5

Requirements for Electronic Voting Machines

The previous chapter describes the requirement development process – including quality assurance measurements – and presents the applied syntax and semantics. The results of this development process are two large, standardised, consistent, and exhaustive lists of requirements. This chapter defines the requirements for stand-alone direct recording electronic voting machines. Before providing the list of requirements the chapter-specific notation is explained; meaning those notations used for this chapter but not in the requirements definition for remote electronic voting systems. In addition, the exact target of evaluation under consideration for the requirement specification is defined. Then, the two main subgroups of system requirements - security and functional requirements - are presented separately. Both parts distinguish between requirements for the polling phase and those requirements for the tallying phase. In addition, the list of functional requirements contains detailed requirements for the audit system. The last part specifies the assurance, usability[1], and operational requirements.

5.1 Citation and Additional Notations

The security and functional requirements listed in this chapter represent a further improvement on the requirements that are listed in [156]. In addition to extensions and textual changes, the requirements have been reordered according to section 4.4. In particular this contains the following aspects:

[1] Although usability requirements belong to the category of system requirements, they are discussed in a different section because these requirements are not further treated in the evaluation part.

M. Volkamer: Evaluation of Electronic Voting, LNBIP 30, pp. 73–91, 2009.

- They are separated into security requirements, which are deduced from threats, and functional requirements, which refer to organisational security policies[2].
- The requirements are labelled by names or shortcuts rather than numbers as in [156].

To indicate the relationship between [156] and the requirements listed here, corresponding labels are added by "Paper Sec_x, Funct_y". The security and functional requirements are categorised into the following sub classes: those that need to hold during the polling phase and those that need to be ensured 'only' after the polling phase. The functional requirement subsection also contains a list of requirements for the audit system.

5.2 Target of Evaluation

The requirements below mainly address one particular group of electronic voting systems, namely those called **stand-alone direct recording electronic voting machines in polling stations** (see Sect. 2.1 and 2.3.1), that is, votes are cast and stored on dedicated electronic voting machines that are not networked. The electronic voting machines in mind should be used instead of traditional polling station elections. Corresponding to the definition of a "stand-alone electronic voting machine in polling stations" in Sect. 2.1, voter registration, identification, and authentication is accomplished manually (the same processes and techniques as in traditional paper-based elections in polling-stations). Thus, the considered target of evaluation does not provide voter registration, voter identification, or voter authentication functionality. Corresponding requirements are therefore not considered. In addition, the functionality of the target of evaluation only covers the polling phase and the tallying phase. Thus, the election setup and archiving phase are not addressed in the security and functional requirements. Instead, it is assumed that the electronic voting machines are set up correctly and contain the proper candidate list and the proper definition of valid and invalid votes (that is, in general proper configuration)[3]. In addition, it is assumed that the machines are set up in polling booths. Therefore, requirements to ensure a protected environment are not addressed. The target of evaluation includes the following components:

- The electronic voting machine with the vote-casting interface.
- A connected poll worker interface to enable and disable the vote-casting interface.
- The tallying software. It can either run on the electronic voting machine or on another external device, such as an arbitrary work station.

[2] In [156] the requirements are also categorised into security and functional requirements, but the separation criteria are not clear.

[3] However, one requirement (that is, O.OSP.SelfCheck) demands that poll workers have the ability to check the configuration before starting the polling phase.

