3

Related Work – A Landscape of Requirement Catalogues

While the different electronic voting systems are proposed and discussed in the first part of the foundation, this chapter presents an overview and analysis of existing approaches for the evaluation of electronic voting systems. It is discussion is necessary to know these approaches and their vulnerabilities in order to provide an exhaustive list of requirements and an evaluation approach.

The surveyed approaches include requirement catalogues, ordinance, laws, and research activities. The discussed list of requirements were developed by people from different disciplines, like a group of security experts, data protection officers, security auditing enterprises, lawyers, or security auditing civil services.

The first part of this chapter concentrates on requirement catalogues for electronic voting machines (in particular, the German and American election regulations) while the second part discusses those for remote electronic voting systems (in particular, the Council of Europe recommendations, the catalogue for “Online-Voting Systems for Non-parliamentary Elections”, the catalogue of the Gesellschaft für Informatik, the Swiss and Austrian election law, as well as the Network Voting System Standards). Afterwards, scientific papers are analysed, in particular Shamos’ commandments, Mercuri’s PhD thesis, a technical report from the EU CyberVote project, and McGaley’s PhD thesis. In all three cases, the analysis is structured according to

- context / background in which the requirements have been developed,
- input sources used,
- type of electronic voting system addressed ,
- categories in which the requirements are classified / level of detail for the requirements,
- proposed evaluation and certification techniques (including underlying trust model), and
- people identified to oversee the evaluation and certification.

The vulnerabilities are summarised in the conclusion.

M. Volkamer: Evaluation of Electronic Voting, LNBIP 30, pp. 37–57, 2009.

3.1 Regulations for Electronic Voting Machines

3.1.1 German Federal Ordinance for Voting Machines

Background. In 1975, the first version of the Bundeswahlgeräteverordnung (BWahlGV – Federal Ordinance for Voting Machines) [143] was integrated into the Bundeswahlgesetz (BWahlG – German Federal Law on Elections). These regulations did allow until recently the use of electronic voting machines in Germany for Federal and European elections[1]. While, the original regulations only addressed mechanical devices, the newest version (which dates back to 1999) extends the list of permitted electronic voting machines to include electronic and software based systems.

Sources. Probably the regulation bases on the Dutch regulations [139]. However, this is not made explicit in the document.

Type of Electronic Voting System. The regulations address *stand-alone electronic voting machines* which are not connected to the Internet or any other network and which are used in polling stations (see Sect. 2.3.1). The devices are used to cast, store, and count the votes while the voter authentication and the inspection of the person's right to vote is done manually by the poll workers.

Requirements. The regulations distinguish between organisational, certification, and technical requirements. The organisational ones mainly define how to deliver the electronic voting machines on election day, what the user-guide must look like, and how to check whether the electronic voting machine is the one that has been evaluated and approved. The technical requirements are defined in the first appendix. Here, the necessary evaluation materials from the manufacturer are defined (this includes the source code). The requirements are divided into two categories: 'technical assembly' and 'functionality'. The 'technical assembly' part is divided in the following sub-categories: construction, resilience, permanency/functional security, reaction, absence of energy supply, and transportation. The 'functionality' part is divided in functional principle, function check, ballot display/appliances, vote storage/tallying/display, sealing, and locking of the devices, vote casting, and ergonomics/usability. These technical requirements are very detailed but at the same time very specific and in some points over-specified; that is they can only be applied to the electronic voting machines in mind.

Evaluation/Certification. The Federal Ordinance for Electronic Voting Machines defines the responsibilities for (re)evaluation, certification, and revocation, but not the evaluation methodology itself, such as the evaluation techniques in use, the evaluation depth, or the underlaying trust model. Some information about the required evaluation can be read out of the necessary

[1] The Federal Constitutional Court decided on March 3th 2009 that the Federal Ordinance for Voting Machines is unconstitutional (compare to [21]).

evaluation material: for instance, the fact that the source code is required might have the consequence that it should be evaluated. There is one evaluation report available [117] but it also does not give any information about the applied evaluation techniques.

Person in Charge. The evaluation needs to be performed by the Physikalisch-Technische Bundesanstalt (PTB – Department of Metrological Information Technology in the National Metrology Institute) and the approval certified by the Federal Ministry of the Interior. But the Federal Ministry of the Interior is currently renewing the regulations and one discussed change is the integration of the Bundesamt für Sicherheit in der Informationstechnik (BSI – Federal Office for Security in Information Technology).

3.1.2 Election Law of the Free and Hanseatic City of Hamburg (Germany)

Background. The state government of the Free and Hanseatic City of Hamburg, Germany was planned to introduce a new type of electronic voting machines for its state parliament (in German: "Bürgerschaft") election in February 2008: the Digital Election Pen. The idea came up because of a change in their local electoral law which causes the use of ballot booklets instead of one side ballot sheets and, thus, results in a time and capacity intensive task for tallying. The persons in charge of the state parliament election proposed a new way to evaluate and certify the Digital Election Pen system because the "Federal Ordinance for Electronic Voting Machines" is not applicable to the Digital Election Pen system. Advised by the Bundesamt für Sicherheit in der Informationstechnik (BSI -Federal Office for Information Security), the person in charge decided to go with the Common Criteria (for more information about this methodology see Sect. 7.1). To do so they contract the Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI -German Research Center of Artificial Intelligence) to develop a corresponding Protection Profile [158]. This Protection Profile has been successfully evaluated by the accredited laboratory TÜV Informationstechnik GmbH and certified by the BSI. Nevertheless, the persons in charge decided to contract the Physikalisch-Technische Bundesanstalt (PTB – Department of Metrological Information Technology in the National Metrology Institute) for a second additional evaluation to benefit from their experiences with the evaluations of electronic voting machines. As a foundation the person in charge developed together with the PTB regulations for electronic voting machines [124] corresponding to the Federal Ordinance for Voting Machines. Recently the persons in charge decided not to use the Digital Election Pen system due to negative press and security reservations.

