Electronic Voting Software

Security Target

EAL 4+

DOCUMENT HISTORY

Version	Date	Author	Comments
0.2	2010-04-10	Scytl R&D	Created Document.
0.7	2010-05-10	Scytl R&D	Draft version for review
0.8	2010-05-12	Scytl R&D	Completed version
0.9	2010-05-20	Scytl R&D	Version with development feedback.
1.0	2010-05-25	Scytl R&D	Reviewed version
1.1	2010-12-03	Scytl R&D	Reviewed version to include recent software changes.
1.2	2011-06-03	Scytl	Added disclaimer, and copyright and next version target
1.3	2011-06-16	Scytl R&D	Updated content, Disclaimer and next version target

DISCLAIMER: Some information in it this document might be obsolete, inaccurate or might be missing. Updates will be made if such discrepancies are found. This disclaimer will be also updated to reflect the state of the document.

NEXT VERSION TARGET DATE:

Version	Date	Author	Comments

QUALITY ASSURANCE:

Version	Date	QA responsible	Comments
1.1	22.03.2011	Markus Harboe	

APPROVAL

Approved by	Role	Sign	Date
Svein Endresen	Project Manager		22.03.2011
Svein Winje	Technical Architect		22.03.2011
Dan Sørensen	Customer		

1 E-Voting TOE

1.1 Security Target and TOE Identification

1.1.1 ST Reference

ST Title	Electronic Voting Software - Security Target
ST Version	1.3
ST Authors	Scytl I+D
ST Publish Date	2011-06-16

1.1.2 TOE Reference

TOE Name	Electronic Voting Software
TOE Version	1.2
TOE Developer	Scytl I+D
TOE Publish Date	2011-06-16

1.2 TOE Overview

This TOE overview defines the system component boundaries that will comprise the E-Voting Security Target. It also summarizes the usage and major security features of the TOE components. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

This TOE comprises the software product components designed to provide an E-Voting platform to conduct electronic elections over the Internet. The basic security functionalities that cover the different steps of the electronic election included in the TOE are:

- E-voting process configuration.
- Voter authentication.
- Vote casting.
- Vote reception and storage.
- Voting receipts generation, delivery, and verification.
- Generation of Return Codes that are used by the voters to ensure the correct registration of their votes.
- Vote counting and delivery of results.
- E-voting and e-counting process auditability.

The e-Voting platform provides a set of security features for the functionalities in order to provide a high reliability:

- Secure generation of cryptographic election parameters.
- Authentication of voters.
- Voter privacy.
- Vote integrity.
- Accuracy of the Election Results.
- Voter verifiability.
- E-voting audit methods.

1.2.1 TOE Environment

As the TOE is a software product, it relies on other external components (hardware and software) which are necessary for its final implementation: These components are:

Environment Component	Description
Physical Servers	Servers where the different TOE modules and the other operational environment components will be installed. These physical servers will require the TPM chip (Trusted Platform Module) to authenticate hardware devices.
Hardware Secure Module	HSM Cryptographic Device to store digital certificates and process digital signatures.
Operating system	CentOS linux - latest stable version. This operating system will need to support: - HSM device drivers. - TPM processor drivers.
Databases	Database PostgresSQL - latest stable version
Application Service	Glassfish Application Server - latest stable version.
Security Monitoring System	AIDE – Advanced Intrusion Detection Environment. Software to detect and monitor integrity of files and configurations.

Table 1: Operational Environment components

1.3 TOE Description

This section provides a description of the TOE, including the physical and logical boundaries of the TOE.

1.3.1 Evaluated Components of the TOE

This TOE comprises a group of components which set together form the e-Voting platform:

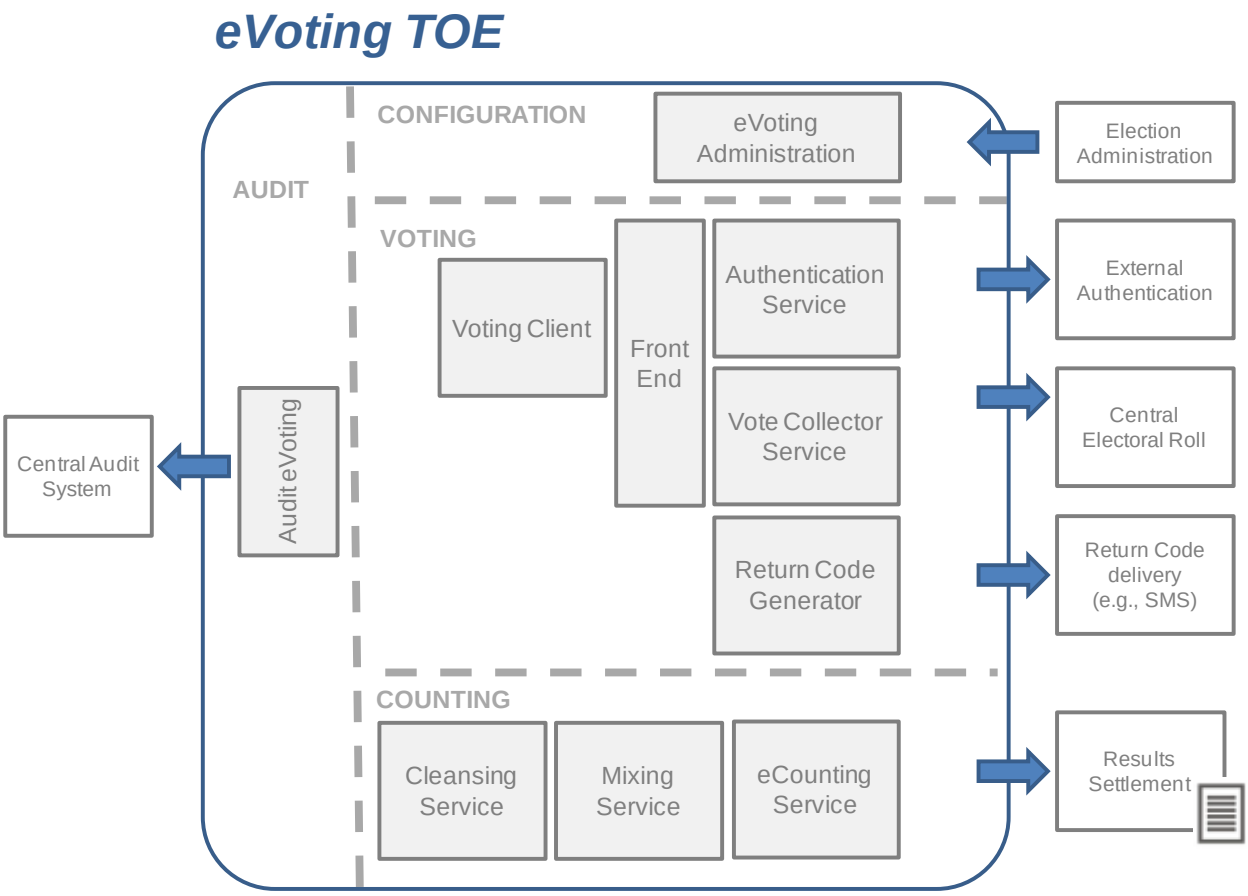

Figure 1: TOE Components

1.3.1.1 E-Voting Administration

The e-Voting Administration module of the TOE generates and certifies the cryptographic keys for other modules in the TOE, and generates the Return Codes printed in Voting Cards and delivered to each voter. This module interacts with the overall Election Administration module that is considered outside the boundaries of the e-Voting TOE. All the communications between the modules inside and outside the boundaries of the TOE are properly secured.

1.3.1.2 E-Voting Client

This is the module used by the voter to interact with the Voting System, where he/she is able to select the voting options.

This module performs the cryptographic operations on the voting terminal, in order to protect voter privacy and provide vote authentication: vote encryption and digital signature, including a timestamp that will be included in the Authentication Token generated by the Authentiaction Service.

It also connects to the Front End in a secured way, where it is redirected to the different services when required by the voting protocol: Authentication Service and Vote Collector Service.

1.3.1.3 E-Voting Front End

This module delivers the ballot templates to the voter browser and manages the connections from the Voting Client, redirecting them to the Authentication Service or to the Vote Collector Service.

1.3.1.4 Authentication Service

This module manages the authentication process of the e-Voting process, supporting the interaction with pre-existing voter authentication schemes and providing a key roaming mechanism to the voters in order to obtain digital certificates. To interact with pre-existing voter authentication mechanisms, the Authentication Service module communicates with any authentication module outside the TOE that will in practice perform the voter authentication (e.g., government CAI, or in-person authentication methods).

This module also interacts with an external Electoral Roll (voter database) for checking the voting status of the voters.

Information about the authenticated voters and security logs are generated in this module and delivered to the Audit eVoting module.

1.3.1.5 Vote Collector Service

The VCS module receives, verifies and stores the encrypted votes submitted by the voters. The votes are stored into a ballot box. The ballot box is signed at the end of the election by the VCS to ensure the box is not being tampered.

This module also generates log information that is delivered to the Audit eVoting module.

1.3.1.6 Return Code Generator

The RCG module calculates the Return Codes and interacts with a gateway outside the e-Voting TOE domain in order to send them through alternative channels not included in the TOE.

This module also generates the voting receipts which will be sent to the voting client to allow the verification that the votes have been processed as cast.

Information about the encrypted votes and security logs are generated in this module and delivered to the Audit eVoting module.

1.3.1.7 Cleansing service

This module validates the integrity of the votes stored in the VCS module and interacts with the centralized Electoral Roll (outside the TOE) in order to select the valid votes of each voter that will be processed by the Mixing module (just one vote is processed by each voter, prevailing paper votes over the electronic ones). Before exporting the votes to the Mixing module, the voter digital signatures are removed from the encrypted vote.

It also generates audit information that is delivered through an information device (CDROM, pendrive…) to the Audit eVoting module.

1.3.1.8 Mixing Service

The Mixing module performs the shuffling of the valid votes by using methods that enforce the voter's privacy and the vote integrity during the process. These methods generate audit data that is delivered to the Auditor in order to verify the correct mixing process.

1.3.1.9 eCounting Service

Implements the tallying process based on the votes shuffled by the Mixing module. This process decrypts the votes, generating cryptographic audit data that is delivered to the Auditor in order to verify the correct decryption process.

This module also counts the decrypted vote's content, and interacts with the Settlement component outside the TOE to provide to the external module the results of the count of e-votes.

1.3.1.10 Audit eVoting

The Audit eVoting module is in charge of the generation and protection of audit data related to the modules in the TOE (i.e. immutable logs), and also of the verification of this data. This module communicates with a central Audit module external to the TOE that manages and monitors the information from this specific Audit eVoting module and from others included in separated TOEs.

1.3.1.11 Excluded from the TOE

There are some modules of the overall election system which are not included in the TOE (and, therefore, not analyzed in this security analysis), but which TOE components interact with.

Although the security functionalities of these external modules are not covered by this document, the communications between modules inside/outside the TOE are always secured in such a way that the integrity of the transmitted information and the authenticity of the entities in the communication are ensured.

These External TOE Components are:

- Election Administration system.
- Centralized Electoral Roll.
- External SMS Gateway.
- External Authentication module.
- Settlement Service.
- Central Audit module.