5.3 Security Requirements

5.3.1 Security Requirements for the Polling Phase

T.AC: An outside intruder gets access to the ·*electronic voting machine*· without knowing or having the access tokens to tamper the ·*electronic voting machine*· in order to reach any of his goals.	–
O.T.AC [all] The ·*electronic voting machine*· `shall` implement an access control policy which restricts all activities on the ·*poll worker interface*· to particular ·*user*·-roles.	Paper Sec_3
T.Tamper: An inside intruder tampers with the ·*electronic voting machine*·, altering its appearance, behaviour, and/or internal data in order to reach any of his goals (for instance, to affect the ·*election result*· by altering, adding or deleting ·*votes*·).	–
O.T.Tamper [all] The ·*electronic voting machine*· (including the ·*e-ballot box*·) `should` be tamper-resistant. The ·*electronic voting machine*· (including the ·*e-ballot box*·) `shall` be tamper-evident. ***Appl. Note:*** The only interfaces to the ·*electronic voting machine*· should be the ·*vote-casting interface*· (including those designed for ·*voters*· with disabilities) and ·*poll worker interfaces*·. Where other interfaces exist they shall be disabled.	BWGV-A1 B(2.1b, 2.4a) CoE [15, 29, 34a, 80, 86a/c, 92] PTB VP[1-2, 4-3, 4-4, 5-2b], CF[1-9b] Paper Sec_15
T.UnauthVotesA: A malicious ·*elector*· logs on the ·*electronic voting machine*· for a second time to cast another ·*vote*· in order to affect the ·*election result*·.	–
T.UnauthVotesB: An outside intruder adds ·*e-vote*· using other interfaces than the ·*vote-casting interface*· in order to affect the ·*election result*·.	–

O.T.UnauthVotes [di] The ·*electronic voting machines*· `shall` ensure that ·*e-votes*· can only be added through the ·*vote-casting interface*· and only during the ·*polling phase*·. ***Appl. Note:*** The ·*electronic voting machine*· shall be automatically put in an ·*inactive state*· after the ·*voting process*· is finished. The ·*poll worker interface*· should provide the functionality to put the ·*electronic voting machine*· in an ·*inactive state*·.	BWGV-A1 B [3.1b, 3.6a-d] CoE [5a, 91, 94b, 96a] PTB VP[1-6, 3-13, 3-17] Paper Sec_1, 12, 18, 19
T.SepDuty: An inside intruder abuses his access privileges to tamper with the ·*electronic voting machine*· in order to reach any of his goals.	–
O.T.SepDuty [all] The access control mechanism `shall` only allow access to the ·*electronic voting machine*·, if at least two different ·*users*· are logged in.	CoE [33]
T.ElectionSecrecy: An in-/outside intruder gets access to the ·*electronic voting machine*· and uses the stored information to link ·*voters*· to their ·*votes*· in order to compromise the secrecy of the vote.	–
O.T.ElectionSecrecy [se] The ·*electronic voting machine*· `should` not store any information which could link the ·*voter*· with his ·*vote*· after the completion of the ·*voting process*·. Where any information which could link the ·*voter*· to his ·*vote*· is stored on the ·*electronic voting machine*·, it `shall` only be accessible to those with appropriate authority. ***Appl. Note:*** The ·*electronic voting machine*· shall store the ·*e-votes*· in a history independent way (that is, the ·*vote casting*· order shall not be preserved and no timestamp shall be stored with the ·*e-vote*·). ***Appl. Note:*** According to O.T.Tamper the electronic voting machine shall be tamper-evident meaning tampering can be detected but with respect to the protection of the secrecy of the vote, it is then already too late.	CoE [16, 17, 34b, 35] PTB VP[1-2, 3-15, 5-2a], CF[1-9c, 3-1, 3-2] Paper Sec_11

T.AvailInfo: An in-/outside intruder in or close by the polling station sees, hears, or measures information provided by the ·*voting process*· in order to compromise the secrecy of the vote.	–
O.T.AvailInfo [se] During the ·*polling phase*· the ·*electronic voting machine*· `shall` not give any information about the ·*voting process*· outside the ·*vote-casting interface*·, except for the current ·*electronic voting machine*· state (·*active state*· or ·*inactive state*·), the number of ·*votes*· ·*cast*· so far, and feedback according to O.T.NegFeedback. ***Appl. Note:*** The ·*electronic voting machine*· shall prevent any emissions which might endanger the secrecy of the ·*vote*·. This includes any kind of sounds and detectable radio waves. The ·*electronic voting machine*· shall protect the secrecy of the ·*vote*· against power analysis.	Paper Funct_1, 2, 3
T.SecrecyAfterBreakd: An inside intruder with access to the ·*electronic voting machine*· after a ·*electronic voting machine*· breakdown, exception, or malfunction reads the last ·*voter's*· ·*selections*· and/or ·*vote*· in order to compromise the secrecy of the vote.	–
O.T.SecrecyAfterBreakd [se] In case of ·*electronic voting machine*· breakdowns, exceptions, and malfunctions, it `shall` not be possible to link the last ·*voter*· with his ·*selections*· or ·*vote*·.	CoE [16, 19] Paper Sec_9