Sources. Hamburg's Regulations for Electronic Voting Machines [124] is based on the Federal Ordinance for Voting Machines in [143] and the election laws and regulations for traditional elections of the city of Hamburg. The Protection Profile [158] was influenced by the parallel work on a Protection Profile for remote electronic voting[2] [161] as well as by the result of a couple of meetings with the persons in charge and the authors of the Protection Profile.

Type of Electronic Voting System. The Digital Election Pen belongs to the paper-based electronic voting systems and here in particular to the optical scan systems. It is described in Sect. 2.3.2.

Requirements. The Hamburg's regulations for Electronic Voting Machines [124] concentrate on the evaluation of functional requirements while the developed Protection Profile [158] concentrates on the security functions deduced from possible threats and policies and it bases on assumptions about the environment. These assumptions are also part of the PTB evaluation. The level of detail in the requirement definition of regulations is compared to the level in the federal ordinance. The requirements defined in the Protection Profile are based on the Common Criteria security functional requirement components.

Evaluation/Certification. The Protection Profile demands an evaluation of the Digital Election Pen system according to the EAL3 (evaluation assurance level) augmented under the trust model defined by the set of assumptions to the environment. The evaluation process is defined in the Common Evaluation Methodology (CEM) [36]. In addition, the Digital Election Pen system is evaluated against the Hamburg's Regulation for Electronic Voting Machines. Similar to the Federal Ordinance for Voting Machines, Hamburg defines the responsibilities for (re)evaluation, certification, and revocation, but not the evaluation process itself, such as the evaluation techniques in use, the evaluation depth, or the underlying trust model.

Person in Charge. The evaluation and certification is done in a cooperation of four institutions in accordance with Hamburg's Election Law for Local Election [52]: Hamburg's Department of the Interior (instead of the Federal Ministry of the Interior) approves the evaluation performed by PTB. Additionally, the BSI certifies an evaluation of the security requirements performed by a Common Criteria accredited laboratory.

3.1.3 American Election Regulations

In the United States, there is a shared responsibility among the three levels of government in overseeing the conduct of elections. Each state sets its own guidelines for the conduct of local, state, and federal elections. States have generally delegated the authority to conduct elections to smaller subdivisions, such as counties, cities or towns. As a result, there are thousands of jurisdictions that administer federal elections throughout the country. However, states must comply with requirements set forth in certain federal legislation in order to receive funding for electoral matters. The most important standards are:

[2] This Protection Profile is called GI/BSI/DFKI Protection Profile and is discussed in Sect. 8.2.

- The Federal Election Commission (FEC) formulated a suggested standard for electronic voting machines in 1990 - the so called Voting System Standard (VSS) [45], but they lacked enforcement authority. The standard was only accepted by two third of the states.
- The Help America Vote Act (HAVA)[3] mandates federal standards for the functionality, accessibility and security of voting systems across the country, as well as for allocating funds to states to help upgrade outdated equipment. HAVA is not exclusively an electronic voting standard; it addresses other types of voting. HAVA established the U.S. Election Assistance Commission (EAC[4]). The EAC's Technical Guidelines Development Committee (TGDC) developed – in cooperation with the National Institute of Standards and Technology – a voluntary guidelines for voting systems, called Voluntary Voting System Guidelines (VVSG) [142]. The VVS guidelines are currently only a draft while the authors ask on their Web page for comments to improve them. They are separated into three parts: part 1 addresses equipment requirements, part 2 documentation requirements, and part 3 testing requirements. Recent discussion by the committee concentrated on the inclusion of mandatory Voter Verifiable Audit Trails and recounts thereof. The main idea for evaluation and certification is that testing equipment for conformance is performed by qualified companies (referred to as an Independent Testing Authority) that are selected by the National Association of State Elections Directors.
- The Institute of Electrical and Electronics Engineers (IEEE) developed an evaluation standard for election voting systems. The purpose of their project (P1583) is to "provide technical specifications for electronic, mechanical, and human factors that can be used by manufacturers of voting machines or by those purchasing such machines. The tests and criteria developed will assure equipment: accessibility, accuracy, confidentiality, reliability, security and usability" [165]. Their detailed report is non-binding but could eventually be incorporated into election system legislation. One group of security experts outside of P1583 was developing a Protection Profile that was expected to be used in the Security Section of P1583. However, this has not been completed, no information is available and it is not clear whether that group is still working on it.

[3] Although HAVA is legally limited to federal elections, in practice it influences virtually all elections in the US. It addresses requirements for electronic voting such as: testing, certification, decertification, and recertification of voting system hardware and software. Also, voting system standards and requirements are addressed (in Sec 301).

[4] The HAVA set up the EAC, a new commission whose responsibility it was to distribute money for updating voting systems and voting administration as well as updating the FEC 2002 Voting System Standards with the assistance of National Institute of Standards and Technology (NIST).

