal databases
		Cables, Backup Cartridges, Smartcards

COUNT SERVERS

NETWORKING

QTY	Reference	Descriptions
1	Switch Cisco 2960-24TT-L	Switch to connect servers, router and scanners
1	Router Cisco 2801 + DSL WAN + HWIC 3G	Router to connect trought VPN to the datacenter.

SERVERS

QTY	Reference	Descriptions
2	DELL PowerEdge R300 (SV3R3003)	Server to count votes (redundant solution)
1	Network Storage Dell PowerVault NX300	Store scanned votes

RACK

QTY	Reference	Descriptions
1	DELL™ PowerEdge™ 2420 Rack (PE24201)	Rack, cables and accesories
1	Avocent Console KVM + TFT - 15" + keyboard	
1	MGE UPS Systems 3000	UPS

IVR SYSTEM

QTY	Reference	Descriptions
1	Nortel MPS 500 (Rackmount)	IVR System for 60 simultaneous calls

LAPTOP (electoral role)

QTY	Reference	Descriptions
130	Novatech Xplora E16	Laptops to check electoral role

3. Detailed Specification of the equipments.

NETWORKING DEVICES

SWITHING

QTY	Reference	Descriptions
4	CISCO WS-C3750G-48TS-S	Cisco Catalyst 3750 48 10/100/1000T + 4 SFP + IPB Image
		The Cisco Catalyst 3750 v2 Series are next-generation energy-efficient Layer 3 Fast Ethernet stackable switches. These new switches support Cisco EnergyWise technology, which helps companies manage the power consumption of their network infrastructure and network-attached devices, thereby reducing their energy costs and carbon footprints.It increases productivity and provides investment protection by helping enable a unified network for data, voice, and video.
	Further information	http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html#

FIREWALLING

QTY	Reference	Descriptions
2	CISCO ASA5540-BUN-K9	ASA 5540 Appliance with SW, HA, 4GE+1FE, 3DES/AES
		Provides intelligent threat defense and secure communications services that stop attacks before they impact business continuity. The Cisco ASA 5500 series enables organizations to lower their deployment and operations costs while delivering comprehensive network security for networks of all sizes. Max firewall throughput: 650 Mbps, Max firewall conn: 400.000, Max firewall connections/second: 25.000, Packets per second (64 byte): 500.000, Max 3DES/AES VPN throughput: 325 Mbps, Max site-to-site and remote access VPN sessions: 5000
	Further information	http://www.cisco.com/en/US/products/ps6120/index.html
2	JUNIPER NS-ISG-1000	NS-ISG 1000 Advanced System, 4-10/100/1000 ports, Fan Tray, 0 I/O modules, AC
		The ISG1000 is a fully integrated FW/VPN/IDP system with multi-gigabit performance, a modular architecture and rich virtualization capabilities, delivering up to 2 Gbps of firewall throughput and up to 1 Gbps of optional integrated IDP throughput. The base FW/VPN system comes with four fixed 10/100/1000 interfaces and two additional I/O modules for interface expansion. Maximum Throughput: 2G FW, 1G 3DES/AES VPN, Max Number sessions: 500.000, Max number of VPN tunnels: 2.000

	Further information	http://www.juniper.net/us/en/products-services/security/isg-series/#products

DDOS Mitigation

QTY	Reference	Descriptions
1	Radware DefensePro 1016	DefensePro 1016 IPS & Behavioral Protection
		Radware's DefensePro is a real-time Intrusion Prevention System (IPS) that maintains your business continuity by protecting your IP infrastructure against existing and emerging network-based threats that can't be detected by traditional IPS' such as: application misuse threats, SSL attacks and VoIP service misuse. DefensePro OnDemand Switch 2S Models. DefensePro 1016 (up to 1Gbps). Designed for the protection of medium-sized data centers deployed by large enterprises, eCommerce and service providers.
	Further information	http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx
1	Radware Insite Professional Security	
		Insite is the management and monitoring tool for the APSolute family of application delivery, access and security solutions. It permits the set-up, configuration and management of all Radware products from one central console. As the central element for the entire APSolute™ product family, Insite provides immediate visibility to real-time APSolute OS Layer 3-7 health monitoring, session and deep-packet inspection information.
	Further information	http://www.radware.com/Products/Management/Insite.aspx

HIPS - CSA

Number	Reference	Descriptions
1	CSA-START-6.0-K9 + 5xCSA-SRVR-K9	CSA 6.0 Starter Kit [MC, 6 Server, and 10 Desktop Agents] + 5 Servers
		Cisco Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.
	Further information	http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