1.4 TOE Boundaries

1.4.1 Physical Boundary

The TOE is a software-only TOE designed to fulfill electronic voting functionalities. This software is typically installed on several physical servers, which are not included in the TOE, as they are considered into the "Operational Environment".

Although these servers will require some protection measures, they have not been included into the TOE scope.

Thus there are no hardware components that come with the TOE.

1.4.2 Logical Boundary

The logical boundary of the TOE is described by its security functionalities:

1. Secure generation of cryptographic election parameters
2. Authentication of voters
3. Voter privacy
4. Vote integrity
5. Accuracy of the Election Results
6. Voter verifiability
7. E-voting audit methods

Secure generation of cryptographic election parameters

The cryptographic election parameters are generated in the e-Voting Administration module before the election process starts. Most of these parameters must be kept in secret, such as the cryptographic private keys for the modules in the TOE and the Return Codes for the voting cards assigned to the voters. Therefore, these parameters are generated in an isolated environment with a high restrictive access control.

Key generation: After the generation, the private keys belonging to the different modules in the TOE are securely deleted from the e-Voting Administration module (only stored encrypted, and memory is zeroized) and securely transported to the other modules in such

a way that the integrity of the keys, their confidentiality, and the authenticity of the sender (e-Voting Administration module) and the receiver (other modules in the TOE) are ensured. The module also provides Multi-Computation methods to generate critical keys in order to prevent them from existing for a while in this module.

Voting Card generation: Once the Return Codes are generated, the voting cards containing these Return Codes are printed and assigned to the voters that have to receive them in a secret way (i.e. printing the name of the voter in the envelope inside which there is the voting card with the Return Codes). After the printing, the Return Codes and their relationship with the voters are securely deleted from the e-Voting Administration module.

1.4.2.1 Authentication of voters

The TOE ensures that only votes from eligible voters are accepted in the system (in the Vote Collector Service module) checking the digital signatures attached to them and the Electoral Roll. Therefore, voters must have or are provided with digital certificates to be able to sign their votes. The Authentication module in the TOE provides interaction with pre-existing voter authentication schemes and providing a key roaming mechanism in order to ensure that all the eligible voters are able to cast votes with valid digital signatures. The Voting Client module (in charge of sending the vote to the VCS module on behalf the voter) and the VCS module have cryptographic methods implemented to sign the votes and verify these signatures respectively.

1.4.2.2 Voter privacy

The TOE guarantees that the voter privacy is maintained during all the voting process. Therefore, the identity of a voter is never connected with the non-encrypted content of his/her vote. The TOE preserves this privacy encrypting the vote in the Voting Client before it is digitally signed using a cryptosystem, the private key of which is kept in secret and divided in shares until the end of the election. Before the private key needed to decrypt the votes is reconstructed, the digital signatures are removed from the votes, which are shuffled in order to be anonymized before the decryption process.

1.4.2.3 Vote integrity

The digital signatures attached to the encrypted votes allow the verification of their integrity until the shuffling process is done in the mixing module. Moreover, the TOE ensures the integrity of the votes when they move from one module to another one (i.e. when they are collected from the VCS module and transmitted to the Cleansing module): the origin module digitally signs the set of votes, and the destination module verifies this signature. In the mixing module the integrity of the votes is proved generating security logs and audit data that are sent to the Audit e-Voting module to be further analyzed.

1.4.2.4 Accuracy of the Election Results

The accuracy of the election results is enforced by the TOE by means of:

- Integrity verification of the set of votes at each module.
- Verification of the correctness of the mixing/decryption process by generating and verifying audit evidences.

- Generation and verification of redundant data: following the protocol, the RCG module stores an integrity evidence of the votes stored in the VCS module.
- All the modules generate audit logs that can be verified.

Therefore, the TOE ensures that all the votes cast by eligible voters are counted in the final tally.

1.4.2.5 Voter verifiability

The voter verifiability in the TOE is divided in two functionalities:

Verify the correct registration of a vote: when a voter casts a vote, it is sent to the Vote Collector Service module and forwarded to the Return Code Generator module, which generates Return Codes from the vote and sends them to the voter. Only if the voting options received by the RCG module are the same that the ones the voter has selected, the Return Codes will match the proper options in the voter voting card. Since the Return Codes of a voting card are only known by the voter, and the private keys of the RCG module and of the VCS module are needed to generate them, an attacker cannot forge the Return Codes to cheat to the voter. Therefore, the voter can verify that the vote has been correctly received.

1.4.2.6 E-voting audit methods

The Audit e-Voting module receives security logs and audit data from the Vote Collector Service module, the Return Code Generator module, the Cleansing module and the Mixing module. The security logs register critical events in these modules and are chained in such a way that a log cannot be erased from the chain without being noticed. The verification of these security logs and the audit data received in the Audit e-Voting module guarantees that all the modules in the TOE have performed their operations correctly. Otherwise, the detection of possible attacks or failures is ensured.

2 Conformance Claim

The Security Target has been developed using the Common Criteria (CC) Version 3.1 R3 (Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of EAL4+.

This ST does not claim conformance to any PPs.

3 Security Problem Definition

3.1 Secure Usage Assumptions

Assumptions	Description
A. Authentication	It is assumed that a secure voter identification and authentication service will be provided by a trusted source (external identify provider, or in-person authentication method).
A. Physical	It is assumed that TOE servers are installed in a physically secure location that can only be accessed by authorized users.
A. Secure Installation and Operation	It is assumed that the TOE and its dependencies (E.g. operating system) are installed and managed in a secure way.
A. Timestamp	It is assumed that the TOE environment provides reliable synchronized time sources.
A. Trusted Administrator	It is assumed that the administrators are well trained and follow all administrator guidances.
A. MonitoringTask	Although the TOE generates logs for every critical action and security violations of the TOE, it is assumed that operators shall perform monitoring tasks, and they will be responsible for responding to security incidences and reporting them.
A. Contingency Plan	It is assumed that a documented plan is provided to maintain continuity of operation in an emergency or disaster.

Table 3-1: Secure usage assumptions

3.2 Threats

The asset under attack is the information transiting the TOE. In general, the threat agent is most likely people with TOE access (who are expected to possess average expertise, few resources and moderate motivation) or failure of the TOE or peripherals.

The following items detail threats in an enterprise network which the TOE is intended to address:

Threat Agent	Description
Voters	Citizens, users of the vote client software. Not high-technical knowledge is assumed.
Sysadmins	People with granted rights over the electoral domain systems (system administrators, operators administrators, or application administrators), and good technical knowledge.
Electoral Authorities / staff	People with granted rights over the application, responsible of the elections. Not high-technical knowledge is assumed.
Attacker / malware	Malicious network attackers with high-technical knowledge, who directly or through malware installed on client PC's (spywares, trojans, keyloggers, …), want to interfere at the election results or access to private information.
Auditors	External stakeholders who require demonstrating the reliability of the election process.
External	Other external entities (suppliers, regulations, ...)

Threats	Description
T1. Unauthorized voter	An unauthorized voter or a voter without the right to vote could try to cast a vote, affecting the election results.
T2. Compromise voter privacy	Identify the voters with their vote-options.
T3. Voter distrust	Social-Political problems, since the voter could have a negative feeling about the voting process.
T4. Voter Impersonation	One voter or an internal/external attacker could try to cast a vote as a different person.
T5. Coercion / selling / buying / intimidation (proof)	One person or organization could try to buy or demand a voter for specific vote options.
T6. Misuse in voting /Voter manipulation	Introduce fraudulent data in [casting the ballot] [during the ballot casting].
T7. Unauthorized Vote modification	Modification of the vote options from an authorized voter [or a valid vote?].
T8. Ballot stuffing	Add a fraudulent ballot into the ballot box.
T9. Vote deletion	Remove a right ballot from the ballot box.
T10. Ballot Box modification / deletion	Modify / delete the complete ballot box.
T11. Unauthorized election configuration change	Modification of the election parameters without the proper authorization.
T12. Logs modification / deletion	Alter or tamper the logs in order to hide an unauthorized action.
T13. Election boycott - denial of service	To “collapse the services” performing a denial of service attack.
T14. Non-authorized intermediate results.	To obtain partial or intermediate results, when it is not authorized.
T15. Anticipated election close.	To finish the voting process, and/or start the tallying process, after the official voting phase end.
T16. Lack of traceability	Not enough operations traceability or unverifiable operations.
T17. Legal requirements non-compliance	Non compliance with current official regulations (regarding data privacy, official procedures, …)
T18. SW / HW/ Supply error	External component errors could affect the availability of the TOE.

Table 3-2: Threats

I = Integrity; A = Availability; Au=Authenticity; T = Traceability; C = Confidentiality; Comp = Compliance

Threat Agent	Threat Description	Impact
Voters	**Unauthorized voter**. An unauthorized voter or a voter without the right to vote could cast a vote in order to manipulate the election result. He could tamper with the identification data in order to impersonate a voter with right to vote and to cast a vote on behalf of the authorized voter.	I
Voters	**Coercion / selling / buying / intimidation (proof)**. A voter with the right to vote uses data on his vote-casting device that are produced by the TOE during the voting phase to prove to a third party that he has voted in a certain way.	I

I = Integrity; A = Availability; Au=Authenticity; T = Traceability; C = Confidentiality; Comp = Compliance

Threat Agent	Threat Description	Impact
Voters	**Misuse in voting / Voter manipulation**. An authorized voter could try to introduce fraudulent data during ballot casting.	I
Voters	**Voter distrust**. An authorized voter could have a negative impression regarding the voting process, without being sure his/her vote has been processed correctly.	T
Sysadmins	**Unauthorized election configuration change**. A person with high-privileges over the system or application (administrator) could try to modify the election parameters without the proper authorization.	I
Sysadmins	**Compromise voter privacy**. A person with high-privileges over the system or application (administrator) could try to connect the voters with their vote-options.	C
Sysadmins	**Ballot Box modification / deletion**. A person with high-privileges over the system or application (administrator) could try to tamper the ballot box, altering the election results.	I
Sysadmins	**Ballot Stuffing**. A person with high-privileges over the system or application (administrator) could try to add votes directly to the ballot box.	I
Sysadmins	**Logs modification / deletion**. A person with high-privileges over the system or application (administrator) could try to tamper the logs in order to hide an unauthorized action.	T
Sysadmins	**Election boycott - denial of service**. A person with high-privileges over the system or application (administrator) could try to "collapse the services" performing a denial of service attack.	A
Sysadmins	**Non-authorized intermediate results**. A person with high-privileges over the application (administrator) could try to obtain intermediate results, when the voting phase is already in process.	I
Sysadmins	**Anticipated election closing**. A person with high-privileges over the application (administrator) could try to finish the voting phase, and/or start the tallying process, after the official voting phase end – cancelling the valid votes arriving after this fraudulent operation	A
Electoral Authorities / staff	**Compromise voter privacy**. Electoral officers or electoral staff could try to identify the vote options from a specific voter.	C
Electoral Authorities / staff	**Ballot Box modification / deletion**. A person from the electoral staff with high-privileges over the application could try to tamper the ballot box, altering the election results.	I
Electoral Authorities / staff	**Ballot stuffing**. A person from the Electoral officers or electoral staff with high-privileges over the application could try to add votes directly to the ballot box.	I