3.2 Requirements for Remote Electronic Voting

3.2.1 Council of Europe Recommendations

Background. In early 2003, the Council of Europe set up a working group to develop a set of standards for e-enabled voting that would reflect member states' differing circumstances. The standards [37] were published in 2004. The correct title is 'legal, operational and technical standards for e-voting - Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum'. Within 112 requirements, the Council of Europe's recommendations are the most comprehensive collection of requirements. The document starts with five recommendations and a list of definitions for election related items. Concrete requirements are then defined in the following three appendices and explained in detail in the "Explanatory memorandum" chapter. This last chapter contains a paragraph "Risk analysis – methodology" where the authors propose the application of the Common Criteria methodology [35] to describe the assets which need to be protected, threats which attack these threats, and corresponding security requirements to protect the threats (here called security objectives according to the Common Criteria). Therefore, they define a long list of assets to be protected, a list of subjects involved and threats which need to be prevented. Based on these threats corresponding security objectives are defined. Even though the work is not completed in the Common Criteria, this parts enables the development of a Common Criteria Protection Profile for these recommendations.

Sources. The group involved in developing these requirements claims to base their results on obligations and commitments from existing international instruments and documents, such as: the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the United Nations Convention on the Elimination of All Forms of Racial Discrimination, the United Nations Convention on the Elimination of All Forms of Discrimination against Women, the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular its Protocol No. 1 (ETS No. 9), the European Charter of Local Self-Government (ETS No. 122), the Convention on Cybercrime (ETS No. 185), the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108), Committee of Ministers Recommendation No. R (99) 5 on the protection of privacy on the Internet, the document of the Copenhagen Meeting of the Conference on the Human Dimension of the Organization for Security and Co-operation in Europe (OSCE), the Charter of Fundamental Rights of the European Union, and the Code of Good Practice in Electoral Matters. The recommendation covers political elections and referendums.

Type of Electronic Voting System. The recommendations address any electronic voting system involving the use of electronic means in at least the casting of the vote and in particular remote electronic voting (defined as "e-voting where the casting of the vote is done by a device not controlled by an election official" [37]).

Requirements. The recommendation of the Council of Europe provides a very comprehensive list of requirements. The document distinguished between legal standards (covering the four election principles of universal, equal, free, and secret suffrages), procedural safeguards (classified in transparency, verifiability/accountability, and reliability/security), operational standards (including the categories: notification, voters, candidates, voting, results, and audits), and technical requirements (containing accessibility, interoperability, systems operation, security, audit, and certification; while security requirements are further classified with respect to election phases and audit requirements with respect to appearing actions like recording and monitoring). In addition, the Election Markup Language (EML) [44] (a standardised XML language for the interchange of data among election services) is recommended.

In 2006, McGaley and Gibson [100] produced a critical analysis of those standards, including a redrafting of the standards themselves in an attempt to overcome some of the drawbacks they had identified in the original. Their analysis "has shown, the CoE standards document is flawed. The inconsistency, incompleteness, over- and under-specification, redundancy and repetition that have been demonstrated could lead to 'bad' systems being certified against these requirements, and/or 'good' systems failing."

In 2007, Rössler used the recommendation of the Council of Europe (in particular the list of security requirements/objectives of the last chapter) as basis to evaluate his proposed remote electronic voting system called EVITA in his PhD thesis "Electronic Voting over the Internet – an E-Government Speciality" [126]. However, he argued that this list needs to be extended. To do so, Rössler applied selected elements of the GI/BSI/DFKI Protection Profile for remote electronic voting[5] [161].

Evaluation/Certification. Requirements 111 in the recommendations states the need for certification process definitions but without giving any details about how such certification could be done. The only information given is in requirement 24 and 25: requirement 24 states that the "components of the e-voting system shall be disclosed" for evaluation purposes. Requirement 25 states that the evaluator has to show that the system "is working correctly and that all the necessary security measures have been taken". However, in order to decide about necessary measures the underlying trust model needs to be defined because this is not yet addressed in the recommendation.

Person in Charge. The recommendation itself does not define the persons in charge of the evaluation or certification. It only states in requirement 25 that the evaluation should be done by an independent body, appointed by the responsible election authority.

[5] This Protection Profile is discussed in Sect. 8.2.

3.2.2 Online-Voting System Requirements for Non-parliamentary Elections

Background. A catalogue of requirements for "Online-Voting Systems for Non-parliamentary Elections" [62] has been developed by the Physikalisch-Technische Bundesanstalt (PTB - Department of Metrological Information Technology in the National Metrology Institute) within the project "Development of concepts for testing and certification of online voting systems" funded by the former German Ministry of Economics and Labour. It has been discussed in two working groups: "Testing and certification" and "Legal framework conditions" ([62] provides a list of groups and people involved in these working groups). The catalogue constitutes a recommendation for developers of electronic voting systems and gives an orientation for the refinement of test concepts. This catalogue is only a recommendation without mandatory regulation character.

Sources. The following already available sources have been considered: the Federal Ordinance for Voting Machines [143], the reports of the CyberVote project [47], the Voting System Standards [45], the Network Voting System Standards [104], and the Swiss Regulations [166] (here especially part 6a: "Pilotversuche mit elektronischer Stimmabgabe" addressing electronic voting).

Type of Electronic Voting System. The electronic voting systems the PTB considered are networked electronic voting machines in polling stations. Remote electronic voting is explicitly not included in the definition. In addition, the authors focused on non-parliamentary elections such as for staff and council work elections as well as shareholder elections.