5.3.2 Security Requirements for the Tallying Phase

T.AffectCounting: An in-/outside intruder installs malware on the machine running the ·*tallying software*· in order to affect the ·*election result*·.	–
O.T.AffectCounting [di] The ·*tallying software's*· operations and data `shall` be unaffected by other applications.	BWGV-A1 B[2.2, 2.5, 3.7c] CoE [26b], PTB CF[1-2, 1-7] Paper Sec_24

T.IntegElecData: An inside intruder tampers with ·*election data*· after the ·*tallying phase*· in order to affect the ·*election result*· in the case of recounts.	–
O.T.IntegElecData [di] The ·*tallying software*· `should` protect the integrity of ·*election data*· (at least including: ·*votes*·, ·*results*·, and audit information) as soon as results are calculated.	BWGV-A1 B[3.4f] CoE [57, 75b, 97] PTB DR[2-7], CF[1-7] Paper Sec_25
T.IntegVotes: An inside intruder tampers with ·*e-votes*· after the ·*polling phase*· and before the ·*tallying phase*· in order to affect the ·*election result*·.	–
O.T.IntegVotes [di] The ·*electronic voting machine*· `shall` protect the integrity and authenticity of ·*e-votes*· as soon as the ·*polling phase*· is closed.	Paper Sec_14
O.T.AuthCheckCount [di] The ·*tallying software*· `shall` verify the integrity and authenticity of ·*e-votes*· before starting the ·*tallying phase*·.	CoE [34c, 86b, 97, 107c] PTB DR[1-3, 2-7] Paper Sec_23
T.LinkInParalElec: An inside intruder with access to ·*e-votes*· after the ·*polling phase*· discovers some aspect of ·*voters'*· identities by examining ·*votes*· that were cast together. For instance, non-citizen residents may have limited voting rights. An intruder could determine which votes came from a particular community.	–
O.T.LinkInParalElec [se] [non-core] The ·*electronic voting system*· `shall` prevent anyone from linking different ·*e-votes*· from the same ·*voter*· to one another (when parallel ·*polls*· are run).	BWGV-A1 B[2.4b] Paper Sec_16

5.4 Functional Requirements

5.4.1 Functional Requirements for the Polling Phase

O.OSP.NeutInter [fr] The ·*electronic voting machine*· and the ·*vote-casting interface*· `shall` be optically neutral.	BWGV-A1 B[3.3a] CoE [90a]
O.OSP.EqualPres [fr] The ·*electronic voting machine*· `shall` ensure equality and accuracy of presentation of ·*voting options*·. ***Appl. Note:*** The ·*electronic voting machine*· shall avoid the display of influencing messages.	BWGV-A1 B[3.3b] CoE [12, 47, 48] PTB VP[3-1 – 3-3, 3-5, 3-8] Paper Funct_4
O.OSP.AccurDisp [fr] The ·*electronic voting machine*· `shall` accurately display the authentic and unaltered ·*ballot*·.	CoE [90a] PTB VP[3-1, 3-2, 3-3] Paper Funct_6
O.OSP.PosFeedback [tr] The ·*electronic voting machine*· `shall` provide feedback to the ·*voter*· regarding the status of his ·*vote*· (It `shall` at least contain the information that his ·*e-vote*· has been successfully stored in the ·*e-ballot box*·).	Paper Usab_5
O.OSP.PWClosePoll [all] The ·*poll worker interface*· `shall` warn the ·*poll workers*· if they try to close the ·*election*· before the final date.	–
O.OSP.Spoil [fr] [non-core] The ·*vote-casting interface*· `should` provide the functionality for the ·*voter*· to ·*spoil*· his ·*vote*·.	BWGV-A1 A[a]
O.OSP.SpoilWarning [fr] [non-core] The ·*vote-casting interface*· `should` warn the ·*voter*· when he tries to ·*spoil*· his ·*vote*· in one or more ·*polls*·.	PTB VP[3-9] Paper Funct_12
O.OSP.StoreAllVotes [di] The ·*electronic voting machine*· `shall` store all ·*e-votes*· ·*cast*· over the ·*vote-casting interface*· in the ·*e-ballot box*·.	BWGV-A1 A[b,1]

O.OSP.NoInteraction [un] The ·*electronic voting machine*· `shall` prevent ·*voter*· interaction in case of exceptions and malfunctions.