I = Integrity; A = Availability; Au=Authenticity; T = Traceability; C = Confidentiality; Comp = Compliance

Threat Agent	Threat Description	Impact
Electoral Authorities / staff	**Unauthorized election configuration change**. A person from the Electoral officers or electoral staff with high-privileges over the application could try to modify the election parameters without the proper authorization.	I
Electoral Authorities / staff	**Election boycott - denial of service**. A person from the Electoral officers or electoral staff with high-privileges over the application could try to "collapse the services" performing a denial of service attack.	A
Electoral Authorities / staff	**Non-authorized intermediate results**. A person from the Electoral officers or electoral staff with high-privileges over the application could try to obtain intermediate results, when the voting phase is already in process.	I
Electoral Authorities / staff	**Anticipated election closing**. A person from the Electoral officers or electoral staff with high-privileges over the application could try to finish the voting phase, and/or start the tallying process, after the official voting phase end – cancelling the valid votes arriving after this fraudulent operation.	I
Attacker / malware	**Compromise voter privacy**. An external attacker could try to identify the voting options selected by voters at the voting client, at the communications network, or at the ballot box.	C
Attacker / malware	**Unauthorized Vote modification**. An external attacker could try to modify the voting options selected by voters at the voting client, at the communications network, or at the ballot box.	I
Attacker / malware	**Vote deletion**. An external attacker could try to make null or delete the voting options selected by voters at the voting client, at the communications network, or at the ballot box.	I
Attacker / malware	**Voter Impersonation**. An external attacker could try to cast a ballot with the identity of a valid voter.	Au
Attacker / malware	**Ballot Stuffing**. An external attacker could try to add a ballot directly to the ballot box.	I
Attacker / malware	**Denial of service**. An external attacker could try to "collapse the services" performing a denial of service attack, at the client platform or at polling services.	A
Attacker / malware	**Logs modification / deletion**. An external attacker could try to tamper the logs in order to hide an unauthorized action.	T
Auditors	**Lack of traceability**. Auditors must observe full transparency at the process, and critical operations must be registered.	T
External	**Legal requirements non-compliance**. Image impacts due to non compliance with current electoral or data privacy laws.	Comp
External	**SW / HW /Supply error**. Externals errors at the software or hardware supporting TOE-software (non-TOE elements).	A

3.3 Organizational Security Policies (OSP)

The overall organizational security policies are tailored from E-vote 2011 Security Objectives defined by Norwegian ministry of local government and regional development.

Organizational Policies	Description
OSP-1. P.Audit	TOE must register every auditable event and collect audit records from the e-voting process. Audit records are protected from unauthorized access and do not pose any security risk of the voter anonymity.
OSP-2. P.Confidenciality	Vote options shall be secret, and nobody must be able to identify the voting options from a voter.
OSP-3. P.EndofElection	The inadvertent ending of the voting phase ahead of time shall be prevented. After the end of the voting phase, it is no longer possible to open or continue a new voting process; in particular it is no longer possible to cast a vote.
OSP-4. P.IntermediateResult	It shall be ensured that the election officers are not able to compute intermediate results.
OSP-5. P.NoCoercionPossible	The voting process shall ensure that the voter is not able to have a definitive proof about his vote decision.
OSP-6. P.OneVoterOneVote	It shall be ensured that only one vote is counted for each voter, and that non-registered voters shall not be able to cast a vote.
OSP-7. P.Tallying	The election officers cannot start the tallying until the voting phase has been ended. All vote records stored in the ballot box, after the end of the voting phase are correctly processed.
OSP-8. P. Least Privileges	User accounts shall be created and managed after the principle of least privilege.
OSP-9. P.Availability	The Polling Service shall be available to allow the voters to exercise his right-to-vote.
OSP-10. P.VoteIntegrity	The TOE shall protect the integrity of the votes, ensuring that ballots are unalterable all along the process (there is not possible to insert a non-valid ballot, and ballots are not modified or deleted).

Table 3-3: Organizational Security Policies

4 Security Objectives

4.1 Security Objectives for the TOE

This section defines the IT Security Objectives that are to be addressed by the TOE.

Security Objective	Description
OS1 - Effective Voter Registration Voting permission is only granted to those whose bona fides have been established.	A combination of procedural and technical measures to ensure that voters are properly identified before being granted permission to vote and that multiple and false identities cannot be registered.
OS2 - Effective Voter Authenticity E-voting services are only available to those eligible to vote.	Access to e-voting services can only be obtained on the presentation of properly constructed access credentials. Voter authentication will be provided by using an approved authentication scheme at a external authentication portal (MinID).
OS3 - Effective Voter Anonymity Neither during the voting process nor at the ballot count should the identity of the voter be disclosed.	A combination of technical and procedural measures to ensure that votes cannot be attributed to individuals either whilst they are voting or during the ballot count.
OS4 - Effective Vote Confidentiality E-voting services must guarantee the confidentiality of the vote.	A combination of technical, procedural and out of band measures to ensure that votes cannot be attributed to an individual candidate during the voting process. To reduce the effectiveness of coercion and vote selling in the Remote Electronic Voting context (REV), the following is proposed: • A voter should be able to change his or her vote an indefinite number of times in the e-voting period. • The REV-system shall not indicate to the voter if he/she has previously cast a ballot – electronic or on paper. • A voter may at any time cast a paper ballot in a polling station. This will invalidate any past or future electronic ballot. • Every vote receipts (counted or not) will be published after the electoral poll is finished.
OS5 – Effective System Identification and Authentication Accountable e-voting service processes are only accessible to those individuals and systems that have been authorized to access such processes.	A requirement for technical measures to ensure that access, to the Election Service Domain (ESD), can only be obtained on presentation of properly constructed access credentials
OS6 – Effective System Registration Access permission to e-voting service processes is only granted to those who bona fides have been established.	A combination of technical and procedural measures to ensure that users, within the ESD, are properly identified and authenticated, and can access only those parts of the system and assets necessary to perform the authorized task.

Security Objective	Description
OS7 – Effective System Access Control Access granted to e-voting service application and assets is the minimum necessary for the identified user to obtain services required.	Will map on to a requirement to ensure that a user/administrator within the ESD, once identified and authenticated, can access only those part of the system and assets necessary to perform the authorized task.
OS8 – Information Integrity Ensuring that the voter's intention is received as intended.	Information transmitted and received by the e-voting service must not be altered or otherwise subverted.
OS9 – Service Availability Continuing access to the e-voting service as and when required must be assured Fallback routines must be in place in case of unavailability of the e-voting system.	Users of the e-voting service must be able to depend on the continuing availability of the service in order for them to meet their obligation to vote – subject to limits imposed by the availability of the Public Network Domain (PND). Voters must not be turned away from a polling station in case of (temporary) service unavailability. The fallback should not disrupt the operation of the e-voting system once service is restored.
OS10 – Information Availability Continued access to e-voting data assets as and when required must be assured.	Data assets of the e-voting service are an important record and must not be lost through accidental, careless or deliberate acts of e-voting service users, or administrative staff, or in the event of equipment failure
OS11 – Service Protection The e-voting service implementation and associated assets must be protected from external interference and penetration.	The e-voting service must be adequately protected from outside attack mounted against the service application or the underlying network infrastructure
OS13 – Open Auditing and Accounting The e-voting service must keep a proper record of significant transactions	A general requirement for a proper record of significant events that may have to be revisited. This will include system configuration to enable external observers to determine that no collusion could have taken place
OS14 – System Disclosability/Openness The e-voting service must be open to external inspection.	This is a general requirement of the e-voting system. The system software, hardware, documentation, microcode, and any custom circuitry must be open for random inspection at any time.

Table 4-1: Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

This section defines the IT Security Objectives that are to be addressed by the Operational Environment of the TOE.

Security Objective for Environment	Description
OS12 – Operator Integrity Those operating and administering the e-voting service should be of an unquestionable record of behavior.	The personnel administering the e-voting services may be in an enhanced position to attack the system.

Table 4-2: Security Objectives for the Operational Environment

4.3 Security Objective Rationale for the TOE

4.3.1 Mapping of Security Objectives to threats and organizational security policies

The following table represents a mapping of the Threats and Organizational Security Policies to the Security Objectives defined in this ST. All Security Objectives for the Operational Environment are considered to be Secure Usage Assumptions.

	OS1 - Effective Voter Registration	OS2 - Effective Voter Authenticity	OS3 - Effective Voter Anonymity	OS4 - Effective Vote Confidentiality	OS5 – Effective System Identification and Authentication	OS6 – Effective System Registration	OS7 – Effective System Access Control	OS8 – Information Integrity	OS9 – Service Availability	OS10 – Information Availability	OS11 – Service Protection	OS12 – Operator Integrity	OS13 – Open Auditing and Accounting	OS14 – System Disclosability/Openness
OSP-1. P.Audit											X	X	X	X
OSP-2. P.Confidentiality			X	X										
OSP-3. P.EndofElection						X	X	X			X			
OSP-4. P.IntermediateResult						X	X	X			X			
OSP-5. P.NoCoercionPossible				X										
OSP-6. P.OneVoterOneVote	X	X												
OSP-7. P.Tallying						X	X	X			X			
OSP-8. P. Least Privileges					X	X	X				X	X		
OSP-9. P.Availability									X	X				
OSP-10. P.VoteIntegrity								X			X			
T1. Unauthorized voter	X	X										X		
T2. Compromise voter privacy			X	X							X			
T3. Voter distrust (proof)													X	X
T4. Voter Impersonation		X												X
T5. Coercion / selling / buying / intimidation (proof)				X										
T6. Misuse in voting / Vote manipulation								X			X			
T7. Unauthorized Vote modification								X			X			
T8. Ballot stuffing								X			X			
T9. Vote deletion								X			X			
T10. Ballot Box modification / deletion								X		X	X			
T11. Unauthorized election configuration change						X	X				X			
T12. Logs modification / deletion								X	X	X	X			
T13. Election boycott - denial of service									X	X	X			
T14. Non-authorized intermediate results.						X	X	X			X			
T15. Anticipated election closing						X	X	X			X			
T16. Lack of traceability									X	X		X	X	
T17. Legal requirements not compliance			X	X										
T18. SW / HW/ Supply error									X	X				

Table 4-3: Mapping of Security Objectives to threats and organizational security policies

4.3.2 Justification of Security Objectives to threats and OSPs

Each threat and OSP included in this ST is covered by the following Security Objectives as explained below.

OS1 - Effective Voter Registration	OSP-6. P.OneVoterOneVote T1. Unauthorized voter
	This security objective is covering the policy "**p.OneVoterOneVote**", since an effective voter registration is ensuring that only authorized voters are exercising their right-to-vote. A trusted platform (identity provider or in-person method) will be referenced for the voter identification, and the Electoral Roll will be consulted to ensure a voter is only granted to vote in contests that he is entitled to vote in. It also covers the threat **T1.UnauthorizedVoter** in a manner that the effective registration process will prevent unauthorized voters to start the voting process.