Requirements. It contains technical and organisational requirements. The requirements are of a sufficiently general level to be described independently of particular systems. The level of detail used in the definition of the requirements is different. The requirements are classified according to the different time intervals or classified as "cross-sectional functions": preparation of election (including preparation of register of voters, provision of means for voter identification and authentication, preparation of ballot, installation of voting system up to and including readiness for service), polling phase (including voter identification and authentication, management of the register of voters, ballot handling, vote transmission, and vote storage), determination of election result (including termination of vote casting and vote tallying), wrap-up, and safe-keeping (including dismantling and disassembly of voting system, (long-term) archiving, safe-keeping, and maintenance of voting system), and cross-sectional functions (including general reliability of software and hardware, communication system underlying the voting system, anonymisation of votes, and technical observation of voting system (technical audit)).

Evaluation/Certification. The catalogue does not describe "any method to be used for meeting the requirements. It is not even prescribed whether particular requirements are to be met by technical measures or by non-technical operational measures". However, requirement CF3-4 requires that the "implementation shall be proved to be correct with respect to the theoretical concept by software test methods (including code inspections) which represent the state of the art." This is a first hint but no concrete evaluation instruction.

With respect to the trust model , requirement CF2-6 states that the system should comply "with the state of the art in relation to the threat potential accepted". Similar in requirement CF3-2, it is demanded that "the concept used including the mathematical methods shall be appropriate for the particular election." These requirements go in the right direction. However, it is not clear how to define the threat potential and how it influence the evaluation and the required security functions of the electronic voting system.

Person in Charge. Missing evaluation procedures lead to the fact that no persons in charge are identified to run the evaluation or even certify any systems.

3.2.3 Catalogue of the Gesellschaft für Informatik

Background. The Gesellschaft für Informatik (GI - the German society of computer scientists) presently has about 24.000 members mainly from Germany. There are also associated memberships in Austria and Switzerland. It was set up in Bonn in 1969. The rules for elections of the bodies of the GI are formally specified by the GI's regulations for elections and polls [50]. Since July 2003, article 3.5.4 of the constitution of the GI allows the application of remote electronic voting. Here, the precondition is that the remote electronic voting system provides the same security level as postal voting. In all cases where postal voting is admitted the election committee can decide to also give members the possibility to use a remote electronic voting system - as long as it is comparably secure. In the summer of 2004, the chairmanship (in German: "Präsidium") decided unanimously to offer both postal voting and remote electronic voting for the chairmanship elections in December 2004. The GI established a group of security experts to accompany the pilot election and the future process of remote electronic voting in the GI. The group consists of German experts in IT security and electronic voting from universities, the Physikalisch-Technische Bundesanstalt (PTB - Department of Metrological Information Technology in the National Metrology Institute), and the executive board of the GI. The main task of the expert group was to develop and enforce ad-hoc security requirements. In December 2004, the Internet voting expert group of the GI decided to develop a requirements catalogue for "Internet-based elections in societies" [113]. The catalogue should be short and crisp and should not exceed six printed pages. After several iterations, the last version was published in 2005.

Sources. Four requirements catalogues were already available and were used as a basis for further development: the Council of Europe recommendation [37], the IEEE Voting Equipment Standards [165], and the PTB requirements "for Online-Voting Systems for Non-parliamentary Elections" [62].

Type of Electronic Voting System. The GI requirements address remote electronic voting using secrets (voting TAN) for authentication.

Requirements. The catalogue starts off with some preliminary notes and explicates assumptions under which any applied Internet voting system must ensure the security requirements. For example, it is assumed that a non-secret name or a membership number (user-id) is applied for the voter identification and a secret alphanumeric password (one-time election PIN) is used for voter authentication. Moreover, it demands in these preliminary notes that the electronic ballot box and the electronic election register are installed on different servers and that the two servers are located in different organisations. This part is very specific compared to other requirement catalogues. The preliminary notes also define issues which are out-of-scope of the security requirements catalogue. For example, the candidate nomination and the maintenance of the list of eligible voters are not considered in the catalogue. Rules for long-time storage of the election results are not addressed, either. The catalogue of 2005 separates the requirements on the system development and on the election execution from the requirements on the remote electronic voting system itself. The requirements on the remote electronic voting system itself are divided into requirements on the election servers and on the election software. The general requirements for system development contain requirements on the type and level of details of the system description, the security analysis and the manuals. There are especially strong requirements on the anonymity concepts. This category includes requirements on the development process, the system tests, and the key management. The requirements on the election execution contain the distribution of the election PIN, the election register management, and the installation as well as the de-installation of the voting system. The catalogue requires the election servers to run a secure operating system, and to isolate the election software from all other applications. Only authorised persons may have access to the servers. For the requirements on the election software the following categories were used: general requirements to a remote electronic voting system and its security, specific functional requirements to the remote electronic voting system, requirements with respect to the anonymity of votes, specific requirements to ensure a universal and equal election, and ergonomic and usability requirements. The general functional requirements include the system's reliability and logging as well as the guarantee of consistent system states in the case of any interruption. Specific functional requirements refer to the electronic register and to the electronic ballot box. Requirements with respect to anonymity specify a secret, equal, and universal election. The last category of requirements on the election software addresses ergonomic and usability issues.

Evaluation/Certification/Person in Charge. The document does not talk about evaluation and certification procedures nor does it talk about the underlying trust model or the person in charge.

3.2.4 Swiss Election Law

Background. The Swiss political system can be described as a direct democracy, meaning each voter has at least four times per year the possibility to cast a vote for referenda on the national, cantonal, and communal level. Moreover, in all cantons[6] postal voting is allowed without any conditions and it is copiously used. Introducing remote electronic voting is seen as a possibility to simplify the processes and decrease the costs. The project "vote electronique" is a consequence of the Swiss strategy to use the new information and communication technologies for the decision making process. Thus, Switzerland started running three pilot projects: in Genève, Neuchâtel, and Zurich. Their notion of remote electronic voting includes casting a vote in elections, referenda, electronic signature of initiatives, requests for referenda and candidate proposals. In order to enable legal binding trials on a federal level, the federal law regulating political rights [53] was changed together with the corresponding regulations [166].