What's Up

QTY	Reference	Descriptions
1	What's Up Gold Standard - Up to 100 devices	
		Gives real-time visibility into how your network is performing, its underlying topology, and its dependencies. Alerts when things go wrong and you also want to reduce the number of problems, by developing proactive network management practices. WhatsUp Gold Standard is a cost-effective network management solution designed to monitor small and mid-sized business (SMB) networks and ensure stable growth in the future.
	Further information	http://www.whatsupgold.com/products/whatsup_gold_standard/index.aspx

Load Balancers

QTY	Reference	
2	F5-BIG-LTM-1600-4G-R	BIG-IP 1600 Local Traffic Manager (4 GB Memory)
		The BIG-IP Local Traffic Manager (LTM) is an application delivery networking system that provides the most intelligent and adaptable solution to secure, optimize, and deliver applications, enabling organizations to effectively and competitively run their business.
	Further information	http://www.f5.com/products/big-ip/product-modules/local-traffic-manager.html

Application Firewall

QTY	Reference	
1	F5-BIG-ASM-3600-4G-R	BIG-IP 3600 Application Security Manager (ASM) (4 GB Memory)
		BIG-IP Application Security Manager (ASM) delivers comprehensive protection for web applications while maintaining low total cost of ownership. BIG-IP ASM can help your organization quickly pass a security audit without requiring changes to the application code. It employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns.
	Further information	http://www.f5.com/products/big-ip/product-modules/application-security-manager.html

NTP Appliance

QTY	Reference	
1	NTS-150	Symmetricon NTS-150 NTP server appliance
		Symmetricom’s Stratum 1 level NTS-150 derives accurate time directly from the atomic clocks aboard the GPS satellite system. By using an integrated, 12-channel GPS receiver,every visible satellite can be tracked and used to maintain accurate and reliable time.
	Further information	http://www.symmetricom.com/media/files/downloads/product-datasheets/ds_nts_150.pdf

RACK

QTY	Reference	
3	**DELL™ PowerEdge™ 4220 Rack (PE42201)**	
		Dell PowerEdge 4220 42U Rack with Doors and Side Panels, 30 x PDU Power Cords different length, 32Amp PDU 230V, Shelf for 24U/42U Racks Kit, 1U LCD 17" flat-panel monitor with DELL rack rails, UK/Ireland touchpad KB and mouse combo PowerEdge 180AS Analogue 8 Port KVM Switch, 8x USB Server Interface Pod + Cables
	Further information	http://www.dell.com/content/topics/topic.aspx/us/segments/bsd/racks?c=us&cs=04&l=en&s=bsd

SERVERS

QTY	Reference	Descriptions
11	**DELL PowerEdge R710 (SV3R710)**	
		1 x Intel® Xeon® E5502, 1.86Ghz, 4M Cache, 4.86 GT/s QPI, 6GB Memory DDR3 1333MHz, 2 x 146GB, SAS 3.5-inch 15K RPM Additional Hard Drive, SAS 6iR Internal RAID Controller Card, High Output Power Supply Redundant (2 PSU) 870W, sliding ready rails with cable management arm, PowerVault RD1000 Internal Backup SATA Drive Bay for 2.5" Chassis, Red Hat Enterprise or Windows 2003 License included
		3 years Warranty - Next Bussiness Day
	Further information	http://www.dell.com/us/en/business/servers/rack_optimized/ct.aspx?refid=rack_optimized&s=bsd&cs=04
6	**DELL PowerEdge 2970 (SV32971)**	
		2 x Quad Core AMD Opteron 2378 2.4GHz 75W ACP, 16GB Memory for 2 CPUs DDR2 800MHz, DVD+/-RW Drive SATA, 3 x 146GB SAS 3.5-inch 15K RPM Hard Drive (Hot Plug), C6 - Motherboard SAS/SATA RAID5 PERC 6/i, Two Hot Plug Power Supplies for Redundancy, Rapid/Versa Rack Rails, Backup drive, Red Hat Enterprise License
		3 years Warranty - Next Bussiness Day
	Further information	http://www.dell.com/us/en/business/servers/rack_optimized/ct.aspx?refid=rack_optimized&s=bsd&cs=04
2	**DELL PowerEdge R905 (PER9051)**	
		4x Quad Core AMD Opteron 8347HE 1.9GHz, HT-1, 16Gb Memory for 2/4 CPUs DDR2 667Mhz, Internal SATA DVD-ROM, 300GB SAS 3.5-inch 15,000 rpm Hard Drive (hot-plug), RAID5 controller SAS PERC 6/i SAS, Redundant High Efficiency Power Supply Unit (2PSU), sliding ready rails, Backup SATA Drive, Red Hat Enterprise License included
		3 years Warranty - Next Bussiness Day
	Further information	http://www.dell.com/us/en/business/servers/rack_optimized/ct.aspx?refid=rack_optimized&s=bsd&cs=04
	Others	
		Cables, Backup Cartridges, Smartcards