PTB CF[1-12]
Paper Sec_7

O.OSP.Robust [un] The ·*electronic voting machine*· `shall` be robust against power outage, unexpected ·*user*· activities, and environmental effects (for instance, mechanical, electromagnetic, and climatic).

BWGV-A1 B[2.2,2,3,2.5,3.7c]
CoE [30]
PTB CF[1-7, 1-9a]
Paper Funct_13, _14

O.OSP.InfoPW [di] [non-core] The ·*electronic voting machine*· `shall` indicate to the ·*poll worker*·

- the number of ·*votes*· ·*cast*· so far and
- its current state.

BWGV-A1 B[3.4d]
PTB VP[1-7]

O.OSP.V-Interface [fr] The ·*vote-casting interface*· `shall` provide the functionality for the ·*voter*· to

- change his ·*selections*· before ·*casting his vote*·,
- easily cancel his ·*voting process*· at any time, and
- clear all his ·*selections*·.

BWGV-A1
B[3.3c/d,3.6b/d/f]
CoE [11, 13]
PTB VP[3-10b, 3-11, 3-14]
Paper Funct_11

O.OSP.PWInterface [se] [fr] The only functionality provided by the ·*poll worker interface*· is

- starting the ·*polling phase*· (which is only possible once),
- resuming the ·*polling phase*· after breakdowns or other problems (according to O.OSP.ErrorRecovery),
- closing the ·*polling phase*· (after which only the export of data and in particular ·*e-votes*· is possible),
- acting according to messages from O.OSP.NegFeedback, and
- checking the ·*electronic voting machine*· in arbitrary ways (according to O.OSP.SelfCheck).

Appl. Note: The ·*electronic voting machine*· shall not provide any functionality to calculate ·*results*· during the ·*polling phase*·.

BWGV-A1 B[3.4f,3.5c/d/e]
CoE [34a, 53a]
PTB PE[4-10b], DR[1-3, 2-1],
VP[3-17, 4-3a, 5-2a, 5-6]
Paper Sec_13

O.OSP.DeleteRecord [se] Whenever a ·*voter*· completes his ·*voting process*· (by ·*casting*· his ·*vote*· or ·*canceling his voting process*·) any records of his ·*voting process*· `shall` be deleted from display.

CoE [11, 52a, 93a]
PTB VP[3-16]
Paper Sec_10

O.OSP.Availability [un] The ·*electronic voting machine*· `shall` be available during the whole ·*polling phase*·.

Appl. Note: Any backup system shall ensure the same requirements as the main voting system.

CoE [70b]
PTB PE[4-5]

O.OSP.PWCheck [all] The ·*poll worker interface*· `shall` provide the functionality to check that the ·*electronic voting machines*· have been set up correctly (for example, order of ·*voting options*· and empty ·*e-ballot box*·).

PTB PE[4-10a]

O.OSP.LastVote [un] The ·*electronic voting machine*· `shall` provide the functionality to determine whether the ·*e-vote*· of the last ·*voter*· was successfully stored in the ·*e-ballot box*· in case of

- exceptions,
- malfunctions, and
- after ·*electronic voting system*· breakdowns.

Paper Sec_8

O.OSP.ErrorRecovery [di] [un] The ·*voting server*· `shall` run a self-check before s resuming is possible. In the case of irreversible problems the ·*voting server*· `shall` prevent a resuming of the ·*polling phase*·.

PTB CF[2-3]

O.OSP.Auditing [tr] The ·*electronic voting machines*· `shall` be capable of producing comprehensive audit data.

CoE [59, 83a, 102, 104]
PTB PE[4-3b], CF[4-1]
Paper Sec_4

O.OSP.NegFeedback [un] The ·*electronic voting machine*· `shall` provide feedback in the form of error messages in case of exceptions and malfunctions.