Sources. From the law it is not deducible whether or which previous available resources defining electronic voting requirements were used for the forming of this law.

Type of Electronic Voting System. The Swiss projects address remote electronic voting where the user can use any kind of device connected to the Internet.

Requirements. Art. 27a-27q of the ordinance of May 24 in 1998 on political rights [166] contains the requirements which must be ensured before the Federal Council can approve pilot trials of remote electronic voting. The Swiss requirements can be summarised as follows: "e-voting has to be as secure and reliable as the traditional voting methods (that is, postal voting and voting at polling stations" [15].

The main regulations are addressed in article 6 a of [166] (Art. 27 a -q). Art 27 (a) – (d) and (q) regulate how pilot projects have to be permitted and be set up in general. The other parts are not clearly structured for people having a technical background. However, the headings of the following parts are: (e) Protection of the formation of options (for example, by enabling the voter to change his choice before he finally casts it), (f) encryption (for example, encryption of the vote before it leaves the voter's device), (g) secrecy of the vote (for example, by demanding that it is not possible to link vote in the electronic ballot box), (h) further mechanisms to ensure the secrecy of the

[6] There is one exception – the canton Tessin, which does not implement postal voting unconditionally, but only for elections and referenda on the cantonal level.

vote (for example, that the voter needs to be informed on how to delete all vote related data from his PC), (i) control of the right to vote, (j) one-voter-one-vote principle, (k) securing cast votes (l) technical state of the art, (m) computation of the election result, (n) solve technical problems, and (o) check the efficiency (meaning analysing the turnout and voter behaviour). There is one big difference between the Swiss regulations and others: the Swiss regulations do not demand that any attack must be prevented but only systematic ones, which seems to be more realistic. As the requirements are formulated in the regulations, they are rather abstract and less technical. Thus, for the developer it is hard to decide which security functionality is sufficient to meet these requirements.

Evaluation/Certification/Person in Charge. Art. 27(l) of the Swiss Election Law demands that the enforcement of the security requirements and the functionality of the electronic voting system needs to be approved by an independent external authority, which is accredit by the Swiss federal chambers (in German: "Bundeskanzlei"). The same holds for changes within the electronic voting system. There is no statement about the evaluation methodology to evaluate a system against the defined requirements. This is left up to the evaluators.

3.2.5 Austrian Election Regulations

Background. In Austria, electronic voting is allowed for student union elections (see [19]) and for the Austrian Federal Economic Chamber (in German: "Wirtschaftskammer") elections (see [18]), since 2001. Both regulations are very similar, in particular, they both require the Austrian citizen card (in German: "Bürgerkarte") for voter identification and authentication.

Sources. From the law it is not deducible whether or even which previous available resources defining electronic voting requirements were used for the forming of this law.

Type of Electronic Voting System. It is not clearly defined what kind of electronic voting system is addressed. Nevertheless from the regulations it can be deduced that Austria wants to either apply remote electronic voting or a kiosk system while in both situations the identification has to be done by the citizen card.

Requirements. The regulations are very short but are embedded in a broad environment of information technology applications. §34 (4) [19]/§74(2) [18] demands that the electronic voting system needs to be compliant with the security objectives for digital signatures according the signature law [20] and the data protection law [17]. Moreover, it also contains the general demand that electronic voting must be as secure as the traditional system (§48 (2) [19]). In §34(5) [19]/§74 (3) [18] some more technical requirements are defined: 1./(a.) ensuring the secrecy of the vote, including that no one can link the voter to his vote at any point in time; 2./(b.) checking the voter's right to vote before he will see the ballot; ensuring the one-voter-one-vote principle; 3./(c.) integrity of cast ballots by the application of digital signatures; secrecy of the vote during transmission by encryption; 4./(corresponding regulation in §74(2) [18]) all possible actions of the responsible election authority are also possible with the electronic voting system; 5./(d.) preventing accidentally cast votes; 6./(e.) providing a polling booth (in case of electronic voting machines). Moreover, according to §48 (2) [19] electronic voting is only allowed to be applied in parallel to a paper-based system. In §78 (6) [18] there is an additional organisation requirement defining that the electronic voting process needs to be stopped if it does not work correctly anymore. For a more detailed discussion see [126] (section 2.3 and 5.2).

Evaluation/Certification. In § 34 (6) [19]/§74 (4) [18] the evaluation procedure is addressed: the state of the art of the used system should be sufficiently and permanently scrutinised. But, it is not stated how this should be done.

Person in Charge. – Furthermore, §27 (6) [19]/§74 (4) [18] demands that the compliance with the security requirements needs to be certified by a certification authority according to §19 of the signature law.

3.2.6 Network Voting System Standards

Background. The Network Voting System Standards (NVSS) are proposed in [104] and have been developed by employees from the VoteHere company (they also retain the copyright in [104]) which developed its own electronic voting system. In parallel to writing these standards the Federal Election Commission of the US (FEC) revised the Voting System Standards [45]. One of their tasks was to include standards for public network direct recording electronic voting systems but explicitly no other online or network voting systems outside the polling station. VoteHere sees their Network Voting System Standards as both, an alternative and as input to the FEC work and to ensure that upcoming trials of remote electronic voting and kiosk electronic voting machines "are conducted using systems that have been evaluated and demonstrated to meet a set of standards sufficient to protect the integrity of the election" [104].

