E-vote 2011
Logs alerts definition on eVoting

Version 1.0

Change history

Date	Version	Description	Author
14.03.2011	0.1	Creation of the document including first alerts	SCYTL R&D
17.03.2011	0.2	Modification to include: - Type of alerts - Alerts criteria. - New threat-pattern alerts	SCYTL R&D
18.03.2011	0.3	The Category of alerts is defined and established. Annex 1 and 2 have been included	SCYTL R&D
21.03.2011	0.4	Annex 2 has been reviewed. Included logs and alerts for RBAC events.	SCYTL R&D
23.03.2011	0.5	An Annex 3 has been added to document what events are not being registered in logs.	SCYTL R&D
24.03.2011	0.6	New error codes have been added	SCYTL R&D
24.03.2011	0.7	What is not planned for the 15/04/2011 but Scytl still wants to put before code publication has been marked in grey	SCYTL DEV&PM
29.03.2011	0.8	Minor changes to alerts	SCYTL R&D
17/06/2011	1.0	New logs on vote validations and TPM errors. Alerts have been updated. Disclaimer has been included.	SCYTL R&D

DISCLAIMER: This document is a work in progress and some information in it might be obsolete, inaccurate or might be missing. Regular updates will be made to the document. This disclaimer will be also updated to reflect the state of the document.

NEXT VERSION TARGET DATE:

Version	Date	Author	Comments
1.1	01/07/2011		

Contents

1. Definition of Alerts

The following document is explaining the process and the results of defining the alerts.

The **scope** which has been considered inside this document is:

- **Covering** all the logs generated by all the application components on the eVoting.
- **Not covering** the infrastructure logs generated by other components (like operating systems, databases, application servers…)

This document is defining the following

- Type of Alerts: How the alerts are going to be defined.
- Alerts Categories. How critical are the raised alerts.
- Alerts Criteria. What is the mechanism to decide if the alert shall be raised or not.
- Alerts. The messages to be managed by the SPLUNK system.

In the annex 1 of the document, all the logs messages (currently implemented) to be registered by the e-voting application have been documented.
In the annex 2 of the document, the whole list of logs from the application is included, and the events which are not being registered in the logs are specified in the annex 3.

1.1 Type of Alerts

Regarding the alerts definition process, we can consider 3 different types of alerts:

- Direct alerts. This is a simple alert detection coming from a simple log entry. It involves having a very important log entry or a very critical error, which is raising an alert just when the message is received.
  In order to prioritize the creation of these alerts, we can consider two phases:
  - Basic Alerts. The minimum alerts to prevent or detect the most critical security attacks.
  - Extended alerts. The full set of alerts to prevent or detect basic security attacks, coming from a simple log entry.

- Threat Patterns security alerts. Advanced alerts generated by analyzing several logs entries which can be related, or a repetition of events which are not an alert on an individual treatment but yes on a group treatment.

- Alerts from the audit functionalities. Alerts generated by analyzing the logs of the audit functionalities (both auditor manual requests as internal and automatic self-test process).

1.2 Alerts Categories

Regarding the importance of the raised alerts, we can categorize them in four different groups. These categories are identifying the criticality, and the origin of the alert (it could be an error, or just useful information).

There have been considered four alerts categories:

- CRITICAL. This alert is related to an error which can be affecting to the related service or affecting the security. It would be necessary to evaluate each different message, but it would probably request some kind of intervention.

- WARNING. This is a message indicating that something could be going wrong. There could be several minor errors, or a security attack could be starting. These alerts need to be investigated in order to decide if a corrective action is required.

- MILESTONE MESSAGE. Initially, a milestone message is a relevant message which is normal to be received inside the usual flow of operations (e.g. the application is starting, or the ballot box is being exported at the end of the election). However, if this “normal” message is not being expected, then it can be considered like a critical message.

- INFO. This alert is not related an error or an attack; it is an information message for administrators, operators, or auditors. The analysis of this information will decide more exhaustive verifications or any other action.

1.3 Alerts Criteria

When defining the criteria from raising an alert or not, the following have been considered:

- Type A: Direct message. The message shall be sent immediately when the log is received.
- Type B: Recurrence, X events in a minute. We are analyzing several consecutive occurrence of the same log. These are short term alerts to detect massive attacks.
- Type C: Recurrence, X events in an hour. We are analyzing several consecutive occurrence of the same log to detect attacks. These are average term alerts.
- Type D: Recurrence, X events in a minute, from the same source. This kind of criteria is focused to detect massive attacks. If the same voter or the same IP address is generating the same error several times per minute, this is probably a massive attack to tamper the application.
- Type E - Special: Send Direct Alert. This is covering more complex combinations of logs to detect security threats. If this criteria is identified, the alert shall be raised immediately.