BWGV-A1 B[3.2b]
PTB VP[5-5a]
Paper Sec_6

O.OSP.DataLoss [di] The ·*electronic voting machine*· `shall` prevent data loss during normal operations and in case of

- exceptions,
- malfunctions, and
- after ·*electronic voting system*· breakdowns.

BWGV-A1 B[2.3, 3.4e]
CoE [34a, 77, 99]
PTB VP[3-9, 5-3], CF[1-9a, 1-11]
Paper Sec_2

O.OSP.AccurRep [fr] The ·*electronic voting machine*· `shall` ensure that the ·*voter's*· ·*selections*· are accurately represented in the ·*e-vote*·.

Appl. Note: Some recommend the provision of a voter-verified paper audit trail. But this points is controversial and disputed. This aspect is not further discussed in this book. However, it is addressed in [99].

BWGV-A1 B[3.3c/e]
CoE [95]
PTB VP[4-1, 4-2]
Paper Funct_5

O.OSP.SelfCheck [tr] The ·*electronic voting machine*· `should` regularly perform automatic self-checks while it is in the ·*inactive state*·. The ·*electronic voting machine*· `shall` be capable of performing self-checks.

Appl. Note: The ·*electronic voting machine*· should automatically check that the ·*e-ballot box*· is empty before the ·*polling phase*· begins. The ·*poll worker interface*· `shall` provide the functionality to check that the ·*electronic voting machine*· has been set up correctly.

BWGV-A1 B[3.2a, 3.5a/b]
CoE [72a, 79, 89b]
Paper Sec_20, _21

O.OSP.CompatClient [all] [non-core] The ·*electronic voting machine*· `should` be compatible with other devices (such as those used by people with disabilities) where appropriate.

CoE [64, 66, 67, 68]
Paper Funct_10

O.OSP.AdequNoVotes [un] [non-core] The ·*electronic voting machine*· `shall` be capable of recording an adequate number of ·*votes*·.

BWGV-A1 B[3.4a]
Paper Funct_8

O.OSP.AdequNoBallotOpt [fr] [non-core] The ·*electronic voting machine*· `shall` support an adequate number of ·*voting options*·

BWGV-A1 B[3.3e]
Paper Funct_9

5.4.2 Functional Requirements for the Tallying Phase

O.OSP.ReadToOtherSystems [tr] The ·*electronic voting system*· `shall` not obstruct the use of alternative ·*tallying software*· to calculate results.	BWGV-A1 B[3.4g/h] CoE [26a] PTB DR[2-5, 2-6] Paper Funct_7
O.OSP.AccurCalc [di] The ·*tallying software*· `shall` accurately calculate and display results using the appropriate algorithm based on all ·*e-votes*· stored in the ·*e-ballot box*· and only based on these ·*e-votes*·.	BWGV-A1 B[3.4b/c/d, 3.5a] CoE [7, 98] PTB VP[5-1], WS[1-2], DR[2-2, 2-3, 2-5, 2-6] Paper Sec_22
O.OSP.Delete [di] The ·*electronic voting machines*· `shall` provide the functionality to completely delete data from previous ·*elections*·.	Paper Sec_5

5.4.3 Functional Requirements for the Audit System

O.OSP.Audit1 [tr] The ·*audit system*· `shall` provide the functionality to record, monitor, and verify audit data.	CoE [101]
O.OSP.Audit2 [tr] The ·*audit system*· `shall` protect the integrity and authenticity of audit records.	CoE [83b, 83c, 109] PTB CF [2-2, 2-6]
O.OSP.Audit3* [tr] The ·*audit system*· `shall` have access to a reliable time source.	CoE [83b, 84, 84b]
O.OSP.Audit4* [tr] The ·*audit system*· `shall` record system configuration and ·*election*· configuration on all ·*electronic voting machines*· at least at the following points • beginning and end of ·*polling phase*·, as well as • before and after tallying.	CoE [100, 103, 106]
O.OSP.Audit5* [tr] The ·*audit system*· `shall` check the ·*e-ballot box*· and the ·*ballot*· content for evidence of tampering.	CoE [107] PTB CF [4-2]

