An Evaluation and Certification Approach to Enable Voting Service Providers

Axel Schmidt[1], Melanie Volkamer[2], Johannes Buchmann[1]

[1]Cryptography and Computer Algebra
Technische Universität Darmstadt
Hochschulstr. 10
D-64289 Darmstadt
Germany
{axel, buchmann}@cdc.informatik.tu-darmstadt.de

[2]Center for Advanced Security Research Darmstadt (CASED)
Mornewegstr. 32
D-64293 Darmstadt
melanie.volkamer@cased.de

Abstract: In this paper we provide an evaluation and certification approach for Voting Service Providers (VSPs) which combines the evaluation of the electronic voting system and the operational environment for the first time. The VSP is a qualified institution which combines a secure voting system and a secure operational environment to provide secure remote electronic elections as a service [La08]. This centralized approach facilitates legal regulation and evaluation. So far, a legal regulation framework for VSPs has been developed which demands evaluation and certification of the VSP [Sc09a]. Therefore the VSP is required to provide a security concept in which it demonstrates satisfaction of the security requirements defined in the legal regulation. However neither the content of this security concept nor an adequate evaluation methodology has been specified so far. We therefore developed a security concept template and a comprehensive evaluation methodology for the VSP, which includes both the voting system and operational environment of VSPs. Our proposal incorporates existing evaluation methodologies to facilitate evaluation and certification. With this paper and the legal regulation a realistic approach to enable the VSP concept is accomplished.

1 Introduction

Security is one of the most important goals in the field of electronic voting. A lot of research has been done to develop sophisticated e-voting protocols with complex cryptographic mechanisms to improve security. An additional approach to strengthen security and trustworthiness is the evaluation and certification of e-voting systems.
Here the security functionality of a system is analyzed for compliance with a predefined and approved set of requirements. In 2008 the first evaluation standards for online voting systems were published–the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" [*sic*] [VV08].

However, in [Sc09b] the authors showed that the security of the operational environment, in which the voting system is implemented, has to be considered as well. One attempt to combine the security of a voting system with a secure operational environment is the Voting Service Provider (VSP) concept [La08]. The VSP is a qualified and professional institution which provides secure remote electronic elections as a service on behalf of the election host. Therefore the VSP provides the secure hardware and software, the voting system, the secure infrastructure as well as the specialist knowledge and the skilled personnel needed to operate electronic elections securely. The VSP is a centralized approach and thereby can be regulated and evaluated easily. Legal regulation is an important means to provide a basis for security, trustworthiness and correct behavior. A corresponding evaluation and certification procedure can verify the compliance with such legal regulation. In [Sc09a] the authors therefore introduced a legal framework for the regulation of VSPs. The framework defines requirements for VSPs and demands their evaluation and certification. The legal regulation stipulates that the evaluation and certification of VSPs is based on a 'security concept.' In this security concept, the VSP needs to demonstrate how the requirements of the legal framework are satisfied. The evaluation authority appointed in the statute uses the security concept as the basis for evaluation and certification of the VSP. The security concept comprises technical and organizational aspects, which have to be addressed by the voting system and/or the operational environment. Concluding, the centralized VSP concept and the legal framework provide an ideal basis for a combined evaluation of the voting system and operational environment.

However neither the content of the security concept for VSPs nor an adequate evaluation methodology has been specified so far. Therefore we developed a comprehensive template for such a security concept for VSPs. Further we propose a combined evaluation approach incorporating existing evaluation methodologies for both the voting system and operational environment. We expand the Common Criteria evaluation for online voting systems [VV08] by including an evaluation approach for the operational environment based on the approved *IT-Grundschutz/ISO27001*[1] methodology [G08d]. In this way we facilitate a fully comprehensive evaluation of VSPs and thereby enable the VSP to be put into practice. Our approach is practical since already existing certificates can be included in the evaluation thereby reducing costs and efforts of the VSP evaluation.