2. Alerts definition

The alerts which will be implemented into SPLUNK are refined, according to the type of alerts.

2.1 Direct Alerts:

All the alerts from the "Direct Alert" type are following the "Type A: Direct Message" criteria.

Component	Log Message	Message Identification		Category
		Action	Code	
VCS / ATS / RCG	Processing of Election Configuration Files	ECPRO	ANY	MILESTONE
VCS / ATS / RCG	Digital signature verification of the Election Configuration Files	ECVER	ANY ERROR 040, 041, 042	CRITICAL
ATS	Voter authentication errors (from MinID, electoral roll, or token errors)	VAUTH	EXCEPTIONAL ERRORS 001, 010	WARNING
ATS	Voter Authentication Token Generation	TKGEN	ANY ERROR 008, 020	WARNING
VCS	Vote validations – unexpected error	VOTVL	EXCEPTIONAL ERROR 049	WARNING
VCS	Vote Storage	VOTST	ANY ERROR 052	CRITICAL
VCS	Ballot Box export (to Cleansing)	BBEXP	ANY	MILESTONE
RCG	Receipt list export (to Cleansing)	RLEXP	ANY	MILESTONE
ALL	RBAC Authorization	RBACA	EXCEPTIONAL ERRORS 821, 822	WARNING
ALL	Key Upload	KEYUP	ANY	MILESTONE
TPM	TPM Alert	ANY except ATTCN	ANY ERROR	CRITICAL

2.2 Threat Patterns security alerts

Component	Log Message	Message Identification		Alert Criteria	Category
		Action	Code		
ATS	Voter authentication errors (from MinID, electoral roll, or token errors)	VAUTH	ANY 001, 002. 003, 005. 006, 008, 009, 010, 015, 016	Type B: Recurrence, 10 or more events in a minute	WARNING
ATS	Voter authentication errors (from MinID, electoral roll, or token errors)	VAUTH	ANY 001, 002. 003, 005. 006, 008, 009, 010, 015, 016	Type D: Recurrence, 3 or more events in a minute, from the same voter (IP address or SSN).	WARNING
VCS	Vote Checking Results	VOTCH VOTVL MIDVL ATKVL SCHVL	ANY ERROR 055, 056, 045, 046, 047, 048, 049, 0'68, 069, 070, 071, 072, 073, 076, 077	Type C: Recurrence, 3 or more events in an hour	WARNING
		ATKVL	074, 075	Type B: Recurrence, 3 or more events in a minute	WARNING
		VOTCH VOTVL MIDVL ATKVL SCHVL	ANY ERROR 055, 056, 045, 046, 047, 048, 049, 0'68, 069, 070, 071, 072, 073, 074, 075, 076, 077	Type D: Recurrence, 3 or more events in a minute, from the same voter (IP address or SSN).	WARNING
RCG	Vote Checking Results	VOTCH MIDVL ATKVL	ANY ERROR 045, 046, 047, 048, 049, 055, 056, 068, 069, 070, 071, 072,	Type E - Special: Send Direct Alert. If the events VOTCH, MIDVL, or ATKVL have been "000	CRITICAL

Component	Log Message	Message Identification		Alert Criteria	Category
		Action	Code		
			073, 074, 075, 076, 077	Successful" in the VCS, but are failing in RCG.	
RCG	Error in tests from VCS (vote, reencryption, vote's test)	SCHVL VOTTV	ANY ERROR 78, 79, 80, 81, 82	Type C: Recurrence, 2 or more events in an hour	WARNING
RCG	Voting Receipt Generation	REGEN	ANY ERROR 400	Type B: Recurrence, 3 or more events in a minute	WARNING
RCG	Voting Receipt Generation	REGEN	ANY ERROR 400	Type C: Recurrence, 10 or more events in an hour	WARNING
RCG	Return Codes Sending	RCSND	ANY ERROR 402	Type C: Recurrence, 10 or more events in an hour	WARNING
VCS	Voting Receipt sending to the applet	RESND	ANY ERROR	Type C: Recurrence, 10 or more events in an hour	WARNING
ALL	RBAC Authorization	RBACA	ANY ERROR 819, 820, 823, 824	Type B: Recurrence, 3 or more events in a minute	WARNING
				Type C: Recurrence, 10 or more events in an hour	WARNING