Count Center

NETWORKING

QTY	Reference	Descriptions
1	**Switch Cisco 2960-24TT-L**	Switch 24 Ethernet 10/100 ports + 2 10/100/1000 uplinks, LAN Base IOS
		Cisco Catalyst 2960 Series Intelligent Ethernet Switches with LAN Base software enable entry-level networks to provide enhanced LAN services. This family of fixed-configuration, standalone, intelligent Ethernet devices provides desktop Fast Ethernet and Gigabit Ethernet connectivity.
	Further information	http://www.cisco.com/en/US/products/ps6406/index.html#
1	**Router Cisco 2801 + HWIC DSL WAN + HWIC 3G Wireless WAN for backup**	
		Integrated services router with AC power, 2FE, 4 Interface Card Slots, 2 PVDM slots, 2 AIMs, and Cisco IOS IP Security
		The ISR architecture of the Cisco 2800 Series provides the performance, availability, and reliability needed to scale mission-critical business applications in the most demanding environments.
	Further information	http://www.cisco.com/en/US/products/ps5854/index.html

SERVERS

QTY	Reference	Descriptions
2	DELL PowerEdge R300 (SV3R3003)	
		Dual Core Intel® Xeon® E3113, 3.0GHz, 6MB Cache, 1333MHz FSB, 4 GBB RAMM DDR2, 16x DVD SATA, Onboard SATA Controller, 250GB, SATA, 3.5-inch, 7.2K RPM Hard Drive, Sliding Rapid/Versa Rack Rails
		3 years Warranty - Next Bussiness Day
	Further information	http://www.dell.com/us/en/business/servers/rack_optimized/ct.aspx?refid=rack_optimized&s=bsd&cs=04
1	Network Storage Dell PowerVault NX300	
		Intel® Xeon® E5502, 1.86GHz, Perc6i, OB NIC, 3GB Mem, Sliding Ready Rails, 3 x 250Gb 7.2K SATA Hot Plug, Redundant Power Supply 500W
		3 years Warranty - Next Bussiness Day
	Further information	http://www.dell.com/us/en/business/storage/unifiedstor/ct.aspx?refid=unifiedstor&s=bsd&cs=04

RACK

QTY	Reference	Descriptions

1	**DELL™ PowerEdge™ 2420 Rack**	
		Dell PowerEdge 2420 24U Rack with Doors and Side Panels, Ground Ship, Rack Power Cord 220V (Kit), 10x PDU Power Cords C14-C13, 1.5m x 5 (Kit), 16Amp PDU, 230V, 13x Low Power Connections
	Further information	http://www.dell.com/content/topics/topic.aspx/us/segments/bsd/racks?c=us&cs=04&l=en&s=bsd
1	**MGE UPS Systems 3000**	
		MGE UPS Systems 3000 RT 3U - UPS - CA 100/120/160/184-284 V - 3000 VA 9 Ah
1	**Avocent LCD15 Rail Rack Console**	
		Avocent LCD15 Single-Rail Rack Console - Console KVM - TFT - 15" - 1024 x 768 - 1U

LAPTOP (electoral role)