Sources. The Network Voting System Standards are based on two technical reports from VoteHere ([163] and [164]). Moreover, the standards are based in part on the Voting System Standards [45] and on the findings and recommendations of the SERVE report [73], the CalTech/MIT Voting Technology Project, a workshop on remote electronic voting and on private research efforts at VoteHere.

Type of Electronic Voting System. The NVVS are intended to be applicable to any electronic voting system which transmits votes over a network and which is not under the physical and logical control of the election officials at all times. This includes remote electronic voting and kiosk electronic voting machines.

Requirements. VoteHere distinguishes in their standards between high-level and functional requirements as well as specific standards. From the high-level requirements the functional ones are deduced. The functional requirements shall be met by all systems regardless specific architectural division between hardware, firmware, and software underlying technology or implementation methodology. They are organised around the four high-level requirements: fairness, accuracy, privacy, and proof[7]. The definition of the demanded standards is distinguished in hardware, software, telecommunication, cryptographic, quality assurance, and configuration management standards. While the functional requirements are discussed in detail these standards cover only one page.

All requirements are qualified by the words "shall" or "must" and in addition they are identified through the use of an ID, a unique alphanumeric number. They also provide background information on some of the requirements for better understanding. Requirements relating to the electoral register are outside the scope of these standards.

Evaluation/Certification. – The Network Voting System Standards propose to start with a design review. In case the design is logically able to meet the requirements, the election result of the first design evaluation provides the necessary details for specific functional review and testing. The evaluation begins in accordance with the NVSS with an examination and review of the technical data package. This includes a check of whether all necessary documentations for the further steps are available and the review of the quality assurance and configuration standards. In the next step the design is reviewed and afterwards there are two steps to be done in parallel: code review and hardware tests. The last step contains system functional testing. Certification processes are not addressed.

Person in Charge. – The standards do not talk about persons in charge for evaluation or certification.

3.3 Scientific Papers

Almost all scientific papers proposing a voting protocol are structured in the following way: the authors start with a set of requirements, then they describe their proposed voting protocol and then show in the analysis part that their system ensures the previously defined requirements. First of all, these requirements are only related to the voting protocol and secondly, it is not that surprising that the protocol ensures its own defined requirements. Thus, such papers are not taken into account for this discussion. This section concentrates on work independent of concrete voting protocols or electronic voting systems. A selection of the most important contributions is discussed in this section:

[7] "Proof – The system must, without violating the privacy requirements, be able to prove that the fairness and accuracy requirements have been met" [104].

Shamos' commandments [137], the PhD thesis from Rebecca Mercuri [101], the list of requirements provided in the CyberVote project [47], and the PhD thesis from Margaret McGaley [99].

(A) **Shamos Commandments**

Background. The work around [137] is based on the author's participation in official evaluations of about fifty different electronic voting systems since 1980 as well as an audit of the election laws of about half of the United States.

Sources. From the paper it is not deducible whether or even which previously available resources defining electronic voting requirements were used for the forming of the commandments.

Type of Electronic Voting System. Shamos does not further limit the implementation of electronic voting. He addresses any electronic voting system that captures and tallies votes.

Requirements. In [137], system requirements for electronic voting are boiled down to the following six high level commandments:

1. "Thou shalt keep each voter's choices an inviolable secret."
2. "Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorised to cast a vote [...]".
3. "Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes."
4. "Thou shalt report all votes accurately."
5. "Thy voting system shall remain operable throughout each election."
6. "Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I."

While 1)-3) are strong ones, 4)-6) are more flexible ones from the author's point of view and the first one is the most important one. Auditing is not part of the commandments because the author argues that "no existing voting system is auditable" [137].

Evaluation/Certification. Evaluation is addressed in [137] by suggesting testing to show that tampering is not possible, but that it is discouraged and difficult. The statement in this paper is that electronic voting systems that meet these six commandments should be certified for use in public elections. However, a particular methodology for the testing is not proposed neither is the impact of different trust models taken into account. In addition, he does not talk about a formal certification process.

Person in Charge. The author does not talk about person in charge to run the evaluation and certification procedures.

(B) Electronic Vote Tabulation – Checks and Balances (Mercuri's PhD Thesis)

Background. Mercuri proposes, in her PhD Thesis "Electronic Vote Tabulation – Checks and Balances" [101] besides other important issues, the application of the Common Criteria methodology to evaluate existing and proposed electronic voting systems. From her point of view, "the establishment of generalised PPs for voting system requirements, therefore, is viewed as an essential base for the development of consistent policies under which evaluation of proposed voting systems can be performed"[8] [101]. With this statement she is first to recommend the application of the Common Criteria for electronic voting and in particular for electronic voting machines. However, she only provides basic discussions about the applicability of the Common Criteria but did not start developing a Protection Profile.

Type of Electronic Voting System. She discusses in her thesis various types of electronic voting machines in polling stations, while concentrating on lever machines and direct recording electronic voting systems.

Requirements. The prosed requirements contain the following categories: system requirements, functionality, correctness (accuracy), accountability, disclosability, reliability, integrity, availability, fault tolerance, data requirements, confidentiality, retention, and recountability, user requirements, administrator requirements, interface usability, documentation, testing, paths, facility management, recovery, system distribution, and compliance with laws and regulations.