O.OSP.Audit6 [tr] The ·*audit system*· and its records `should` be tamper-resistant and `shall` be tamper-evident.	CoE [83, 109] PTB CF [4-4]
O.OSP.Audit7* [tr] For every action performed by ·*poll workers*· the ·*audit system*· `shall` record a timestamp, the nature of the action, and the ID of the particular ·*poll worker*·(where available).	CoE [100]
O.OSP.Audit8 [tr] The ·*audit system*· `shall` record (with timestamps, where appropriate) breakdowns, exceptions, malfunctions, and results of any self-checks.	CoE [100, 103c] PTB CF[2-5, 4-3]
O.OSP.Audit9 [tr] The ·*audit system*· `shall` implement the access control policy defined by the ·*responsible election authority*·.	CoE [23, 56, 104, 105] PTB [CF 4-4]
O.OSP.Audit10* [tr] The ·*audit system*· `should` not record any information which might endanger the secrecy of the vote. Where such information is stored it `shall` only be accessible to those with appropriate authority.	CoE [106]

5.5 Assurance Requirements

Assur.1 [all] The ·*responsible election authority*· `shall` define the trust model for their particular ·*election*·.	–
Assur.2 [all] The ·*manufacturer*· `shall` develop the ·*electronic voting machines*· according to software engineering best practice, including use of version control, and bug tracking for all documents and source code.	BWGV-A1 B[2.1a] PTB CF [1-4, 1-5]

Assur.3* [all] The ·*manufacturer*· `shall` produce the following documents ensuring that they are exhaustive, consistent, unambiguous, appropriate, comprehensible, and concise:

- Complete system specification
- Implemented security functions
- Requirement conformance claim
- Description of each component
- Environmental assumptions
- Testing record
- Development security measures
- User-guide containing
  - normal use instructions for all ·*users*· for all phases
  - appropriate responses to all system messages
- delivery procedure

BWGV [§2(6),§7(1a)]
BWGV-A1 B[1, 4]
PTB PE [3-1, 4-1, 4-2],
VP [5-5],
CF [1-4, 1-6]

Assur.4 [un] The ·*manufacturer*· `shall` build the ·*electronic voting system*· from reliable components.

BWGV-A1 B[2.3]
PTB CF [1-8]

Assur.5* [tr] The ·*manufacturer*· `shall` disclose the documentation from O.OSP.Assur3, executable program, source code, bug tracking, and version control (at least to the ·*testing authority*·).

BWGV-A1 B[1]
CoE [24]
PTB CF [1-1, 3-3]

Assur.6* [all] The ·*manufacturer*· `shall` test the ·*electronic voting machines*·, including functional and usability tests.

CoE [25, 66]
PTB PE [2-4, 4-8, 4-9]

Assur.7 [fr] [un] [non-core] The ·*manufacturer*· `should` involve ·*users*· in the interface development process.

CoE [62]

Assur.8* [all] The ·*testing authority*· `shall` do a risk analysis based on the threat model.

CoE [28]
PTB CF [2-6]

Assur.9* [all] The ·*manufacturer*· `shall` limit the functionality of the ·*electronic voting machines*· and ·*tallying software*· to that necessary for the ·*election*·.	BWGV-A1 A[f] PTB CF [1-2]
Assur.10* [all] The ·*testing authority*· `shall` evaluate the ·*electronic voting machines*· against the requirements. Tests `shall` include penetration, and usability tests.	CoE [25, 28, 72a] PTB PE [2-4, 4-8], CF [1-3, 3-4]
Assur.11* [all] The ·*testing authority*· `shall` examine the ·*manufacturer's*· documentation from O.OSP.Assur2, executable program, source code, bug tracking, and version control for compliance with requirements and software engineering best practice.	CoE [25, 28, 72a] PTB PE [4-8], CF [1-3, 3-4]
Assur.12* [all] The ·*testing authority*· `shall` examine the delivery procedures for the ·*electronic voting machines*·, the identified development security measures, and the applied software engineering approach.	CoE [28]