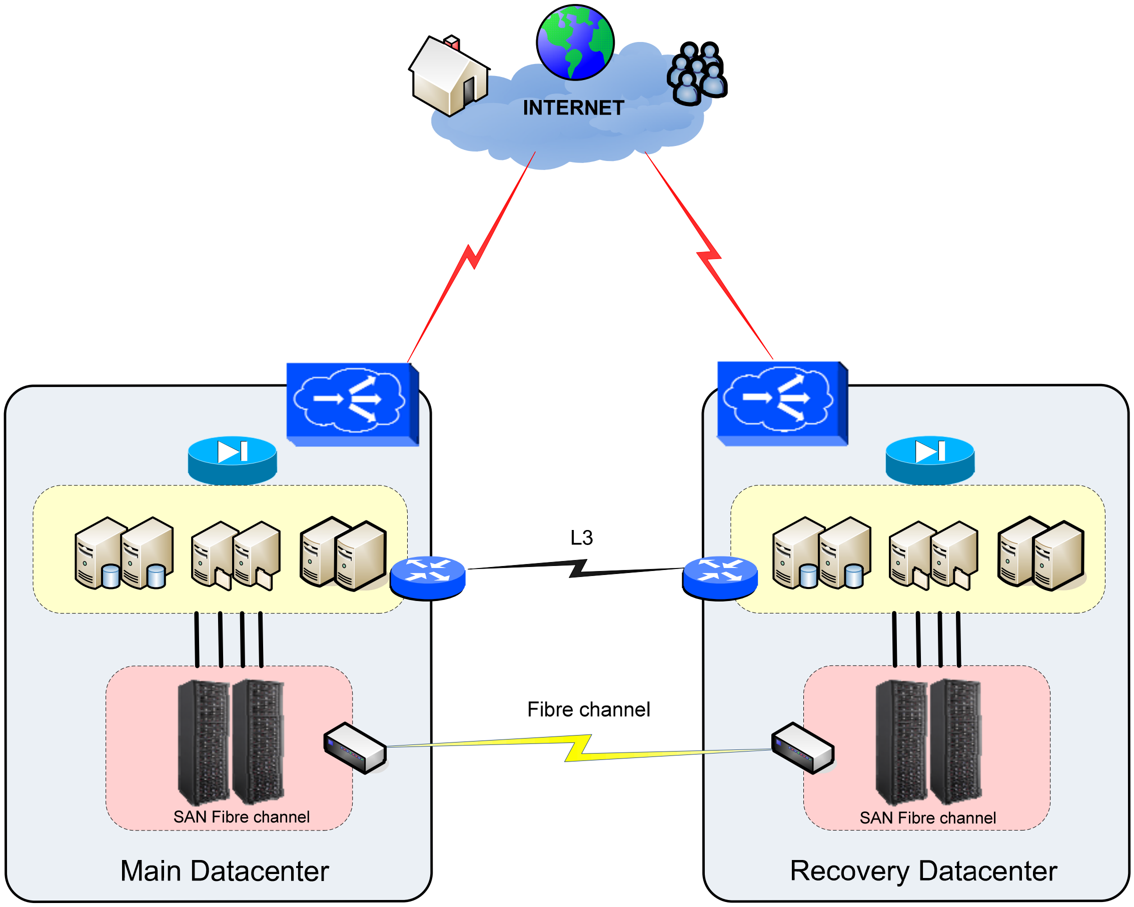
Number	Model	
130	**Novatech Xplora E16**	
		AMD TF20 1.6Ghz, 250Gb 2.5" SATA HDD, 2Gb DDR2 Memory, 8x SATA DVD Writer, Free Linux Distribution, USB External Smart Card
	Further information	http://www.novatech.co.uk/novatech/laptop/range/xplorae16.html

4. Considerations for full Implementation after 2011

This could be an approach for the full implementation after 2011.

The proposed solution has two datacenters. The datacenters can work in an active/active or active/passive configuration, as desired. To load balance the service is needed one Global Load Balancer in each datacenter. Basically those devices use Dynamic DNS resolutions to redirect the users to one datacenter (F5 BIG-IP 1600 Global Traffic Manager).

Internally both datacenters are routed through a L3 connection. This L3 communication can be encrypted with a router (high performance hardware encryption). Addicionally there is a Fibre Channel connection. The synchronization of the databases and applications of both datacenters will be via SAN Fibre channel.



Due to the amount of servers needed we recommend the use of a virtualization solution, as VMWare.

5. Other Requirements

5.1. Mandatory Constraints

Elaboration of Requirement MC2
Indra will fully comply with this requirement. In particular:

- The ownership of copyright for software components developed for the Customer will be transferred to the Customer
- Any software developed by Indra, including standard software, shall be open source.
- Indra will tem components must as a minimum be licensed to allow the Customer to make the source code available to the public and allow anyone to copy, modify, inspect, compile, debug and run the core for testing purposes.
  The following components may not be open source software for backup, monitoring or similar operational tasks, ICR/OCR-software.
- The operating system on which the system runs shall be licensed under a generally recognized open source license.

Elaboration of Requirement MC5
The system Indra will delivered for this project shall not have any closed source core components.

5.2. General Requirements

Elaboration of Requirement MC6
Please refer to section 2.1.8. “Physical security” of this Appendix.

Elaboration of Requirement GR 1.5
The system implements a local copy of the electoral roll in the computers installed at the polling stations (electronic poll books). In case of loss of communication the system works against the local copy. Once communications are restored the system automatically synchronizes with the central master copy thus ensuring integrity.

Some considerations about the operation in periods of loss of communication:

> In normal operation, the system prevents a voter casting two p-votes on election day since the voter is marked off in the electronic electoral roll (central server) when he casts the first p-vote. The only exception to this is the case of loss of communication with the central server (electronic electoral roll). In this case the voter is marked off in the local copy of electoral roll. In polling stations with several computers (electronic poll books), there is a theoretical possibility of a voter casting two p-votes when in this period of time.
>
> Since we do not recommend stopping the voting process during periods of loss of communication, we would recommend splitting the electoral roll in volumes and loading one volume per computer in the same way as the paper poll books are split in volumes (A to M and N to Z for instance). This way, voters that would want to cast a second p-vote have to go through the same computer where he was marked off the first time.

Indra would like to propose the following option: In the future when e-voting becomes the standard way of casting a vote and p-votes become residual, the Customer may want to assess the option of establishing that all p-votes on election day are cast in special envelopes to promote the concept of vote anywhere.

Elaboration of Requirement GR 3.6

Please refer to the Appendix 7 Total price and pricing provision for the full implementation software licenses costs