OS2 - Effective Voter Authenticity	OSP-6. P.OneVoterOneVote T1. Unauthorized voter T4. Voter Impersonation
	T1. Unauthorized voter and **T4. Voter Impersonation** are covered by the mechanisms provided by the authenticity verification process, which ensures that voters who are accessing to the voting platform are actually authorized voters. A trusted platform (identity provider or in-person method) will be referenced for the voter identification, which uses a double channel authentication method (user-password and sms-message in case of the identity provider, or personal identification and identity card in case of in-person authentication). In addition, a generated authentication token will be provided to protect from non-registered voters. Moreover, this security objective is covering the policy "**p.OneVoterOneVote**", since the authenticity verification mechanism is ensuring that only authorized voters are exercising their right-to-vote.

OS3 - Effective Voter Anonymity	OSP-2. P.Confidentiality T2. Compromise voter privacy T17. Legal requirements not compliance
	This security objective addresses the threat "**T2. Compromise voter privacy**" and the policy "**OSP-2. P.Confidentiality**". Ensuring the voter anonymity through cryptographic methods and securing the communications lines, will allow the voter privacy to be maintained. In addition, "**T17.Legal requirements not compliance**" is covered, since legal requirements - regarding data privacy – must be considered and implemented.

OS4 - Effective Vote Confidentiality	OSP-2. P.Confidentiality OSP-5. P.NoCoercionPossible T2. Compromise voter privacy T5. Coercion / selling / buying / intimidation (proof) T17. Legal requirements not compliance
	"**T2. Compromise voter privacy**" and "**OSP-2. P.Confidentiality**" are covered by controls in place to ensure that votes cannot be attributed to individual candidates. Votes are encrypted from the vote casting process (in the voter PC) until the counting process.

	Communication lines are also encrypted. Coercion and vote selling are also specifically addressed by this security objective ("**OSP-5. P.NoCoercionPossible**" and "**T5. Coercion / selling / buying / intimidation (proof)**"). A voter will be able to cast a vote an indefinite number of times, without indicating if a ballot has been casted previously, accepting paper votes too. In addition, "**T17.Legal requirements not compliance**" is covered, since legal requirements - regarding data privacy – must be considered and implemented.

OS5 – Effective System Identification and Authentication	OSP-8. P. Least Privileges
	An Effective System Access Control (from the election administration software) will be in place with a password-based authentication mechanism, in order to ensure only authorized users are accessing to the application. Users shall be granted based on the policy "**OSP-8. P. Least Privileges**".

OS6 – Effective System Registration	OSP-8. P. Least Privileges OSP-3. P.EndofElection OSP-4. P.IntermediateResult OSP-7. P.Tallying T11. Unauthorized election configuration change T14. Non-authorized intermediate results. T15. Anticipated election closing.
	An Effective System Access Control (from the election administration software) will be in place with a password-based authentication mechanism. One the user has been identified, a role-based Access Control will be in place to ensure users have only granted rights to those functions they need to perform the authorized tasks. These mechanisms will prevent the election from threats related to the election management and tallying process (**T11.Unauthorized election configuration change**, **T14. Non-authorized intermediate results, T15. Anticipated election closing**, **OSP-3. P.EndofElection, OSP-4. P.IntermediateResult, OSP-7. P.Tallying**).

OS7 – Effective System Access Control	OSP-8. P. Least Privileges OSP-3. P.EndofElection OSP-4. P.IntermediateResult OSP-7. P.Tallying T11. Unauthorized election configuration change T14. Non-authorized intermediate results. T15. Anticipated election closing.
	A role-based Access Control will be in place to ensure users have only granted rights to those functions they need to perform the authorized tasks. This mechanism will prevent the election from threats related to the election management and tallying process (**T11.Unauthorized election configuration change**, **T14. Non-authorized intermediate results, T15. Anticipated election closing**, **OSP-3. P.EndofElection, OSP-4. P.IntermediateResult, OSP-7. P.Tallying**).

OS8 – Information Integrity	OSP-3. P.EndofElection OSP-4. P.IntermediateResult OSP-7. P.Tallying OSP-10. P.VoteIntegrity T6. Misuse in voting / Vote manipulation T7. Unauthorized Vote modification T8. Ballot stuffing T9. Vote deletion T10. Ballot Box modification / deletion T12. Logs modification / deletion T14. Non-authorized intermediate results. T15. Anticipated election closing.
	Information integrity will be protected from the following points of view: - The vote digital signature and vote encryption will prevent malicious software from manipulation of votes (**T7. Unauthorized Vote modification, T8. Ballot stuffing, T9. Vote deletion,** and **T10. Ballot Box modification / deletion**). - Voter client software will be designed and developed to prevent "**T6. Misuse in voting / Vote manipulation**". - Additional controls are performed at the Vote Collector Server, regarding vote integrity. - The "Immutable Logs" implemented mechanism, will also detect the modification or deletion of log files ("**T12. Logs modification / deletion**"). - The integrity of the process will be assured by the operations flow, in order to prevent intermediate results counting, or anticipated election finish (**T14. Non-authorized intermediate results, T15. Anticipated election closing**, **OSP-3. P.EndofElection, OSP-4. P.IntermediateResult, OSP-7. P.Tallying**).

OS9 – Service Availability	OSP-9. P.Availability T13. Election boycott - denial of service T16. Lack of traceability T18. SW / HW/ Supply error
	After detected malfunctions of the application (due to "**T13. Election boycott - denial of service**" or "**T18. SW / HW/ Supply error**") the application will be able to enter in a secured maintenance mode, with manual methods to return to a secure state. The service availability objective covers the threat "**T13. Election boycott - denial of service**" in a preventive manner also, with configurations which are detecting DoS attacks. In addition, the availability of the log files shall be ensured too, covering the threat "**T16. Lack of traceability**".

OS10 – Information Availability	OSP-9. P.Availability T10. Ballot Box modification / deletion T12. Logs modification / deletion T13. Election boycott - denial of service T16. Lack of traceability T18. SW / HW/ Supply error
	The security objective "**OS10 – Information Availability**" addresses the threats related to data deletion (**T10. Ballot Box modification / deletion, T12. Logs modification / deletion**) including log files deletion (**T16. Lack of traceability**). Data will be monitored and backed-up, in order to prevent data loss. Moreover, threats related to service availability have also been addressed (**T13. Election boycott - denial of service, T18. SW / HW/ Supply error**), as the information availability is included in the service availability procedures and controls.

OS11 – Service Protection	OSP-3. P.EndofElection OSP-4. P.IntermediateResult OSP-7. P.Tallying OSP-8. P. Least Privileges OSP-10. P.VoteIntegrity T2. Compromise voter privacy T6. Misuse in voting / Vote manipulation T7. Unauthorized Vote modification T8. Ballot stuffing T9. Vote deletion T10. Ballot Box modification / deletion T11. Unauthorized election configuration change T12. Logs modification / deletion T13. Election boycott - denial of service T14. Non-authorized intermediate results. T15. Anticipated election closing.
	The Security Objective "**Service Protection"** is covering all threats related to the integrity of the configuration / voting / tallying processes, information integrity (which could affect to the election results) and the voters' privacy.

OS13 – Open Auditing and Accounting	OSP-1. P.Audit T3. Voter distrusts (proof) T16. Lack of traceability
	Open Auditing and Accounting covers "**OSP-1.P.Audit"** and "**T16. Lack of traceability**" with the implementation of detailed application logs registering every important action performed by voters, administrators, and operations performed by the application. Log files are protected with the "Immutable logs" mechanism, which ensures that any log modification or deletion is detected. In addition, the traces or vote-records registered by the application which are sent to the user would prevent occurrence of the threat "**T3. Voter distrusts (proof)** ", since the voter will receive return-codes (by SMS) that ensure the correct reception of the vote.

OS14 – System Disclosability/Openness	OSP-1. P.Audit T3. Voter distrusts (proof)
	The electronic voting software is open for random inspection. In addition, the application openness would minimize the impact regarding the threat "**T4. Voter distrusts (proof)**".

4.4 Security Objective Rationale for the Operational Environment

4.4.1 Justification of Operational Environment Security Objectives and assumptions

TOE software has some security dependencies on the technological environment which are supporting the Electronic Voting Software.

An operational Environment Security Objective has been established, in order to ensure that the operation and administration tasks of the operational environment are performed as an unquestionable record of behavior.

This is a really important objective, since the personnel administering the operational environment may be in an enhanced position to attack the system.

Related to this operational objective, several assumptions have been defined, which are not covered by TOE - technological controls:

- Authentication – External authentication service.
- Physical – Physical Security.
- Secure Installation and Operation.
- Timestamp - Right timestamp configuration.
- Trusted Administrator – Servers are properly administrated.
- Monitoring Task – Monitoring tasks performed by operators.
- Contingency Plan – A documented Contingency Plan exists.

5 Security Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are taken from part 2 of the CC.

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [*detailed*] level of audit; and c) Voting transactions, vote checking results, integrity checking results, application user login attempts (successful and unsuccessful), operators and application administrators' activities. d) Process results from cleansing process, mixing process, and counting process.
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [related object identification, session id, IP address or other location information from the user or system which generates the event].

5.1.1.2 FAU_GEN.2 User identity association

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [system administrators, security operators, auditors] with the capability to read [FAU_GEN.1.1 generated audit] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_STG.1 Protected audit trail storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to [*detect*] unauthorised modifications to the stored audit records in the audit trail.

5.1.2 Class FCO: Communication

FCO_NRO.2 Enforced proof of origin

Hierarchical to:	FCO_NRO.1 Selective proof of origin
Dependencies:	FIA_UID.1 Timing of identification
FCO_NRO.2.1	The TSF shall **enforce the generation of** evidence of origin for transmitted [electronic votes, election configuration information, and voting receipts] at **all times.**
FCO_NRO.2.2	The TSF shall be able to relate the [digital certificate information, date and time, identification code] of the originator of the information, and the [vote id or object id] of the information to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [*recipient*] given [its digital signature].

5.1.2.1 FCO_NRR.2 Enforced proof of receipt

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FCO_NRR.2.1	The TSF shall be enforce the generation of evidence of receipt for received [*electronic votes*] at all times.
FCO_NRR.2.2	The TSF shall be able to relate the [identity] of the recipient of the information, and the [digital signature] of the information to which the evidence applies.
FCO_NRR.2.3A	The TSF shall provide a capability to verify the evidence of receipt of information to [*the voter*] given [*the return codes calculated at RCG service*].
FCO_NRR.2.3B	The TSF shall provide a capability to verify the evidence of receipt of information to [*the voting client*] given [*the voting receipts generated at RCG service*].
FCO_NRR.2.3C	The TSF shall provide a capability to verify the evidence of receipt of information to [*the VCS*] given [*the voting receipts generated at RCG service*].

5.1.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] , FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA key generation algorithm*] and specified cryptographic key sizes [*minimum key size equivalent to a symmetric key of 100 bits (FNISA (French Network and Information Security Agency) Recommendations 2010)*] that meet the following: [*according to the standard FIPS 140-2, the RSA key generation algorithm follows the specifications in FIPS 186-3*].

5.1.3.1 FCS_CKM.2 Cryptographic key distribution

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method: [*private keys are encrypted when they are entered in or output from a specific module*] that meets the following: [*FIPS 140-2*].

5.1.3.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*methods for key zeroization*] that meets the following: [*FIPS 140-2*].