2.3 Audit security alerts

Component	Log Message	Message Identification		Alert Criteria	Category
		Action	Code		
*ATS, VCS, RCG	Digital signature verification of the Election Configuration File	ECVER	ANY ERROR 812	Type A: Direct message.	CRITICAL
*ATS, VCS, RCG	Verification of the configuration file vs configuration database	ECDBV	ANY ERROR 812	Type A: Direct message.	CRITICAL
ALL	Service-Check	SRVCH SELFT	ANY ERROR	Type A: Direct message.	WARNING
Cleansing	Cleansing activities (checking results, rejected votes, exceptions, errors, vote selection information...)	VERIF CLREA CLSEL	ANY	Offline process. No alert, send information by e-mail.	INFO
Mixing	The mixing process will generate information regarding voting groups (locations) and number of votes processed per group.	MIXBB	ANY	Offline process. No alert, send information by e-mail.	INFO
Counting	Counting results	COUNT	ANY	Offline process. No alert, send information by e-mail.	INFO

Annex 1. Current error messages

001 MinID signature non valid
002 MinID timestamp expired
003 MinID token already used
005 Voter not electoral roll
006 Voter doesn't have any contest
008 P12 file not found
009 General authentication error
010 Error getting the electoral roll
015 Invalid user session
016 Cannot get the voter from the Authentication token
020 Error signing the Authentication token
030 Error retrieving key
031 Key not found"
035 Wrong parameters
036 Error uploading key
040 - Missing EML data
041 - Error processing the EML
042 - Error saving the zipped EML
043 Error verifying EML signature
044 EML already exists
045 Vote length is different
046 Error: SSN in Voter Certificate
047 Voter Digital Certificate
048 The election event not exists or is closed
049 Contest/s specified is/are not authorized
050 Error doing Partial decrypt, test calculation or reencryption
051 Error sending the vote to RCG
052 Error storing the vote
055 Error while checking the vote.
056 Unexpected exception while checking the vote.
068 Error verifying MinID Token unique ID
069 MinID Token unique ID has been received before
070 Error validating Min ID digital signature and certificate
071 Error validating Min ID Identification Service Issuing Time
072 Error verifying Authentication Service Digital signature and certificate
073 Error verifyng Authentication Service Issuing Time
074 Error verifyng Authentication Expiration Time
075 Auth Token unique ID has been received before
076 Error verifying Auth Token unique ID
077 Error verifying Schnorr Signature
078 Error verifying Vote Schnorr Signature
079 Error verifying Exp Schnorr Signature

080 Error verifying Key Schnorr Signature
081 Error in vote digital signature.
082 Error in vote partial decryption
300 Error on attestation tool
301 received PCRs don't match baseline
302 Quote Validation failed
303 Attestation tool reported ERROR
304 Can't run AIK Quote Verification
305 Can't read PCR's from quote
306 Error reading report for validation
307 Received report doesn't contain neither valid nor invalid hooks
308 Error connecting to remote host
309 Invalid key format
310 Cryptographic operation failed
311 Error persisting message
312 Report Signature Validation Failed
313 Failed Validation
314 Failed Validation with Exception (see comments)
315 Failed Report Validation
316 Error reading certificate
317 IOError
318 No report received
319 Received empty signature
320 Error reading from host: timeout
321 Received report has no hooks
400 Voting receipt generation error
401 Return codes generation error
402 Return codes sending error
403 Backup receipt list error
404 Backup Ballot Box error
500 Error restoring ballot box
501 Error restoring Electoral Roll
502 Error restoring receipts list
540 Error at cleansing + info
510 - Voter SSN is not in Electoral Roll
511 - There is another paper vote casted by the same voter
512 - There is another vote casted before by the same voter
513 - There is another controlled environment vote casted by the same voter
514 – Error verifying Voter Digital certificate using local CA
515 - Error verifying Voter Digital signature using voter digital certificate
516 - Vote time stamp is not from the past
517 - Vote time stamp is not in the voting period
519 - AuthTokenId has been received before for the same contest
520 - Internal AuthTokenId has been received before for the same contest
521 - SSN stored in Voter digital certificate is not equal to voter identifier
522 - SSN stored in AuthToken is not equal to voter identifier
523 - Error verifying Schnorr signature using SSN stored in AuthToken
524 - Error verifying Authentication Service certificate using local CA