5.6 Additional Requirements

5.6.1 Usability Requirements

Usab.1 [un] All user interfaces `shall` be user-friendly.	BWGV-A1 B[3.1d] CoE [1b, 65] PTB PE [1-2, 3-1], DR [1-5, 2-4], VP [1-3, 1-7, 3-12]
Usab.2 [un] [fr] All system messages provided by all user interfaces `shall` be understandable.	BWGV-A1 B[3.7] CoE [1a]
Usab.3 [un] The ·*vote-casting interface*· `shall` make provision for ·*voters*· with disabilities.	CoE [3, 61, 63]
Usab.4* [eq] The ·*vote-casting interface*· `shall` clearly indicate to the ·*voter*· whether the ·*electronic voting machine*· is in the ·*active state*·.	–

Usab.5* [tr] The ·*vote-casting interface*· `shall` provide immediate feedback to the ·*voter*· regarding the status of his ·*vote*·.	BWGV-A1 B[3.6g] CoE [14] PTB VP [3-18, 3-19]
Usab.6* [fr] The ·*vote-casting interface*· `shall` protect the ·*voter*· from accidentally ·*casting*· his ·*vote*·	BWGV-A1 B[3.6f] CoE [10] PTB VP [3-9, 3-14]
Usab.7* [all] The ·*poll worker interface*· `shall` protect the ·*poll workers*· from taking any action accidentally.	–
Usab.8 [un] [tr] All used methods `shall` be efficient, thus, the ·*voting process*· does not take more time as necessary.	PTB CF [3-5]

5.6.2 Operational Requirements

Op.1* [all] The ·*responsible election authority*· `shall` educate ·*poll workers*· in the use of the ·*electronic voting machines*· and `shall` ensure that information provided to them is understandable.	BWGV [§7(3)] CoE [1a, 20]
Op.2* [di] The ·*responsible election authority*· `shall` ensure that ·*election data*· is stored with its authentication codes from ·*electronic voting machines*· (and, where applicable, from the ·*tallying software*·) for the prescribed ·*archiving phase*·.	CoE [75c, 99] PTB WS [1-1, 2-2, 2-5]
Op.3* [fr] [un] The ·*responsible election authority*· `shall` educate ·*voters*· in the use of the ·*electronic voting machines*· and `shall` ensure that the information provided to them is understandable.	BWGV [§8(1c)] CoE [1a, 20, 22, 38, 46, 61, 62] PTB PE [2-6, 4-2], VP [3-6]

Op.4* [all] The *·responsible election authority·* `shall` develop procedures covering all stages of the *·election·* including

- secure storage of *·electronic voting machines·* at all times
- logistics (transport of *·electronic voting machines·*, spare *·electronic voting machines·*, accessories, etc.)
- configuration of *·electronic voting machines·* (including *·ballot·* details and order on *·electronic voting machines·* and *·tallying software·*)
- checking *·electronic voting machines·* (including configuration and empty *·e-ballot box·*)
- response to any kind of exceptions, malfunctions and breakdowns
- recording of *·poll worker·* activities, *·electronic voting machine·* state changes, system resumings, etc.
- ensuring that *·electronic voting machines·* are in the appropriate state at every stage in the *·election phase·*.
- closing the *·poll(s)·*, including disabling *·electronic voting machines·*
- tallying and re-tallying
- comparing number of *·votes·* recorded with number of *·electors·*
- *·archiving phase·* including data deletion at the end

BWGV [§7(2), §8(1,2), §10(1), §11(5), §12, §13, §14(1,3,5), §15 (1,3), §16, §17(3)]
BWGV-A1 B[2.6]
CoE [28, 29, 31, 51, 52b, 69b, 73, 74, 75, 75a, 77, 79]
PTB PE [2-1, 2-2, 2-3, 2-5, 4-3, 4-6, 4-11], VP [1-4, 3-3, 4-5], DR [1-1, 1-3, 1-4], WS [1-2, 2-1, 2-4,2-6], CF [1-11]

Op.5 [tr] The *·responsible election authority·* `shall` develop a contingency plan describing appropriate responses to at least the following circumstances:

- Results produced by recount or alternative *·tallying software·* do not agree with original result
- Number of *·votes·* recorded does not match number of *·electors·*
- Any kind of exceptions, malfunctions, and breakdowns
- Case where *·voter·* leaves a *·electronic voting machine·* in *·active state·*

BWGV [§11(4), §14(5), §15(2)]
CoE [28, 70a, 71a, 75b]
PTB PE [4-11, 4-12], VP [4-7, 5-5]

Op.6** [all] The ·*responsible election authority*· `shall` define all ·*responsible election authority*· variables, prescribe the certification process (including decertification and recertification) and appoint the ·*testing authority*· and the ·*certification authority*·.