We consider related work in Section 2. In Section 3 we develop a security concept template as the basis for evaluation of VSPs. The template specifies which requirements need to be considered. In Section 4 we introduce the Common Criteria and *IT-Grundschutz/ISO27001* certification methodologies and show how they can be used in a security concept based VSP evaluation. In Section 5 we discuss the applicability of these certification methodologies to the VSP scenario and conclude the paper.

[1] eng.: IT Basic Protection/ISO27001

2 Related Work

In the area of e-voting, evaluation is mainly considered in the Common Criteria Protection Profile for online voting products [VV08], which we incorporated in our work. Its development has been discussed in [VKG07]. Several companies are striving to have their e-voting software certified accordingly, e.g. the Polyas voting software by Micromata [RJ07].

Regarding the operational environment, there exist several methodologies. For example, ITIL is a collection of best practices concentrating on IT service management and the optimization of service quality[2]. However, ITIL is less security-oriented. A Swiss project in Geneva is working on the implementation and evaluation of an e-voting system[3]. The coordinators specified security requirements for their voting system[4] and used the ISO27001 methodology for evaluation which is a standard for Information Security Management Systems (ISMS) [Re07, Tr09, Is08]. Our evaluation approach is more comprehensive since it builds on a specialized legal regulation and incorporates the Common Criteria Protection Profile [VV08], being the current evaluation standard for online voting systems, which we expand by using the *IT-Grundschutz/*ISO27001" methodology for evaluation of the operational environment. Thereby we extend the basic ideas of the Swiss approach. Weldemariam et al. provided a more theoretical approach to assess the operational environment of e-voting systems [WVM07]. In contrast, our work focuses on the practicability of the evaluation in real-world scenarios.

In Germany, the evaluation of Certification Authorities (CAs) is based on an approach similar to the VSP evaluation. The "German Signature Ordinance" legally regulates CAs and requires them to provide a security concept (see [G01] § 2). However profound information on the content of the security concept is missing thereby complicating the CA evaluation. To improve the situation for VSPs, we therefore developed a detailed security concept template facilitating VSP evaluation.

3 A Security Concept Template for Voting Service Providers

The legal framework introduced in [Sc09a] specifies only the basic structure of the security concept for VSPs. We therefore developed a detailed security concept template which contains all requirements a VSP must satisfy in order to comply with the legal regulation. We point out that the legal framework for VSPs was developed in Germany and therefore might need adjustment in order to be applied in other countries. This is considered future work.

[2] http://www.ogc.gov.uk/guidance_itil.asp

[3] http://www.ge.ch/evoting/english/welcome.asp

[4] http://unpan1.un.org/intradoc/groups/public/documents/Other/UNPAN022422.pdf

3.1 Methodology

To identify the requirements, which have to be considered by the VSP in the security concept to comply with the legal regulations [Sc09a], we deeply analyzed the legal framework including the act and ordinance. In order to facilitate the interpretation of the requirements by VSPs, we adapted these requirements to the technical field of application. To this end, we analyzed the corresponding preambles of the legal frameworks. They contain additional information which is relevant for implementation and thereby facilitate concretizing the legal requirements. Moreover we incorporated existing technical standards and requirements catalogs in order to further concretize and supplement the requirements from the legal framework. Therefore we utilized recent standards including the "Legal, Operational and Technical Standards for E-voting" from the Council of Europe [Co04], which define comprehensive requirements for electronic elections, as well as the catalog of requirements for the operational environment of electronic elections presented in [Sc09b], which is based on a multitude of existing literature on e-voting security. We used applicable requirements from these sources for adapting the legal requirements to the technical field and integrated them in our template. As a result many requirements from the catalog [Sc09b] and [Co04] have been included in the template. We structured the resulting requirements based on the provisions from the legal framework. Our approach and especially the incorporation of existing technical standards are inspired by the interdisciplinary KORA[5] methodology [Ha92]. KORA describes a procedure to derive technical requirements and implementation proposals from legal stipulations for the similar scenario of information and communication systems. It has been tried and tested many times (see for example [Ha94] and [Id00]).