525 - Authentication time stamp is not from the past
526 - Authentication time stamp is not in the voting period
527 - ContestId is not one of the allowed contests in AuthToken
528 - Error verifying MinID digital signature and certificate
529 - Error verifying Authentication Service digital signature using Authentication Service certificate
530 - Error verifying RCG Digital certificate using local CA
531 - Error verifying RCG Digital signature using RCG digital certificate
532 - Error verifying a vote in VCS has its corresponding receipt in RCG"
533 - The difference between receipt time stamp and vote time stamp exceed the limit of time between authentication and voting
534 - The difference between receipt time stamp and authentication time stamp exceed the limit of time between authentication and voting
535 - Receipt time stamp is not from the past
536 - Receipt time stamp is not in the voting period
540 - Error at cleansing
600 Failed Uploading Cbbs on Mixing Manager
601 Error verifying cleansed ballot box signature
602 Failed Mixing Ballot Boxes on Mixing Manager
604 Error: Upload point uplPointId not found
605 Error: There are no cleansed ballots for uploading point specified:
606 Error: Thread execution has been canceled due to an exception:
607 Error: Create output zip file has been failed:
608 Error in Operation - Audit Mixing finished for adtPoint %s, mxPointId %s. Error message: %s
609 Error in Mixing Audit: + info
651 Error verifying incoming Ballot box signature
652 Error: Failed Net Mixing on node
653 Error exporting the mixed ballot box
654 Error signing the mixed ballot box
655 Error: Failed mixing audit on node" + info
700 Error uploading mixed ballot boxes
701 Error verifying mixed Ballot box signature
702 Error with upload point
703 Error with ballot file: Specified file does not have data
705 Unexpected error when decrypting ballot box
706 Unexpected error when processing ecounting
800 Error during VCS check
801 Error verifying KS service
802 Error during Authentication Service check
803 Error during RCG service check
810 Error during Gateway service check
811 Error during Receipt service check
812 Error during EML verification
814 Error during Return Code Generator service check
815 Error during Min ID service check

816 Error during electoral roll service check
817 Error during Ballot Box service check
818 Error during Evote system check
819 The RBAC authentication token is not present
820 The RBAC authentication token is either expired or not valid
821 The RBAC certificate is not available or revoked
822 The RBAC signature is not valid
823 The RBAC token does not grant access
824 The RBAC election event does not match the message one
900 The mobile phone could not be obtained
901 The mobile phone is not set
INFO1 Vote has voted in paper
000 Successful Operation
000 Successful Operation - - AS checked
000 Backup receipt list
000 Ballot box restore successful operation.
000 Decrypting process finished Successful Operation.
000 Decrypting request received
000 Ecounting process finished Successful Operation.
000 Ecounting request received.
000 Electoral Roll restore successful operation.
000 Evote system check completed, please review results
000 Key access successful operation
000 Key access successful operation
000 Key access successful operation
000 Mixing Manager (Uplaod) process successful operation.
000 Mixing Manager (Upload) request successful operation.
000 Mixing Manager database successful operation - Cleansed ballot box stored into database
000 Mixing Manager database successful operation - Set point uploadPoint to database
000 Mixing Manager process successful operation - Mixing Ballot Boxes finished
000 Mixing Manager request successful operation - Mixing Ballot Boxes request received
000 Mixing Manager signature verification successful operation - Cleansed ballot box signature verified
000 Successful Cleansing and exporting cleansed ballot box
000 Successful audit mixing request for adtPoint: %d with seed: %d
000 Auditing process: %s, with seed: %d, seed+hashVotes: %d
000 "Successful Operation - Audit Mixing process finished for mxPointId: %d
000 Received and stored information for process: %d, from node: %d.
000 Successful processed and stored information to be verified by Auditor module.
000 Successful Operation - Audit Mixing finished for adtPoint %s, mxPointId %s
000 Successful Operation - Mixing Ballot Boxes finished and exported
000 Mixing Manager Submit task to mixing node.
000 Net mixing process successful operation.
000 Net mixing request successful operation.
000 Receipt list restore success
000 Receipt request received

000 Return codes generation success operation
000 Return codes sending
000 Successful Operation - Cleansing
000 Successful Operation - RCG service checked
000 Successful Operation - VCS checked, ballots:XXY
000 Successful AS token generation
000 Success verifying Schnorr Signature
000 Voting receipt generation sending operation
000 Mobile obtained
000 Send receipt
000 Backup receipt list
000 Backup Ballot Box
000 RBAC token verification succeeded
000 Upload mixed BB process successful operation
000 Upload mixed BB request successful operation
000 Voting receipt generation successful operation