5.1.3.3 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] , FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1.1	The TSF shall perform [*digital signature and verification functions; digest functions; message authentication functions*] in accordance with a specified cryptographic algorithm [***digital signature and verification**: RSA; **hash algorithm**: SHA-256; **message authentication:** HMAC*] and cryptographic key sizes [***RSA:** minimum key size equivalent to a symmetric key of 100 bits (FNISA (French Network and Information Security Agency) Recommendations 2010); **HMAC:** minimum key size 128 bits*] that meet the following: **[***according to the standard FIPS 140-2, we follow the specifications for each cryptographic operation: **digital signature and verification**: specifications in PKCS#1 v2.1 for the RSA digital signature and verification (RSASSA-PSS); **hash algorithm**: specifications in FIPS 180-3 ; **message authentication:** specifications in*

FIPS 198a for HMAC function in combination with SHA-256 hash function].

5.1.4 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1A	The TSF shall enforce the [*voter identification through an external and (non-TOE) identity provider*] on [the voting client].
FDP_ACC.1B	The TSF shall enforce the [*election staff identification through a non-TOE user & password identity service*] on [eVoting *administration application, for administrators, operators, and auditors*].

5.1.4.1 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control.
FDP_ACF.1A.1	The TSF shall enforce the [*voter access control through an external (non-TOE) identity provider*] to objects based on the following: [*electoral roll (user authorization for voting, authorized election contest), and election period date and time*].
FDP_ACF.1A.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*if the voter is authorized to vote in the selected contest, and the election period is opened*].
FDP_ACF.1A.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no rules*].
FDP_ACF.1A.4	The TSF shall explicitly deny access of subjects to objects based on the [*access by a voter without the proper authorization*].
FDP_ACF.1B.1	The TSF shall enforce the [*election staff access control through a non-TOE user & password identity service*] to objects based on the following: [*user role permissions over the system, user role assignment to the users*].

FDP_ACF.1B.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*if the user role has been explicitly granted access to the objects*].
FDP_ACF.1B.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*no rules*].
FDP_ACF.1B.4	The TSF shall explicitly deny access of subjects to objects based on the [*access to files, data, functions, or applications that are not permitted to their roles profile assignment, shall be denied*].

5.1.4.2 FDP_DAU.2 Data Authentication with Identity of Guarantor

Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [*electronic votes, election configurations, and application logs*].
FDP_DAU.2.2	The TSF shall provide [*electronic voting services (Authentication Service, VCS, RCG, cleansing service, mixing service, and counting service*] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

5.1.4.3 FDP_ETC.2 Export of user data with security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.2.1	The TSF shall enforce the [authorization through authentication credentials] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE:

- *[Rule 1]: The Ballot Box from the VCS, and voting receipts from the RCG, cannot be exported until election has finished.*
- *[Rule 2] (Ballot Box) Encrypted data – votes – is exported encrypted from the VCS.*
- *[Rule 3]: Any exported data must be digitally signed before be exported (Ballot box from the VCS, voting receipts from the RCG, cleansed ballot box from the cleansing service, mixed ballot box from the mixing service, and counting of e-votes fom the counting service).*
- *[Rule 4] In any case, data must be exported completely or otherwise is not exported – no partial exports.*

5.1.4.4 FDP_IFC.1A Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1.A The TSF shall enforce the [*SFP for election management*]

on the *following subjects, information, and controlled operations:*

- *Subject: Electoral Officers.*
- *Information: Election configurations, cryptographic keys, voting cards.*
- *Controlled operations: Election configuration management, electoral period opening and closing process, electoral administration activities, cryptographic keys generation and management, voting cards generation.*

The SFP for election management shall adhere to the following security principles:

- *The controlled operations shall only be executed if they are specifically authorized, according to the defined segregation of duties rules.*

- *Election configuration, cryptographic keys, and voting cards, shall be created before the voting process starts.*
- *Cryptographic Keys and Election Configuration information must be distributed digitally signed by a trusted entity, using a distribution method which ensures the proper delivery to the right receptor.*
- *No operations can be performed once the election period has finished.*

5.1.4.5 FDP_IFF.1A Simple security attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control initialization.
FDP_IFF.1A.1	The TSF shall enforce the [*SFP for election management*] based on the following types of subject and information security attributes: [*Authenticated users, user rights definition and digital signatures*].
FDP_IFF.1A.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: • *[Rule 1] User-Roles administration shall be implemented to allow defining the roles, with a proper segregation of duties rules which ensure that critical operations cannot be executed in an unauthorized manner* • *[Rule 2] If the configuration management process is interrupted while running, the configuration management operation shall be rolled-back and the officer shall be informed about that issue.*
FDP_IFF.1A.3	The TSF shall enforce the following additional SFP rule: • *[Rule 3] Election configuration, cryptographic keys, and voting cards, shall be digitally signed by a proper authorized entity, and this digital signature must be validated before any of this information is processed.*
FDP_IFF.1A.4	The TSF shall explicitly authorize an information flow based on the following rule:

- *[Rule 4] Authorized Operations requested by the appropriate election officer, according to the defined user-roles.*

FDP_IFF.1A.5 The TSF shall explicitly deny an information flow based on the following rule:

- *[Rule 5] Any file which digital signature is not properly verified.*

5.1.4.6 FDP_IFC.1B Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1.B The TSF shall enforce the [*SFP for voting process*]

on the *following subjects, information, and controlled operations:*

- *Subject: Voter.*
- *Information: Identification data, Encrypted vote record, digital signature, vote authentication token, timestamp.*
- *Controlled operations: Identification, Authentication, voting, vote checking, voting receipt generation, return code generation.*

The SFP for voting process shall adhere to the following security principles:

- *The identification and authentication operations can be executed before the election starts, in order to allow the voter verify the contests she is eligible to vote; but the other controlled operations shall only be executed during the voting phase;*
- *The vote casting operation shall only be executed after the identification and authentication operations performed at the external (non-TOE) trusted platform for authentication (MinID in-person Issuing points…); these services will generate a voter authentication token (digitally signed by the expeditor).*
- *Once the voter has been identified by the external identity service, the following operations will be performed at the authentication service:*

- *The digital signature from voter authentication token will be checked.*
- *The voter authentication token has not been used yet (reviewing a used token list).*
- *The non-TOE electoral roll will be reviewed to ensure that the voter is able to vote in the contests that he is entitled to vote in.*
- *The election process shall be open to allow the voter cast a vote.*

- *Vote records sent by the voter must be checked by the Vote Collector Service – VCS before the vote accepting, at the following terms:*
  - *Not reused voter authentication token (reviewing a used token list).*
  - *Voter authentication token is properly assigned to the voter casting the ballot.*
  - *Authorized vote digital signature.*
  - *Electoral roll verification (the voter is entitled to vote for the contest for which he is voting).*
  - *Adequate timestamp: not in the future and not after the expiration time.*
- *Once the VCS verified the vote, the ballot must be sent to the RCG Service – to obtain a voting receipt back. The VCS shall be waiting for the voting receipt (with a configured timeout) otherwise the process shall be repeated until the vote receipt is back or the maximum number of repetitions (predefined) has been reached.*
- *When the Return Code Generator Service receives the ballot from the VCS, it shall check if the ballot has been already processed. If not, the ballot shall be verified and the vote receipt shall be created, stored, and sent to the VCS.*

- *The RCG Service must generate and send the Returns Codes just after the vote receipt has been sent to the VCS.*
- *Vote records shall only be stored in the ballot box during the voting phase;*
- *The voters will be able to vote as many times as they want, and they will receive the related return codes for each vote.*
- *The voting receipt generated by the RCG will not be shown to the Voter, but it will be verified by the voting client to ensure the vote has been properly processed.*
- *The voter will never have access to modify or delete his vote, once it has been processed and stored in the ballot box.*

5.1.4.7 FDP_IFF.1B Simple security attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control.
FDP_IFF.1B.1	The TSF shall enforce the [*SFP for voting process*] based on the following types of subject and information security attributes: [*Authenticated Voters, voting process attributes, and election period*].
FDP_IFF.1B.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: • *[Rule 1] The voter may identify and authenticate herself at the external (non-TOE) identification service. The vote authentication token generated by this service, will be checked by the TOE authentication service – reviewing its digital signature and a used token list.* • *[Rule 2] The non-TOE electoral roll shall be checked in order to ensure the authenticated voter has the right-to-vote property, and the contest for which he/she is entitled to vote in; otherwise, if the voter is not included into the electoral roll, he/she shall not be able to cast a vote. Also the election period shall be reviewed*

to ensure it is opened. These checks must be performed on authentication process, and when the vote is being cast.

- *[Rule 3] By selecting voting options, the voter may make his voting decision and initiate the vote casting, if the voter has been successfully authenticated. Voting options shall be accompanied by a voter authentication token (delivered by the authentication process).*
- *[Rule 4] The voter will be asked for confirming his voting options, and signing and sending the ballot. Once the ballot has been sent, the voter cannot revoke his vote.*
- *[Rule 5] The voting receipt and the return codes will be generated and sent, only if the ballot has been accepted.*
- *[Rule 6] If the process is interrupted once the return codes have been sent, but before the ballot has been stored, the voter shall be notified about that issue and the voting receipt is not sent.*

FDP_IFF.1B.3 The TSF shall enforce the following additional SFP rule:

- *[Rule 7] The VCS and RCG service will perform different checks regarding vote information, voter authentication token, digital signature verification, electoral roll verification, and vote integrity. If any of the checks is not successful, the vote will not be accepted (and consequently, voting receipt and return codes will not be sent).*

FDP_IFF.1B.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1B.5 The TSF shall explicitly deny an information flow based on the following rules: [*non-authenticated users, authenticated users not included into the electoral roll or any votes cast outside of the voting period*].

5.1.4.8 FDP_IFC.1C Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1.C

The TSF shall enforce the [*SFP for tallying process*]

on the *following subjects, information, and controlled operations:*

- *Subject: electoral officers, auditors.*
- *Information: Ballot Box, voting receipts, election results, election intermediate results, application logs.*
- *Controlled operations: Starting the tallying process, cleansing process, mixing process (includes auditing), counting process, determining the electoral result.*

The SFP for tallying process shall adhere to the following security principles:

- *The controlled operations shall only be executed if the appropriate election officer is authorized to execute them, according to the defined user-roles (and segregation of duties rules).*
- *No information flow between the election officer and the content of the ballot box shall induce that vote records are stored or stored records are changed or deleted;*
- *No information flow between the election officer and the content of the ballot box shall induce that intermediate results are directly, i.e. by tallying, or indirectly, i.e. by disclosure of the content of stored vote records, calculated;*
- *The following operations flow is mandatory and unique, and it cannot be executed in a different order, with jumps, or activities repetition:*
    - *Voting process closing.*
    - *Tallying phase start.*
    - *Cleansing process.*
        - *Vote filtering.*
        - *Vote selection.*
        - *Removal of digital signatures.*
    - *Mixing process (including Mixing Audit process).*

- *Counting process.*
  - *Vote decryption.*
  - *Vote counting.*
- *Results determining.*
- *Tallying phase end.*

Just the following exceptions can be considered.