3.2 Template Structure and Content

The legal framework provides a basic structure for the security concept. For our template we adjusted the structure slightly in order to merge related requirements. Due to space limitations, we cannot present the complete security concept template in this paper[6]. We present the structure and an overview of the included requirements. We provide detailed examples in Section 4.3.

Technical, structural and organizational safeguards: The VSP shall describe all technical, structural and organizational measures essential for the operation of a VSP according to the legal regulations. Here we incorporated the majority of requirements from the catalog [Sc09b]. The section includes requirements for secure communication channels that provide unaltered and confidential communication between the voter and election server. Secure storage media must provide integrity, availability, and sufficient capacity. Secure erasure of sensible data as well as archiving and system cleansing measures must be provided.

[5] *Konkretisierung Rechtlicher Anforderungen*, eng.: Implementation of legal requirements

[6] The complete template will be published as a technical report shortly.

The VSP must realize the management of cryptographic keys and certificates and correct time for all system components. The VSP shall prevent attacks and unauthorized access to the voting server. The VSP must ensure correct setup of the voting system, set and publish time tables and register the voters correctly.

Technical products for remote electronic elections: The VSP shall list the technical products used for its electronic voting services, e.g., electronic voting software or election server hardware. If a product is certified this should be indicated here.
Setup and operation of remote electronic elections: The VSP shall demonstrate how it achieves availability; confidentiality and integrity of the voting services and election data; and how it realizes the operation of the election, the briefing of voters, and election host. The VSP's voting services must fulfill the election principles of the particular type of election. It must achieve the secure identification and authentication of the voters. The VSP must demonstrate how the legal requirements for ballot casting are satisfied [Sc09a]. Integrity and verifiability of tallying must be accomplished. The VSP must show how the election and adherence to law are documented and how integrity protection and archiving of such data are achieved. The secure system state must be ensured. This includes correct initial state, secure system interruption, and closure of the voting phase. The VSP must ensure the secure delivery of authentication means to the voters and correct representation of the electronic ballot.

Warranty of data protection: The VSP is required to prove that the applicable legal data protection provisions, i.e., the German Federal Data Protection Act, the German State Data Protection Act, and the German Teleservices Act, were observed. This can be achieved by a data protection audit, e.g., by the German Independent Centre for Privacy Protection Schleswig-Holstein[7] or *IT-Grundschutz*, which provides a data protection module[8].

Guarantee and maintenance of operation: The VSP shall demonstrate the precautions taken to guarantee and maintain the operation of the electronic voting service, especially in case of emergencies.

Personnel: The VSP shall demonstrate that the employed personnel have the reliability (i.e., guarantee that the legal provisions regarding the VSP's operation are observed) and the specialist qualifications (i.e., the knowledge, experience and skills necessary for their work).

Residual security risks: The VSP must assess and value remaining security risks in order to evaluate its reliability. This relates to the residual risk of system failure or interruption in particular with regard to deployed technology. The VSP may refer to valuation from evaluation authorities or manufacturers of deployed products. We discuss this in Section 4.4.

[7] https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm

[8] https://www.bsi.bund.de/cae/servlet/contentblob/475580/publicationFile/31090/moduleb01005_pdf.pdf

4 Combined Evaluation Approach

The legal framework [Sc09a] for VSPs does not demand a specific methodology for evaluating the security concept. However the incorporation of existing evaluation certificates is explicitly allowed. The intention is to facilitate the evaluation process and avoid double checking. We show how this approach can be realized by applying two approved evaluation methodologies for both voting system and operational environment to the security concept evaluation. We analyzed the requirements contained in our security concept template and found that many requirements are satisfied by either a voting system certified according to the Common Criteria Protection Profile [VV08] or by safeguards for the operational environment from the *IT-Grundschutz/ISO27001* catalogs [G05]. To this end we compared both the 'objectives' of the Protection Profile and the 'modules' and safeguards from the *IT-Grundschutz/ISO27001* catalogs with the requirements from our template. We describe this in more detail in the following sections. By utilizing an accordingly certified voting system and a certified operational environment, the security concept evaluation effort is reduced to evaluating only a few remaining requirements not covered by those certificates. We therefore propose to combine these methodologies for the security concept based evaluation of VSPs. Thereby we enable the combined evaluation and make it usable for the VSP evaluation. We introduce the methodologies in the following sections. While the *IT-Grundschutz* methodology originates in Germany, we point out that the "*IT-Grundschutz* based on ISO27001" certification is internationally accepted, as is Common Criteria.