Annex 2. Logs definition

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
Application activities to be registered at logs (pre-election phase)						
VCS	Processing of Election Configuration File (user, date&time, file identification)	VCS	ECPRO	EML	Hash(eml)	**000 Successful** **040 Missing EML data** **044 EML already exists**
RCG	Processing of Election Configuration File (user, date&time, file identification)	RCG	ECPRO	EML	Hash(eml)	**000 Successful** **040 Missing EML data** **044 EML already exists**
VCS	Digital signature verification of the Election Configuration File	VCS	ECVER	EML	Hash(eml)	**000 Successful** **041 Error processing the EML** **042 Error saving the zipped EML** **043 Error verifying EML signature**
RCG	Digital signature verification of the Election Configuration File	RCG	ECVER	EML	Hash(eml)	**000 Successful** **041 Error processing the EML** **042 Error saving the zipped EML** **043 Error verifying EML signature**
VCS	Key Store Upload	VCS	KEYUP	KEY	key_id	**000 Success** **035 Wrong parameters** **036 Error uploading key**
RCG		RCG	KEYUP	KEY	key_id	**000 Success** **035 Wrong parameters** **036 Error uploading key**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
AS		AS	KEYUP	KEY	key_id	**000 Success** **035 Wrong parameters** **036 Error uploading key**
Application activities to be registered at logs (during the polling phase)						
VCS	Key Store Access	VCS	KEYAC	KEY	key_id	**000 Key access successful operation** **030 Error retrieving key** **031 Key not found**
RCG		RCG	KEYAC	KEY	key_id	**000 Key access successful operation** **030 Error retrieving key** **031 Key not found**
AS		AS	KEYAC	KEY	key_id	**000 Key access successful operation** **030 Error retrieving key** **031 Key not found**
AS	Voter authentication errors (from MinID, electoral roll, or token errors)	AS	VAUTH	voter or minID token	ssn o MinID token	**001 MinID signature non valid** **002 MinID timestamp expired** **003 MinID token already used** **005 Voter not electoral roll** **006 Voter doesn't have any contest** **009 General authentication error** **010 Error getting the electoral roll** **015 Invalid user session** **016 Cannot get the voter from the Authentication token** **003 MinID token already used**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
AS	Voter authentication & Voter Authentication Token Generation	AS	TKGEN	voter or AS token	ssn o AS token	**000 Successful AS token generation** **008 P12 file not found** **020 Error signing the Authentication token**
VCS	Vote Reception	VCS	VOTRE	vote	hash(vote)	**000 successful**
VCS	Vote Checking Results	VCS	VOTCH	vote	hash(vote)	**000 Vote Checked** **055 Error while checking the vote.** **056 Unexpected exception while checking the vote.**
			VOTVL	vote	hash(vote)	**045 Vote length is different** **046 Error: SSN in Voter Certificate** **047 Voter Digital Certificate** **048 The election event not exists or is closed** **049 Contest/s specified is/are not authorized**
			MIDVL	vote	hash(vote)	**068 Error verifying MinID Token unique ID** **069 MinID Token unique ID has been received before** **070 Error validating Min ID digital signature and certificate** **071 Error validating Min ID Identification Service Issuing Time**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
			ATKVL	vote	hash(vote)	**072 Error verifying Authentication Service Digital signature and certificate** **073 Error verifyng Authentication Service Issuing Time** **074 Error verifyng Authentication Expiration Time** **075 Auth Token unique ID has been received before** **076 Error verifying Auth Token unique ID**
			SCHVL	vote	hash(vote)	**077 Error verifying Schnorr Signature**
VCS	Partial Decrypt, Vote's test calculation, and Vote reencryption	VCS	VOTTC	vote	hash(vote)	**000 successful** **050 Error doing Partial decrypt, test calculation or reencryption**
VCS	Vote sending to the RCG	VCS	VOTSN	vote	hash(vote)	**000 Successful** **051 Error sending the vote to RCG**
RCG	Reception from VCS (vote, reencryption, vote's test)	RCG	VOTRE	vote	hash(vote)	**000 Receipt request received**
RCG	Vote Checking Results	RCG	VOTCH	vote	hash(vote)	**000 Successful** **055 Error while checking the vote.** **056 Unexpected exception while checking the vote.**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
			VOTVL	vote	hash(vote)	**045 Vote length is different** **046 Error: SSN in Voter Certificate** **047 Voter Digital Certificate** **049 Contest/s specified is/are not authorized**
			MIDVL	vote	hash(vote)	**068 Error verifying MinID Token unique ID** **069 MinID Token unique ID has been received before** **070 Error validating Min ID digital signature and certificate** **071 Error validating Min ID Identification Service Issuing Time**
			ATKVL	vote	hash(vote)	**073 Error verifyng Authentication Service Issuing Time** **074 Error verifyng Authentication Expiration Time** **075 Auth Token unique ID has been received before** **076 Error verifying Auth Token unique ID**
			SCHVL	vote	hash(vote)	**078 Error verifying Vote Schnorr Signature** **079 Error verifying Exp Schnorr Signature** **080 Error verifying Key Schnorr Signature** **000 Successful Schnorr Signature**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