- *A controlled and managed error could affect the process by stopping it.*
- *Cleansing and Mixing processes can be repeated for a ballot box – only if vote decryption has not been started – to allow tallying process coordination with paper voting.*
- *Mixing process can be decoupled in multiple independent Mixing processes based on subsets of votes (e.g., votes grouped by voting districts). In this case each Mixing process behaves independently from the others.*

- *At the beginning of each process execution inside the specified operations flow, a check will be performed to ensure the received information has been digitally signed with the proper digital certificate, and at the end of the process the generated information will be digitally signed.*

5.1.4.9 FDP_IFF.1C Simple security attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control.
FDP_IFF.1C.1	The TSF shall enforce the [*SFP for tallying process*] based on the following types of subject and information security attributes: [*Authenticated users, user rights definition, activities flow order*].
FDP_IFF.1C.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- *[Rule 1] User-Roles definition shall provide the capability to assign the roles in a manner that allows a proper segregation of duties rules, which ensure that critical operations cannot be executed in an unauthorized manner.*
- *[Rule 2] One user with auditor role shall be authenticated to introduce the data which will be used to validate the mixing process. This user shall check the accuracy of the mixing process.*
- *[Rule 3] A pre-defined threshold of Electoral Board members shall contribute with their shares of the election private key when executing the decryption operations.*
- *[Rule 4] The operations flow cannot be executed in a different order than: Voting process closing – tallying phase start – cleansing process – mixing process – vote decryption - counting process - results determining - tallying phase end.*
  Just the specified exceptions (FDP_IFC.1.1.C) can be managed.

FDP_IFF.1C.3 The TSF shall enforce the following additional SFP rule:

- *[Rule 5] Voting process closing shall be performed in accordance to the election date and time configuration.*

FDP_IFF.1C.4 The TSF shall explicitly authorize an information flow based on the following rule:

- *[Rule 6] Authorized Activities requested by the appropriate election officer, according to the defined segregation of duties rules, if the mandatory operations flow is not broken.*

FDP_IFF.1C.5 The TSF shall explicitly deny an information flow based on the following rule:

- *[Rule 7] Operations outside of the specified flow:*
  Voting process closing – tallying phase start – cleansing process – mixing process – vote decryption – counting process – results determining – tallying phase end.
  Just the specified exceptions (FDP_IFC.1.1.C) can be managed.

5.1.4.10 FDP_IFF.5 No illicit information flows

Hierarchical to:	FDP_IFF.4 Partial elimination of illicit information flows
Dependencies:	FDP_IFC.1 Subset information flow control
FDP_IFF.5.1	The TSF shall ensure that no illicit information flows exist to circumvent [*SFP for electoral management, SFP for voting process, and SFP for tallying process*]. *a) No information input will be accepted outside of the specified operations flow.* *b) Any kind of error in a transaction (vote casting, configuration …) will provoke the transaction to be rejected.*

5.1.4.11 FDP_ITT.1 Basic internal transfer protection

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ITT.1.1	The TSF shall enforce the *SFP* to prevent the [*disclosure, modification, or loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

5.1.4.12 FDP_ITT.3 Integrity monitoring

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FDP_ITT.1 Basic internal transfer protection
FDP_ITT.3.1	The TSF shall enforce the *SFP* to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [*integrity check errors, uncompleted transmission*].
FDP_ITT.3.2	Upon detection of a data integrity error, the TSF shall: • *Reject data transmission.* • *Prepare and generate a log entry.* • *Operation roll-back.*

5.1.4.13 FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a *resource or buffer* is made unavailable upon the *allocation of the resource to and de-allocation of the resource from* the following objects: the cryptographic keys used for digital signature and decryption at any component, the selected voting options at the voting client, any precalculation or cryptographic secret data at any component, the permutations performed at the mixing process, any processed password, and the RBAC tokens.

5.1.4.14 FDP_ROL.1 Basic rollback

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ROL.1A.1	The TSF shall enforce the *SFP for voting process* to permit the rollback of the [*vote selection*] on the [*voting client-side*].
FDP_ROL.1A.2	The TSF shall permit operations to be rolled back within the [*scope of the client-side operations, if the vote transaction has not been processed*].
FDP_ROL.1B.1	The TSF shall enforce the *SFP for voting process* to permit the rollback of the [*vote storage and electoral roll update*] on the [*voting server-side*].
FDP_ROL.1B.2	The TSF shall permit operations to be rolled back within the [*scope of the server-side operations, if any of the vote storage and electoral roll update transactions has not concluded successfully]*.
FDP_ROL.1C.1	The TSF shall enforce the *SFP for election management* to permit the rollback of the [election *configuration import*] on the [*configuration management process*].
FDP_ROL.1C.2	The TSF shall permit operations to be rolled back within the [*scope of configuration management, if the configuration can be revoked*].
FDP_ROL.1D.1	The TSF shall enforce the *SFP for tallying process* to permit the rollback of the [*cleansing – mixing – counting process*] on the [*tallying process*].

FDP_ROL.1D.2	The TSF shall permit operations to be rolled back within the [*scope of the mandatory operations flow, just for serious integrity errors*].

5.1.4.15 FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1	The TSF shall enforce the *SFPs* to be able to *transmit and receive* user data in a manner protected from unauthorized disclosure.

5.1.4.16 FDP_UIT.1 Data exchange integrity

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FDP_UIT.1.1	The TSF shall enforce the *SFPs* to be able to *transmit and receive* user data in a manner protected from *modification, deletion, insertion, and replay* errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion, and replay* has occurred.

5.1.5 Class FIA: Identification and Authentication

5.1.5.1 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [*RSA algorithm with cryptographic key size minimum 2048 bits; HMAC with cryptographic key size minimum 128 bits; ElGamal with cryptographic key size minimum 2048 bits; and Cryptographics Zero Knowledge Proofs (ZKP)].*

5.1.5.2 FIA_SOS.2 TSF Generation of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet [*RSA algorithm with cryptographic key size minimum 2048 bits; HMAC with cryptographic key size minimum 128 bits; ElGamal with cryptographic key size minimum 2048 bits; and Cryptographic Zero Knowledge Proofs (ZKP)]]*
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for [*vote sending from the vote client, vote processing and verification in the VCS and RCG Service, and cryptographic key generation*].

5.1.5.3 FIA_UAU.1 Timing of authentication (for voters)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [*no action*] on behalf of the user *(voters)* to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user *(voter)* to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

5.1.5.4 FIA_UAU.2 User authentication before any action (for election officer)

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each *individual election officer* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.5.5 FIA_UAU.3 Unforgeable authentication

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_UAU.3.1	The TSF shall *prevent* use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall *prevent* use of authentication data that has been copied from any other user of the TSF.

5.1.5.6 FIA_UAU.4 Single-use authentication mechanisms (for voters)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to *voter authentication tokens, external authentication tokens (from MinID service), and encrypted voting options*.

5.1.5.7 FIA_UID.1 Timing of identification (for voters)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1	The TSF shall allow [*no process*] on behalf of the users (*voters*) to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user *(voter)* to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

5.1.5.8 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.6 Class FMT: Security Management

5.1.6.1 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.

Dependencies:	FMT_SMR.1 Security roles . FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [*upload*] the [*election configuration files*] to [*application administrators*].

5.1.6.2 FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for [*MinID tokens, Authentication tokens, RBAC tokens, election configuration files*].

5.1.6.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions:

1) *Administration Board: Group responsible of election configuration. The configuration validation is performed through the digital signature.*
    a. *Cryptographic Keys Generation (of Administration Board).*
    b. *Sign (distributed) of election configuration files.*
    c. *Sign of decrypted ballot box signing.*
2) *Electoral Board: Group responsible of protect the results privacy and sign the decrypted ballot box.*
    a. *Cryptographic Keys Generation (of Electoral Board).*
    b. *Ballot box decryption.*
3) *Election Administrator. Group responsible of proper election running:*
    a. *Cryptographic Keys Generation / administration.*
    b. *Voting-cards Generation.*

c. *Election Configuration File management and importing process.*
d. *Extract and sign the ballot box.*
e. *Extract and sign the voting receipts.*
f. *Revoke Certificates.*

4) *Election Operator: Election Monitoring Profile.*
   a. *Service-check and status Monitoring.*
   b. *View ballot box status.*
   a. *View application logs.*
5) *Auditor. Read-only profile for auditors.*
   a. *View application logs.*
   b. *View Election Configurations.*
   c. *View Vote Receipts vs. Ballot Box (from the application logs).*
   d. *Review integrity of the mixing process.*
   e. *Review integrity of the decrypting process.*

User profiles 1-Electoral Board, and 2-Administration Board, will not be required to start a user-interactive session at the application. These users will be only granted to operate through their secret keys.

5.1.6.4 FMT_SMR.2 Restrictions on security roles

Hierarchical to:	FMT_SMR.1 Security roles
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.2.1	The TSF shall maintain the roles: [*Administration Board; Electoral Board; Election Administrator; Election Operator; Application Administrator; Auditor].*
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions are satisfied *[Cond1] – One user could be granted to more than one role. However, he will be only logged with one user-profile each time.* *[Cond2] – One role can be granted to an undefined number of users*.

5.1.6.5 FMT_SMR.3 Assuming roles

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
FMT_SMR.3.1	The TSF shall require an explicit request to assume the following roles: [*any role*].

5.1.7 Class FPR: Privacy

FPR_ANO.1 Anonymity

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPR_ANO.1.1	The TSF shall ensure that [*all users*] are unable to determine the real *voter identity* bound to *a decrypted vote*.

5.1.7.1 FPR_UNL.1A Unlinkability (network)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPR_UNL.1A.1	The TSF shall ensure that [*all users*] are unable to determine whether *the operations related to the initiation of vote casting and final vote casting are related to the vote casting by checking if the length of the transmitted ballots or vote records corresponds to a specific number of selected voting options, the position of voting options within the ballot or an invalid vote.*

5.1.7.2 FPR_UNL.1B Unlinkability (decrypted votes)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPR_UNL.1B.1	The TSF shall ensure that *after the determination of the election result, the election officer* is unable to determine whether *the vote records obtained from the mixing process were stored in a particular order or at a particular time.*

5.1.8 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*integrity errors, communication errors*].

5.1.8.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

5.1.8.2 FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITI.1.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [*verification of digitally signed information*].
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [stop the related transaction and *create a log entry*] if modifications are detected.

5.1.8.3 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITT.1.1	The TSF shall protect TSF data from [*disclosure or modification*] when it is transmitted between separate parts of the TOE.

5.1.8.4 FPT_ITT.3 TSF data integrity monitoring

Hierarchical to:	No other components.
Dependencies:	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.3.1	The TSF shall be able to detect [*modification of data, substitution of data, re-ordering of data, deletion of data, or any other integrity errors*] for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2	Upon detection of a data integrity error, the TSF shall take the following actions: [stop the related transaction and *create a log entry*].

5.1.8.5 FPT_RCV.4 Function recovery

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_RCV.4.1	The TSF shall ensure that [*the user front-end, the Vote Collector Service, the ballot box database, or the return code generator*] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

5.1.8.6 FPT_RPL.1 Replay detection

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [*vote casting*].
FPT_RPL.1.2	The TSF shall perform [*replay rejection*] when replay is detected.

5.1.8.7 FPT_SSP.1 Simple trusted acknowledgement

Hierarchical to:	No other components.
Dependencies:	FPT_ITT.1 Basic internal TSF data transfer protection
FPT_SSP.1.1	The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

5.1.8.8 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

5.1.9 Class FTA: TOE access

5.1.9.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [*a configurable time interval of user inactivity*].