Evaluation/Certification. By proposing the Common Criteria methodology, the evaluation and certification procedure is appointed to the Common Evaluation Methodology (see Sect. 7.1 for more information on the Common Criteria). In this context she discusses the evaluation depth. Mercuri proposes the Common Criteria evaluation assurance level EAL4 as the lowest level that should be applied to certify electronic voting systems, "since all lower levels omit salient requirements involving the development process. EAL4 does not include any covert channels analysis, which first appear in EAL5, so perhaps the higher level should be used as the minimal assurance evaluation standard [...] Since the attack potential of the voting system is likely to be high, the more stringent EAL6 evidence of resistance should also be included" [101]. However, as her thesis only serves as first step, she did not discuss possible trust models as part or the Common Criteria evaluation.

Person in Charge. She does not explicitly name persons in charge, but one may suppose that she – according to the CC – suggests the evaluation to be done by an accredited testing authority and the certification to be done by corresponding CC authorities.

[8] PP means Protection Profile in the Common Criteria. For more information see Sect. 7.1.

(C) Voting System Requirements in the CyberVote Project

Background. The list of requirements in [47] has been developed in the EU CyberVote project which is a research and development (RDT) programme funded by the European Commission under the fifth framework programme (FP 5). The objective of the project was to develop a highly secure voting prototype which can be used for remote electronic voting (using a PC or mobile phone). The project is carried out by a consortium led by MATRA Systemes & Information and a grouping together of British Telecommunications, NOKIA Research Centre, K.U.Leuven Research & Development, Technische Universiteit Eindhoven, Freie Hansestadt Bremen, Mairie d'Issy-les-Moulineaux, and Kista Stadsdelsnämnd.

Sources. The list of requirements results from discussions among the CyberVote consortium and from various interviews with responsible election authorities and electronic voting experts from Germany, France, and Sweden.

Type of Electronic Voting System. – The project addressed remote electronic voting while different kinds of authentication techniques have been used in different trials and the developed voting protocols [133] use homomorphic encryption in order to ensure the secrecy of the vote.

Requirements. In [47], the authors distinguish between user requirements and functional specification. The first class contains those system requirements from a user's perspective (VOT) (users are the voters, responsible election authority, and the service providers), meaning those functions required to support the user tasks and the user-interfaces. The second set is classified in two categories: legal requirements (LEG) and technical requirements (TEC). It is distinguished in general requirements and those addressing specific national issues or sometimes reflect different ways of approaching remote electronic voting. They are all uniquely identified.

The authors make an interesting point with respect to the list of user requirements: their development is an ongoing process because in the beginning users may not appreciate the benefits that an innovative system can offer them; but once they understand the benefit of a new technical solution, their requirements may change.

Evaluation/Certification. The document recommends the evaluation of the system by different parties: national experts and software experts. Moreover, they propose interviews and usability tests with potential voters and mathematical proof for the correctness of the system. However, a detailed evaluation instruction as well as the incorporation of the trust model is missing.

Person in Charge. The authors do not talk about person in charge to run the evaluation and certification procedures.

(D) E-voting: An Immature Technology in a Critical Context (McGaley's PhD Thesis)

Background. McGaley explores in her PhD Thesis "E-voting: an Immature Technology in a Critical Context" [99], besides other important issues, two approaches to develop requirements for e-voting (top-down starting with the Recommendations of the Council of Europe [37] and bottom-up like in this book) and discusses the evaluation of systems. For the Recommendations of the Council of Europe, she reveals flaws and problems and then improves the requirement document. The following considerations are only done for the bottom-up approach.

Sources. It is based on the requirements listed in the German Regulations for Electronic Voting Machines [143], the requirements defined in the recommendations of the Council of Europe [37], and the "Online-Voting Systems for Non-parliamentary Election" catalogue developed by the Physikalisch-Technische Bundesanstalt (PTB – Department of Metrological Information Technology in the National Metrology Institute) [62].

Type of Electronic Voting System. "As these requirements were developed for critical elections, remote e-voting systems are not considered [...]. Similarly, it is assumed that the election devices are not networked (data can only be transferred between election devices by physically moving some storage medium). We exclude voter-registration and voter-authentication from our current analysis [...]; we assume that they are implemented as per paper-only elections. [...] The requirements in their current form are not flexible enough to cover non- DRE e-voting systems. [...] Therefore, this catalogue excludes, for example, mark-sense (also known as optical-scan) and digital election pen systems" [99].

Requirements. The catalogue is divided into security, functional, usability, organisational, assurance, audit system, and VVAT requirements (where VVAT means Voter Verified Audit Trail).

Evaluation/Certification. In [99] the following evaluation methodologies are proposed: usability testing, including "sociology-style experimentation with suitably representative test subjects", election observation to evaluate whether organisational, assurance and VVAT requirements are met, manufacturer compliance tests, code review, functionality testing, end-to-end testing, and environmental testing by an independent testing authority as well as red team testing (meaning penetration tests). It is not discussed how the testing should happen, how deep the evaluation should be and on which trust mode the evaluation should base.

Person in Charge. Person in charge of the evaluation is mainly named by independent testing authorities. The responsible election authority is in charge of the system certification.