RCG	RCG Filter - vote digital signature and partial decryption.	RCG	VOTTV	vote	hash(vote)	**081 Error in vote digital signature.** **082 Error in vote partial decryption**
RCG	Voting Receipt Generation	RCG	REGEN	vote	hash(vote)	**000 Voting receipt generation successful operation** **400 Voting receipt generation error**
RCG	Voting Receipt sending	RCG	RESND	receipt	hash(vote)	**000 Voting receipt generation sending operation**
RCG	Return Codes Generation	RCG	RCGEN	vote	hash(vote)	**000 Return codes generation Success operation** **401 Return codes generation error**
RCG	Mobile phone gathering	RCG	RCMOB	Voter	SSN	**000 Mobile obtained** **900 The mobile phone could not be obtained** **901 The mobile phone is not set**
RCG	Return Codes Sending	RCG	RCSND	vote	hash(vote)	**000 Return codes sending** **402 Return codes sending error**
VCS	Vote Storage	VCS	VOTST	vote	hash(vote)	**000 Successful** **052 Error storing the vote**
VCS	Voting Receipt sending to the applet	VCS	RESND	receipt	Hash(vote)	**000 Send receipt**
VCS	Ballot Box export (to Cleansing)	VCS	BBEXP	BB	BB_id	**000 Backup Ballot Box** **404 Backup Ballot Box error**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
RCG	Receipt list export (to Cleansing)	RCG	RLEXP	Receipt list	Receipt_list id	**000 Backup receipt list** **403 Backup receipt list error** error1 signature error
ALL	RBAC Authorization	ALL	RBACA	Securable Object	Securable_string	**000 Rbac token verification succeeded** **819 The RBAC authentication token is not present** **820 The RBAC authentication token is either expired or not valid** **821 The RBAC certificate is not available or revoked** **822 The RBAC signature is not valid** **823 The RBAC token does not grant access** **824 The RBAC election event does not match the message one**
Audit verification to be registered at logs (audit functions executed at start-up and periodically)						
VCS	Digital signature verification of the Election Configuration File	VCS	ECVER	EML	**Hash(eml)**	**812 Error during EML verification**
RCG	Digital signature verification of the Election Configuration File	RCG	ECVER	EML	**Hash(eml)**	**812 Error during EML verification**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
VCS	Verification of the configuration file vs configuration database	VCS	ECDBV	EML	**Hash(eml)**	**812 Error during EML verification**
RCG	Verification of the configuration file vs configuration database	RCG	ECDBV	EML	**Hash(eml)**	**812 Error during EML verification**
AS	Service-Check	AS	SRVCK	Election	election_id	**000 Successful Operation - - AS checked** **802 Error during Authentication Service check** **801 Error verifying KS service** **816 Error during electoral roll service check** **815 Error during Min ID service check**
VCS	Service-Check	VCS	SRVCK	Election	election_id	**000 Successful Operation - VCS checked, ballots:XXX** **800 Error during VCS check** **801 Error verifying KS service** **812 Error during EML verification** **817 Error during Ballot Box service check** **000 Evote system check completed, please review results** **818 Error during Evote system check**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
RCG	Service-Check	RCG	SRVCK	Election	election_id	**000 Successful Operation - RCG service checked** **803 Error during RCG service check** **801 Error verifying KS service** **810 Error during Gateway service check** **811 Error during Receipt service check** **812 Error during EML verification** **814 Error during Return Code Generator service check**
Application activities to be registered at logs (during the tallying phase)						
CL	Data imports at cleansing (ballot box, voting receipts, paper electoral roll, …)	CL	DAIMP	BABOX	BB_id	**000 Ballot box restore successful operation.** **500 Error restoring ballot box**
				RCPTL	Receipt List_id	**000 Receipt list restore success** **502 Error restoring receipts list**
				ELCRO Paper ER	Electoral Roll_id Paper ER_id	**000 Electoral Roll restore successful operation.** **501 Error restoring Electoral Roll**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
CL	Cleansing activities (checking results, rejected votes,...)	CL	VERIF	BB	BB_id	**512 - There is another vote casted before by the same voter** **513 - There is another controlled environment vote casted by the same voter** **521 - SSN stored in Voter digital certificate is not equal to voter identifier** **514 – Error verifying Voter Digital certificate using local CA** **515 - Error verifying Voter Digital signature using voter digital certificate** **516 - Vote time stamp is not from the past** **517 - Vote time stamp is not in the voting period** **519 - AuthTokenId has been received before for the same contest** **520 - Internal AuthTokenId has been received before for the same contest** **522 - SSN stored in AuthToken is not equal to voter identifier** **523 - Error verifying Schnorr signature using SSN stored in AuthToken** **524 - Error verifying Authentication Service certificate using local CA** **529 - Error verifying Authentication Service digital signature using**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