BWGV [§1, §2(3,4), §3, §4]
CoE [85, 111]

Op.7* [all] The ·*responsible election authority*· `shall` define (for all ·*election*· phases)

- timetables,
- access control policy (including separation of duties and minimum team size) inclusive audit data and system related access control,
- administration activities,
- ·*user*· roles,
- key management policy,
- incident levels, and
- reporting procedures.

BWGV [§10(2)]
CoE [23, 28, 32, 33, 36, 56 74, 76, 80, 81, 104]
PTB PE [4-3, 4-4], WS [2-3], CF [3-6]

Op.8* [tr] [non-core] Before the ·*election*· the ·*responsible election authority*· `shall` publicly disclose all technical information about the ·*electronic voting machines*· (including design, configuration, version numbers for all software, etc.).

Appl. Note: Exceptions are only acceptable where it can be shown that such a disclosure would either endanger the security of the ·*electronic voting system*· or genuinely endanger the intellectual property of the ·*manufacturer*·.

BWGV [§6(b)]
CoE [20, 21, 24, 28, 69a]

Op.9* [tr] [non-core] The ·*responsible election authority*· `should` arrange alternative ·*tallying software*· to check results.

CoE [28]

Op.10* [un] [non-core] The ·*responsible election authority*· `shall` clearly indicate whether the ·*electronic voting machines*· are being used in a real ·*election*·.

CoE [50]

Op.11* [fr] [non-core] The *·responsible election authority·* `should` ensure that all *·electronic voting machines·* display the *·ballot·* in a uniform way.	PTB VP [3-4]
Op.12* [tr] [non-core] Before the *·election·*, the *·responsible election authority·* `shall` inform *·voters·* about polling stations where the *·electronic voting system·* will be used.	BWGV [§6(a)]
Op.13 [all] The *·poll workers·* `shall` follow the procedures described by the *·responsible election authority·*.	BWGV [§7(1), §10(2b)] CoE [71b, 73, 77]
Op.14* [all] The *·poll workers·* `shall` respond to system messages in accordance with the user-guide.	PTB PE [4-11]

5.7 Summary

This chapter defines the exact target of evaluation, stand-alone direct recording electronic voting machines used in polling stations, and itemises these requirements for this type of electronic voting systems. This list contains 59 system requirements (while these are divided in 12 security requirements, 38 functional requirements, and eight usability requirements), 12 assurance, and 14 operational requirements. According to Sect. 4.4, all requirements are labelled by the election principle(s) from which they are deduced. In addition, the defined requirements refer to corresponding requirements in [37], [143], and [62]. Requirements from these documents that are not referred to the requirements for remote electronic voting systems in Chap. 6 or treated in appendix D[4].

Section 5.1 clarifies the relationship between the requirements in this chapter and those provided in [156]. In order to be able to refer to this paper an additional notation is introduced. Then, Sect. 5.2 describes the exact target of evaluation, in particular that the considered systems do not provide voter registration, voter identification, voter authentication, or archiving functionality; that is, only the functionality for the polling phase and the tallying phase are considered.

The 12 security requirements in Sect. 5.3 are deduced from corresponding threats which are also specified (including the type of attack and the

[4] Here, it is explained why particular requirements are not referred to the requirements presented in this book.

motivation). These requirements are divided into those for the polling phase and those for the tallying phase. The functional requirements, in Sect. 5.4, are composed of 26 requirements for the polling phase, three requirements for the tallying phase, and 10 requirements for the audit system. While the security requirements are deduced from threats the functional requirements are related to policies. However, these policies are not specified due to space reasons. Assurance requirements, in Sect. 5.5, address either the tasks of the manufacturer (and thus the development process), the testing authority (how to evaluate the system), or the responsible election authority. In addition, Sect. 5.6 presents the list of usability and organisational requirements, while the last category addresses only responsible election authority tasks as well as documents and procedures to define.

The requirements specified in this chapter serve as basis for the requirement definition for remote electronic voting systems.