5.1.9.2 FTA_SSL.4 User-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.

5.1.9.3 FTA_TSE.1 TOE session establishment

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [*user authorization to log-in*].

5.1.10 Class FTP: Trusted path/channels

FTP_TRP.1 Trusted path

Hierarchical to:	No other components.

Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [*voters as remote*] users that is logically distinct from other communication paths and provides assured *identification* of its end points, and protection of the communicated data from [*modification or disclosure*].
FTP_TRP.1.2	The TSF shall permit [*voters as remote users*] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [*voter authentication and voting process*].

5.2 Security Functional Requirements dependencies

Requirement	Dependencies	Dependency met
FAU_GEN.1	FPT_STM.1	**Yes**
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	**Yes**
FAU_SAR.1	FAU_GEN.1	**Yes**
FAU_STG.1	FAU_GEN.1	**Yes**
FCO_NRO.2	FIA_UID.1	**Yes**
FCO_NRR.1	FIA_UID.1	**Yes**
FCS_CKM.1	FCS_CKM.4 and FCS_COP.1	**Yes**
FCS_CKM.2	FCS_CKM.1, FCS_CKM.4 and FCS_COP.1	**Yes**
FCS_CKM.4	FCS_CKM.1	**Yes**
FCS_COP.1	FCS_CKM.4 and FCS_CKM.1	**Yes**
FDP_ACC.1	FDP_ACF.1	**Yes**
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	**Yes** **No**
FDP_DAU.2	FIA_UID.1	**Yes**
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	**Yes**
FDP_IFC.1	FDP_IFF.1	**Yes**
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	**Yes** **No**
FDP_IFF.5	FDP_IFC.1	**Yes**
FDP_ITT.1	FDP_ACC.1 and FDP_IFC.1	**Yes**
FDP_ITT.3	None	n/a
FDP_RIP.1	None	n/a
FDP_ROL.1	FDP_ACC.1 and FDP_IFC.1	**Yes**
FDP_UCT.1	FDP_ACC.1, FDP_IFC.1 and FTP_TRP.1	**Yes**
FDP_UIT.1	FDP_ACC.1, FDP_IFC.1 and FTP_TRP.1	**Yes**
FIA_SOS.1	None	n/a
FIA_SOS.2	None	n/a
FIA_UAU.1	FIA_UID.1	**Yes**
FIA_UAU.2	FIA_UID.1	**Yes**
FIA_UAU.3	None	n/a
FIA_UAU.4	None	n/a
FIA_UID.1	None	n/a
FIA_UID.2	None	n/a
FMT_MTD.1	FMT_SMF.1 and FMT_SMR.2	**Yes**
FMT_MTD.3	FMT_MTD.1	**Yes**
FMT_SMF.1	None	n/a
FMT_SMR.2	FIA_UID.1	**Yes**
FMT_SMR.3	FMT_SMF.1	**Yes**
FPR_ANO.1	None	n/a
FPR_UNL.1	None	n/a
FPT_FLS.1	None	n/a

Requirement	Dependencies	Dependency met
FPT_ITC.1	None	n/a
FPT_ITI.1	None	n/a
FPT_ITT.1	None	n/a
FPT_ITT.3	FDP_ITT.1	**Yes**
FPT_RCV.4	None	n/a
FPT_RPL.1	None	n/a
FPT_SSP.1	FPT_ITT.1	**Yes**
FPT_STM.1	None	n/a
FTA_SSL.3	None	n/a
FTA_SSL.4	None	n/a
FTA_TSE.1	None	n/a
FTP_TRP.1	None	n/a

5.2.1 Justification why dependencies are not met

FDP_ACF.1 and FDP_IFF.1 are referring to FMT_MSA.3 component. These components require the FMT_MSA component to manage security attributes from users and roles. However:

- The system access control (through a password based mechanism) is managed in an external non-TOE application (the election management system).
- The user-roles assignation to individual users is managed in an external non-TOE application (the election management system).
- Although the relationship between user-roles and application user functionalities is defined at the TOE, it cannot be modified or managed.

5.3 Mapping of TOE Security Requirements to Objectives

The following table shows the mapping between TOE Security Requirements and Objectives defined in this ST.

Requirement	Security Objectives
FAU_GEN.1	OS13, OS14
FAU_GEN.2	OS13, OS14
FAU_SAR.1	OS13, OS14
FAU_STG.1	OS13, OS14
FCO_NRO.2	OS2, OS5, OS8
FCO_NRR.1	OS2, OS5, OS8
FCS_CKM.1	OS2, OS3, OS.4, OS8, OS11
FCS_CKM.2	OS2, OS3, OS.4, OS8, OS11
FCS_CKM.4	OS2, OS3, OS.4, OS8, OS11
FCS_COP.1	OS2, OS3, OS.4, OS8, OS11
FDP_ACC.1	OS3, OS4, OS5, OS6, OS11
FDP_ACF.1	OS3, OS4, OS5, OS6, OS11
FDP_DAU.2	OS3, OS4, OS5, OS6, OS11
FDP_ETC.2	OS3, OS4, OS5, OS6, OS8
FDP_IFC.1	OS6, OS7, OS8, OS11
FDP_IFF.1	OS6, OS7, OS8, OS11
FDP_IFF.5	OS6, OS7, OS8, OS11
FDP_ITT.1	OS6, OS7, OS8, OS11
FDP_ITT.3	OS13, OS14
FDP_RIP.1	OS8, OS11
FDP_ROL.1	OS8, OS11
FDP_UCT.1	OS3, OS4
FDP_UIT.1	OS8, OS11
FIA_SOS.1	OS3, OS4
FIA_SOS.2	OS3, OS4

Requirement	Security Objectives
FIA_UAU.1	OS1, OS2, OS3, OS11
FIA_UAU.2	OS5
FIA_UAU.3	OS1, OS2, OS5, OS6, OS7, OS11
FIA_UAU.4	OS1, OS2, OS3, OS11
FIA_UID.1	OS1, OS2, OS3, OS11
FIA_UID.2	OS1, OS2, OS5, OS6, OS7, OS11
FMT_MTD.1	OS6, OS7
FMT_MTD.3	OS6, OS7
FMT_SMF.1	OS6, OS7, OS8, OS9, OS10, OS11
FMT_SMR.2	OS6, OS7, OS8, OS9, OS10, OS11
FMT_SMR.3	OS6, OS7, OS8, OS9, OS10, OS11
FPR_ANO.1	OS3, OS4
FPR_UNL.1	OS3, OS4
FPT_FLS.1	OS8, OS9, OS10, OS11
FPT_ITC.1	OS3, OS4, OS11
FPT_ITI.1	OS8, OS13
FPT_ITT.1	OS3, OS4, OS11
FPT_ITT.3	OS8,OS13
FPT_RCV.4	OS9, OS10, OS11
FPT_RPL.1	OS8, OS11
FPT_SSP.1	OS8, OS10, OS11
FPT_STM.1	OS8
FTA_SSL.3	OS5, OS6, OS7, OS11
FTA_SSL.4	OS5, OS6, OS7, OS11

Requirement	Security Objectives
FTA_TSE.1	OS5, OS6, OS7, OS11
FTP_TRP.1	OS1, OS3, OS4, OS8

Table 5-1: Mapping of TOE Security Requirements to Objectives.

5.4 Justification of TOE Security Requirements to Objectives

The following table shows how each TOE Security Requirement satisfies the Objectives defined in this ST.

FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1	OS13 – Open Auditing and Accounting OS14 – System Disclosability/Openness
Components from the Security Audit class require TSF to identify and register application logs, regarding critical operations, potential malfunctions, and security incidents. This application log shall be accessible by operators and auditors, and shall be protected from unauthorized modifications or deletions. These requirements are addressed in the "**open audit and accounting**" and "**system disclosability**" security objectives.	

FCO_NRO.2 FCO_NRR.1	OS2 - Effective Voter Authenticity OS5 – Effective System Identification and Authentication OS8 – Information Integrity
Components from the Communication class require the generation, identification, and timing, of the evidence of origin for the critical information transmitted (**OS2 - Effective Voter Authenticity** for voters and **OS5 – Effective System Identification and Authentication** for administrators). Evidence verification is also required which is performed through digital signatures verification (**OS8 – Information Integrity**).	

FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1	OS2 - Effective Voter Authenticity OS3 - Effective Voter Anonymity OS4 - Effective Vote Confidentiality OS8 – Information Integrity OS11 – Service Protection
Cryptographic Support is required regarding key generation, key distribution, key destruction, and other cryptographic operations, in order to ensure the **authenticity, anonymity, and confidentiality** from the voter operations, and to preserve the information **integrity** from the whole system. Cryptographic Support is a key component for the **service protection**.	

FDP_ACC.1 FDP_ACF.1 FDP_DAU.2	OS1 - Effective Voter Registration OS5 – Effective System Identification and Authentication OS6 – Effective System Registration OS11 – Service Protection
Access Control attributes regarding User Data Protection, require TSF to ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are controlled and attached to an access control SFP; It is covering the security objectives related to **voter registration** and **system identification and registration**. An adequate access control is a key component for the **service protection**.	

FDP_ETC.2	OS3 - Effective Voter Anonymity OS4 - Effective Vote Confidentiality OS5 – Effective System Identification and Authentication OS6 – Effective System Registration OS8 – Information Integrity
A set of security rules has been defined to protect the **anonymity**, **confidentiality**, and **integrity**, of the voter information, when it is exported outside the TOE. Effective system identification, authentication, and registration, shall be performed to execute the export function.	

FDP_IFC.1 FDP_IFF.1 FDP_IFF.5 FDP_ITT.1	OS6 – Effective System Registration OS7 – Effective System Access Control OS8 – Information Integrity OS11 – Service Protection
There have been defined three different information flow controls (for election management, voting phase, and tallying phase), and related security attributes, in order to ensure the **service protection** and **information integrity**. These information flows and security controls are supported by a secure **system registration** and **system access controls**.	

FDP_ITT.3	OS13 – Open Auditing and Accounting OS14 – System Disclosability/Openness
Integrity monitoring controls are required, and implemented through the application logs maintenance. These requirements are addressed in the "**open audit and accounting**" and "**system disclosability**" security objectives.	

FDP_RIP.1	OS8 – Information Integrity OS11 – Service Protection
The software will ensure that any previous information content of a resource or buffer is made unavailable, in order to ensure **service protection** and **information integrity**.	

FDP_ROL.1	OS8 – Information Integrity OS11 – Service Protection
Roll-back operations will be permitted and controlled, in order to ensure **service protection** and **information integrity**.	

FDP_UCT.1	OS3 - Effective Voter Anonymity OS4 – Effective Voter Confidentiality
Data transmission is protected from unauthorized disclosure, in order to ensure **voter anonymity and confidentiality**.	

FDP_UIT.1	OS8 – Information Integrity OS11 – Service Protection
Data transmission is protected from unauthorized modifications, insertions, or deletions, in order to ensure **information integrity** and **service protection**.	