						Authentication Service certificate **525 - Authentication time stamp is not from the past** **526 - Authentication time stamp is not in the voting period** **527 - ContestId is not one of the allowed contests in AuthToken** **528 - Error verifying MinID digital signature and certificate** **530 - Error verifying RCG Digital certificate using local CA** **532 - Error verifying a vote in VCS has its corresponding receipt in RCG**
CL	Cleansing activities (checking results, rejected votes,...)	CL	VERIF	BB	BB_id	**531 - Error verifying RCG Digital signature using RCG digital certificate** **533 - The difference between receipt time stamp and vote time stamp exceed the limit of time between authentication and voting** **534 - The difference between receipt time stamp and authentication time stamp exceed the limit of time between authentication and voting** **535 - Receipt time stamp is not from the past** **536 - Receipt time stamp is not in the voting period**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
						511 - There is another paper vote casted by the same voter **510 - Voter SSN is not in Electoral Roll** Error13 Vote length error
CL	Cleansing exceptions and errors.	CL	CLREA	BB Receipt List Electoral Roll Paper ER	BB_id Receipt List_id Electoral Roll_id Paper ER_id	**000 Successful Operation - Cleansing** **540 - Error at cleansing** Exception Error
CL	Votes selection at cleansing.	CL	CLSEL	BB	BB_id	Success Exception Error
CL	Ballot Box export at Cleansing (cleansed ballot box: user, date&time).	CL	CLEXP	CL_BB	CL_BB_id	**000 Successful Cleansing and exporting cleansed ballot box** **540 Error at cleansing + info**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
MX	Data imports at mixing server (cleansed ballot box: user, date&time).	MX	DAIMP	CL_BB	UplPointId	**000 Mixing Manager (Upload) request successful operation.** **000 Mixing Manager (Uplaod) process successful operation.** **600 Failed Uploading Cbbs on Mixing Manager** **601 Error verifying cleansed ballot box signature** **000 Mixing Manager database successful operation - Set point uploadPoint to database** **000 Mixing Manager signature verification successful operation - Cleansed ballot box signature verified** **000 Mixing Manager database successful operation - Cleansed ballot box stored into database**
MX	Data imports at mixing server (cleansed ballot box: user, date&time).	MX	DAIMP	NODE	mxPointId	**000 Net mixing request successful operation.**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
MX	Mixing activities (for each voting groups, date&time, amounts, and successfull or not)	MX	MXACT	Node	mxPointId	**000 Net mixing process successful operation.** **651 Error verifying incoming Ballot box signature** **652 Error: Failed Net Mixing on node** **653 Error exporting the mixed ballot box** **654 Error signing the mixed ballot box** Exception Error
MX	Auditor data input (user, date&time)	MX	AUDIN			**000 Successful audit mixing request for adtPoint: %d with seed: %d** **000 Auditing process: %s, with seed: %d, seed+hashVotes: %d** **609 Error in Mixing Audit: + info**
MX	Mixing Proof Generation	MX	PROOF	Node	Node_id	**000 "Successful Operation - Audit Mixing process finished for mxPointId: %d** **655, "Error: Failed mixing audit on node" + info**
MX	Auditor data export (date&time)	MX	DAEXP	Node	Node_id	**000 Received and stored information for process: %d, from node: %d.** **000 Successful processed and stored information to be verified by Auditor module.** **609 Error in Mixing Audit: + info**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
MX	The mixing process will generate information regarding voting groups (locations) and number of votes processed per group.	MX	MXACT	Mixed BB	mxPointId	**000 Mixing Manager request successful operation - Mixing Ballot Boxes request received** **000 Mixing Manager process successful operation - Mixing Ballot Boxes finished** **602 Failed Mixing Ballot Boxes on Mixing Manager** **604 Error: Upload point uplPointId not found** **605 Error: There are no cleansed ballots for uploading point specified:** **000 Mixing Manager Submit task to mixing node.** **606 Error: Thread execution has been canceled due to an exception:** **607 Error: Create output zip file has been failed:** Exception Error
MX	Mixed Ballot Box export at Mixing Server.	MX	MXEXP	Mixed BB	Mixed BB_id	**000 Successful Operation - Mixing Ballot Boxes finished and exported** **602 Error: Failed Mixing Ballot Boxes on Mixing Manager + info**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
CO	Data imports at counting server mixed ballot box: user, date&time).	CO	COIMP	Mixed BB	uploadPointId	**000 Upload mixed BB request successful operation** **000 Upload mixed BB process successful operation** **700 Error uploading mixed ballot boxes** **701 Error verifying mixed Ballot box signature** **702 Error with upload point** **703 Error with ballot file: Specified file does not have data**
CO	Ballot box decryption	CO	BBDEC	Mixed BB	uploadPointId	**000 Decrypting request received** **000 Decrypting process finished Successful Operation.** **705 Unexpected error when decrypting ballot box**
CO	Vote errors at counting.	CO	VTERR	vote	vote	**710 Error in vote factorization, remaining product is not one. mxsBallot.uuid = + mxsBallot.getDbid()** **711 Error in vote factorization, number of vote options is greater than maximum vote length for that contest. mxsBallot.uuid = + mxsBallot.getDbid()**