3.4 Result of the Analysis

Within the proposal of existing requirement catalogues, their vulnerabilities are pointed out for each catalogue. These identified vulnerabilities can be categories in three classes, namely those related to the requirement definition, those addressing the underlying trust model and those concerning the evaluation and certification process. According to this classification, the vulnerabilities can be summarised as follows:

- The specified lists of *requirements* – the electronic voting system needs to ensure – differ in the level of detail and with respect to their focus. The different levels of detail occurs also inside one document. In particular the laws define rather high level requirements, while other documents formulate a set of more detailed and more technical requirements. Some of the requirements are over specified, others under specified or too abstract. Sometimes, documents contain contradicting requirements. There are also cases where the defined requirements are tied that much to a particular electronic voting system that it is impossible to apply such requirements to any other electronic voting system. Moreover, for a better understanding a clear definition of important terms is missing.
- With respect to the definition of a *trust model*, a (detailed) description of the limiting factors is missing or at least not made explicit in the analysed documents.
- The applied *evaluation methodology* is not considered in most of the documents. Thus, evaulators could concentrated on the evaluation of the voting protocol or the development process, the electronic voting system as a whole, the user-interfaces, or the robustness against unexpected events. What kind of test are required is also not defined (for instance, penetration, functional, black box tests).

  Furthermore, a concrete statement about the evaluation depth is missing: is a source code analysis of the whole system or of important parts of the system required or is the evaluation of the high level design of the electronic voting system enough.

Consequently, it is not obvious how to decide for most of these catalogues why a system should pass or fail an evaluation. Moreover, some group of experts could decided that a particular system is secure enough while other would not recommend to use this system. Note, the only exceptions are those dealing with the Common Criteria as evaluation methodology. However, this approach has been proposed and discussed several times but has never been completely implemented[9].

The above critic does also hold for projects where no such catalogues were available or used; and the responsible election authoritys, caused by their

[9] The only exception is the Protection Profile for the Digital Pen. However, this is based on the same approach as proposed in this book and is written by the same author (as one of two authors).

non-technical background, were supported in their decision making process concerning whether a particular electronic voting system is “secure (enough)” (for instance in the Estonia and Dutch remote electronic voting project and in the Irish electronic voting machine project). Here, experts were asked to evaluate particular electronic voting systems (but without specifying the evaluation methodology). Thus, depending on the experts’ background and knowledge as well as the project set-ups, including time and money constraints, the evaluation process differs in all three relevant aspects: underlying requirements, the trust model, and the applied evaluation methodology.

Additional Outcome. The analysis of existing literature also shows that the list of requirements depends on the type of electronic voting system in mind. From a high level point of view the requirements are the same, while as soon as more technical requirements needs to defined, it is necessary to know whether the electronic voting system in mind is a remote electronic voting system or the Digital Election Pen.

3.5 Summary

This chapter elaborates on existing requirement documents for electronic voting to learn from their vulnerabilities and to provide an exhaustive list of requirements in this book.

In the category of documents for electronic voting machines the German Federal Ordinance for Voting Machines, the Hamburg Regulations for Voting Machines, the Protection Profile for the Digital Election Pen, and the American approaches are presented and analysed according to the proposed structure (in Sect. 3.1). The requirement documents for remote electronic voting systems discussed in Sect. 3.2 are: the Council of Europe recommendations, the PTB catalogue, the GI list of requirements, the Swiss and Austrian regulations, as well as the Network Voting System Standards. The discussed scientific work from Sect. 3.3 contains Shamos’ commandments, the Mercuri’s PhD thesis, the CyberVote requirements, and McGaley’s PhD thesis. Many of these documents refer to each other or even form the bases for each other. Figure 3.1. illustrates this relationship.

Section 3.4 discusses the vulnerabilities of the analysed documents which mainly address the different levels of detail for the requirement definition, the missing introduction of a trust model, and the absence of concrete guidance for the evaluation, including a statement about the evaluation depth. Additionally, the analysis shows that the list of requirements depends on the type of electronic voting system in mind.

The requirement documents presented in this chapter are used as input for this book to develop an exhaustive list of requirements for electronic voting which overcomes the identified vulnerabilities. In order to demonstrate the exhaustiveness character, the new list of requirements proposed in Chap. 5

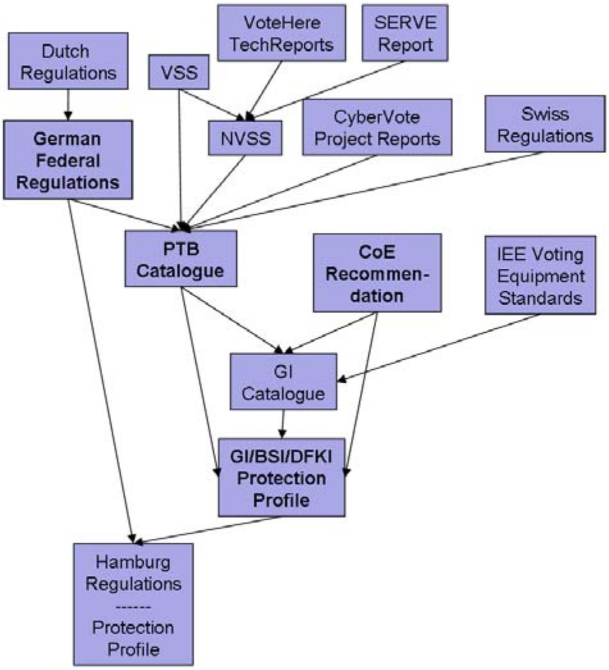

Fig. 3.1. Relation between different requirement catalogues

and 6 refers to the corresponding requirements in existing documents. Due to time and place constraints, the provided requirements only refer to a subset of these documents. These are the following ones:

- The Council of Europe Recommendations [37] because it contains the most comprehensive and exhaustive list of requirements
- The Federal Ordinance for Voting Machines [143] because it has already been applied for system evaluations
- The PTB catalogue for “Online-Voting Systems for Non-parliamentary Elections” [62] because it results from a research project with a huge advisory board