FIA_UAU.3 FIA_UID.2	OS1 - Effective Voter Registration OS2 - Effective Voter Authenticity OS5 – Effective System Identification and Authentication OS6 – Effective System Registration OS7 – Effective System Access Control OS11 – Service Protection
Generic identification and authentication security attributes have been defined (failure handling, attribute definition, user identification, and unforgeable authentication) for both election application users and voters, in order to ensure the **service protection** through a secure **identification, authentication, registration,** and **access control.**	

FIA_SOS.1 FIA_SOS.2	OS3 - Effective Voter Anonymity OS4 - Effective Voter Confidentiality
Secrets' Generation and Verification mechanisms are required to ensure voter **anonymity and confidentiality**.	

FIA_UAU.1 FIA_UAU.4 FIA_UID.1	OS1 - Effective Voter Registration OS2 - Effective Voter Authenticity
Secure voter **registration and authenticity** verification mechanisms will be provided, through an authentication token – after a successful identification at an external (non-TOE) trusted identification service (MinID, in-person issuing point…) – and the vote digital signature.	

FIA_UAU.2	OS5 – Effective System Identification and Authentication
After a non-TOE identification process (from the election administration software), the user **authentication** will be verified to ensure the user account with which he has been previously identified, ant the user-roles assigned to this user account.	

FMT_MTD.1 FMT_MTD.3	OS6 – Effective System Registration OS7 – Effective System Access Control
Components from Security Management Class are required to ensure an **Effective System Registration and System Access Control**, Through the credentials verification with the external access control service.	

FMT_SMF.1 FMT_SMR.2 FMT_SMR.3	OS6 – Effective System Registration OS7 – Effective System Access Control OS8 – Information Integrity OS9 – Service Availability OS10 – Information Availability OS11 – Service Protection
A role-based model for election application users has been defined, in order to ensure the **service protection, information integrity, service availability, and information availability**, through a secure **system registration and access control** which ensures that election application users can access only those parts of the system and assets necessary to perform the authorized tasks.	

FPR_ANO.1 FPR_UNL.1	OS3 - Effective Voter Anonymity OS4 - Effective Vote Confidentiality
Anonymity Component from Privacy Class is required to ensure Voter Anonymity and confidentiality, through the encryption mechanism which prevents a user to determine the voting options from a voter.	

FPT_FLS.1	OS8 – Information Integrity OS9 – Service Availability OS10 – Information Availability OS11 – Service Protection
Security requirements regarding preservation of secure state on failures are considered, to address the **Information Integrity, Service Availability, Information Availability,** and **Service Protection** security objectives.	

FPT_ITC.1 FPT_ITT.1	OS3 - Effective Voter Anonymity OS4 - Effective Vote Confidentiality OS11 – Service Protection
The **service shall be protected** from unauthorized disclosure (which affects the voter **anonymity and confidentiality**) during transmission to another trusted IT products or another parts of the TOE.	

FPT_ITI.1 FPT_ITT.3	OS8 – Information Integrity OS13 – Open Auditing and Accounting
Unauthorized modifications of the information shall be detected, to be compliance with the **information integrity** and **open auditing** security objectives.	

FPT_RCV.4	OS9 – Service Availability OS10 – Information Availability OS11 – Service Protection
Critical operations will have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state. It covers the **service availability, information availability, and service protection** security objectives.	

FPT_RPL.1	OS8 – Information Integrity OS11 – Service Protection
Replay detection functions are required to preserve **information integrity** and ensure the **service protection**.	

FPT_SSP.1	OS8 – Information Integrity OS10 – Information Availability OS11 – Service Protection
Trusted acknowledgements functions are required to preserve **information integrity, information availability,** and ensure the **service protection**	

FPT_STM.1	OS8 – Information Integrity
The reliable timestamp requirement will protect the **information integrity**.	

FTA_SSL.3 FTA_SSL.4 FTA_TSE.1	OS5 – Effective System Identification and Authentication OS6 – Effective System Registration OS7 – Effective System Access Control
The system **identification, authentication, registration,** and **access control** mechanisms, are protected by security requirements regarding user sessions locking controls, and denying session establishment according to the log-in process.	

FTP_TRP.1	OS1 - Effective Voter Registration OS3 - Effective Voter Anonymity OS4 - Effective Vote Confidentiality OS8 – Information Integrity
Secure Connections Controls are required between voters and servers, after the **effective voter registration**, to ensure the **anonymity, confidentiality, and integrity**, of the transmitted information.	

5.5 Security Assurance Requirements

The Assurance Security Requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 4 as defined by the CC.

Assurance Class	Assurance Component	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.2	Testing: security enforcing modules
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis

Table 5-2: Security Assurance Requirements for EAL4+

5.5.1 Rationale for Security Assurance Requirements

EAL4+ is chosen to provide a moderate to high level of assured security. This assurance level is consistent with the threat environment.

The security assurance requirements for the EAL4 level are taken from part 3 of CC.

EAL4+ represents an increase in assurance from EAL4, by requiring a more exhaustive vulnerability analysis over the TOE. In this way, AVA_VAN assurance component from AVA assurance class (vulnerability assessment) is increased from AVA_VAN.3 to AVA_VAN.4.

6 TOE Summary Specification

6.1 TOE Security Functions Rationale

The TOE consists of 5 Security Functions:

- Security audit
- Identification and authorization
- Process Integrity
- Cryptographic support
- Service Availability

Table 6-1 below demonstrates the tracing of TOE security functions back to aspects of the security functional requirements (SFRs).

	Security Audit	Identification and authorization	Process accuracy	Cryptographic support	Service Availability
FAU_GEN.1	**X**				
FAU_GEN.2	**X**				
FAU_SAR.1	**X**				
FAU_STG.1	**X**				
FCO_NRO.2			**X**		

	Security Audit	Identification and authorization	Process accuracy	Cryptographic support	Service Availability
FCO_NRR.1			**X**		
FCS_CKM.1				**X**	
FCS_CKM.2				**X**	
FCS_CKM.4				**X**	
FCS_COP.1				**X**	

	Security Audit	Identification and authorization	Process accuracy	Cryptographic support	Service Availability
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_DAU.2		X			
FDP_ETC.2		X			
FDP_IFC.1			X		
FDP_IFF.1			X		
FDP_IFF.5			X		
FDP_ITT.1			X		
FDP_ITT.3	X				
FDP_RIP.1			X		
FDP_ROL.1			X		
FDP_UCT.1			X		
FDP_UIT.1			X		
FIA_SOS.1				X	
FIA_SOS.2				X	
FIA_UAU.1		X			
FIA_UAU.2		X			
FIA_UAU.3		X			
FIA_UAU.4		X			
FIA_UID.1		X			
FIA_UID.2		X			
FMT_MTD.1		X			

	Security Audit	Identification and authorization	Process accuracy	Cryptographic support	Service Availability
FMT_MTD.3		X			
FMT_SMF.1		X			
FMT_SMR.2		X			
FMT_SMR.3		X			
FPR_ANO.1			X		
FPR_UNL.1			X		
FPT_FLS.1			X		
FPT_ITC.1			X		
FPT_ITI.1			X		
FPT_ITT.1			X		
FPT_ITT.3			X		
FPT_RCV.4					X
FPT_RPL.1					X
FPT_SSP.1					X
FPT_STM.1					X
FTA_SSL.3		X			
FTA_SSL.4		X			
FTA_TSE.1		X			
FTP_TRP.1		X			

Table 6-2: Security functions to SFR mapping

The following rationale explains how the TOE is providing its Security functions.

6.1.1 Security audit

All components from the e-voting TOE, send a copy of their logs to the audit system. If a system or infrastructure component is broken, a local copy of the log is always available.

The system logs all significant events, recording the user, time, and event details. This includes logs of all events at all levels of the complete Electronic Voting Software. It also includes all voting transactions, attacks on the operation of the electronic voting system, its system failures, malfunctions and other threats to the system and events.

Log messages recorded are status/informational messages (i.e., executed transactions and their result) as well as errors/issues. All log entries contain the following information:

- Date and time of the event.
- Type of event.
- Related object identification.
- Subject identity (username, session id, IP address or any other location information from the user or system which generates the event).
- And the outcome (success or failure) of the event.

Logs are stored with the “Immutable log” mechanism, which ensures that any change to the log files will be detected.

6.1.2 Identification and authorization

Identification and authorization mechanism are based on the user-role mechanism. This security control is used to prevent any non-properly authenticated and authorized user from accessing objects, as described in the Security Functional Requirement (SFR).

The TOE maintains the following roles:

1. **Administration Board**: Group responsible for the election configuration. The configuration validation is performed through the digital signature.
2. **Electoral Board**: Group responsible for protecting the results privacy, and sign the un-encrypted ballot box.
3. **Election Administrator**. Group responsible for proper election running:
4. **Election Operator**: Election Monitoring Profile.
5. **Auditor**. Read-only profile for auditors.

Users and roles have some general rules that shall be considered:

- One user could be granted to more than one role. However, she will be logged with one user-profile each time.
- One role can be granted to an undefined number of users.
- User accounts and user rights shall be granted with the principle of least privileges.
- No generic user accounts shall be created.

6.1.3 Process Accuracy

The Electronic Voting Software will be responsible for the vote casting, safe storing, processing and counting. Because the high importance of these processes, the software shall ensure that there is no possibility to perform any unexpected or non-authorized operation over the voting process.

Voter confidentiality, and polling integrity and confidentiality, shall be protected.

Three information flows have been defined to manage and protect the security of the process:

1) **Election Management**: Election configuration management, electoral period opening and closing process, electoral administration activities, cryptographic keys generation and management, and voting cards generation.
2) **Voting Process:** Voter Identification and Authentication, vote casting, vote checking, vote receipt generation and sending, return code generation and sending, vote storing.
3) **Tallying Process.** Starting the tallying process, cleansing process, mixing process (includes auditing), counting process, determining the electoral result.

Additional security controls have been defined to protect the communications operations and the data integrity.

6.1.4 Cryptographic support

Every critical information asset and operation will be protected through cryptographic mechanisms which ensure information confidentiality, authenticity, and integrity. E.g:

- Communications are encrypted between the PC of the voters and the Front End.
- Votes are encrypted and digitally signed by the voter.
- Election Configurations are digitally signed by the electoral administrators.
- The ballot box is digitally signed by every service (step) which manipulates it (Vote Collector Service, Cleansing Service, Mixing Service, and Counting Service).

- Vote receipts are digitally signed by the Return Code Generator.
- Log Files are digitally signed by the Electronic Voting Software.
- …

The Electronic Voting Software will use cryptographic keys and algorithms in accordance with the following standards:

- **Key generation algorithm**: RSA, minimum key size equivalent to a symmetric key of 100 bits (FNISA (French Network and Information Security Agency) Recommendations 2010); meet the specifications in FIPS 186-3.
- **Digital signature and verification**: RSA, minimum key size equivalent to a symmetric key of 100 bits; specifications in PKCS#1 v2.1 for the RSA digital signature and verification (RSASSA-PSS);
- **Hash algorithm**: SHA-256; specifications in FIPS 180-3 ;
- **Message authentication**: HMAC, minimum key size 128 bits; specifications in FIPS 198a for HMAC function in combination with SHA-256 hash function.

6.1.5 Service Availability

The availability of the Electronic Voting Service shall be ensured, in order to allow the voters to exercise his right-to-vote.

Critical operations will have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.