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
CO	Counting results	CO	COUNT	Dec BB	dcrPointId	**000 Ecounting request received.** **000 Ecounting process finished Successful Operation.** **706 Unexpected error when processing ecounting** Exceptions

		COMPONENT	ACTION	OBJECT TYPE	OBJECT ID	OUTCOME
TPM	Attestation Build Machine Attestation Build baseline Attestation Attestate Attestation Load P12 Attestation Preconditions check Attestation Connect Attestation Connection Completed Attestation Response Attestation validate report signature Attestation validate report Attestation validate quote Attestation compare to baseline Attestation init logger	TPM	ATTBM ATTBB ATTAT ATP12 ATTPR ATTCN ATTCC ATTRP ATTVS ATTVR ATTVQ ATTCB ATTIL	ATTLA ATTVA ATTIT ATTPR ATTPP ATTMC ATTHS ATTLO	Attestation Latest Attestation Validation Attestation Item Attestation Attestation Precondition Passed Attestation Machine Attestation Host Attestation Logger	300 Error on attestation tool 301 received PCRs don't match baseline 302 Quote Validation failed 303 Attestation tool reported ERROR 304 Can't run AIK Quote Verification 305 Can't read PCR's from quote 306 Error reading report for validation 307 Received report doesn't contain neither valid nor invalid hooks 308 Error connecting to remote host 309 Invalid key format 310 Cryptographic operation failed 311 Error persisting message 312 Report Signature Validation Failed 313 Failed Validation 314 Failed Validation with Exception (see comments) 315 Failed Report Validation 316 Error reading certificate 317 IOError 318 No report received 319 Received empty signature 320 Error reading from host: timeout 321 Received report has no hooks

Annex 3. Activities which are not being logged

The following operations are not being registered in the immutable logs.

Key Management Process		
KMS	**Key Generation**	The keys are being registered in the “upload” process into the different key stores, not when generated.
KMS	**Key distribution**	It is delegated to the operating system audit.
Voting Process		
PC	**Voter activities at the applet**	The voter activities at his/her PC will not be registered.
VCS	**The voting options.**	Only the hash of the encrypted vote is being registered. The voting options are private.
RCG	**The generated return codes**	The action of return codes generation is registered. But the return codes are confidential.
RCG	**The phone number of the voter**	It is private information. Only the hash of the number is registered.
Tallying Process		
MX	**Mixing operations**	The privacy of the ballot box could be compromised.
CO	**Electoral Board KEY reconstruction**	This operation is done in the client, which is not registering logs.
CO	**Administration Board KEY reconstruction**	This operation is done in the client, which is not registering logs.