4.1 Common Criteria

The "Common Criteria for Information Technology Security Evaluation" (CC) is an international standard (ISO/IEC 15408) for computer security evaluation and certification[9]. CC focuses on the evaluation of IT products like hardware or software components. Besides the evaluation of concrete products, CC allows specifying generalized security requirements for a family of products in a 'Protection Profile' (PP). Manufactures thereby are enabled to develop corresponding products. An evaluation authority then evaluates and certifies the compliance of the product's security functionality with the PP. In 2008, the German Federal Office for Information Security certified and published the "Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products" [*sic*] [VV08]. This PP specifies basic security requirements for online voting system software for non-political elections with low attack potential. The included requirements represent the essential foundation upon which voting systems for all election scenarios can build. It is an important step towards the certification of e-voting systems and is therefore planned to be mandatory for such systems in Germany. For our evaluation approach, the PP 'objectives' and 'assumptions' are relevant. The objectives specify the security goals which certified voting software is able to achieve.

In order to achieve these security objectives several assumptions are assumed to be realized, which cannot be achieved by the voting software. These assumptions must be satisfied by the operational environment. We show how PP-certified voting software can

[9] http://www.commoncriteriaportal.org/

facilitate the evaluation of a VSP. Our analysis revealed that many requirements included in the VSP's security concept can be fulfilled by such certified voting software and therefore do not need to be evaluated again in the VSP evaluation (see Section 4.3). Moreover we expanded the PP approach: since we incorporated the requirements from the catalog [Sc09b] into the security concept template (see Section 3.1), we especially included the assumptions towards the operational environment from the PP because these are contained in the catalog. Consequently a certified VSP realizes the secure operational environment assumed necessary in the PP to achieve the security objectives of the voting software. We discuss the applicability of the PP to the VSP scenario in Section 5. For further details on PP evaluation we refer to [VV08] and [VK07].

4.2 IT-Grundschutz/ISO27001

IT-Grundschutz (eng.: IT Basic Protection) provides a methodology to ensure and certify the security of complex 'information domains' which consist of infrastructural, organizational, personnel and technical components. *IT-Grundschutz* includes a comprehensive catalog of safeguards which can be implemented in order to satisfy protection requirements [G05]. The evaluation and certification methodology of *IT-Grundschutz* has been adapted to incorporate the methodology and the generic requirements on information security management systems from ISO27001 [Is08]. ISO27001 is an approved international standard that specifies requirements for the introduction, operation and improvement of information security management systems (ISMS) [KRS08]. It includes a sophisticated risk management methodology. ISO27001 is the first international standard for information security management that allows certification [G08a]. While ISO27001 specifies requirements, it only provides a very limited number of rather indefinite safeguards to fulfill those requirements. *IT-Grundschutz* can fill this gap by providing a multitude of concrete safeguards which can be used to satisfy the generic requirements from ISO27001. A synthesis of *IT-Grundschutz* and ISO27001 therefore seems plausible [KRS08]. Moreover, *IT-Grundschutz* includes predefined risk assessment to avoid a complex risk analysis at least in scenarios with normal protection levels. Concluding, the *IT-Grundschutz/ISO27001* approach facilitates implementation of the ISO27001 methodology by providing an immense set of safeguards and decreases efforts by reducing the need for costly risk analysis. Compared to classical risk analysis the *IT-Grundschutz* approach is more cost-effective and has been tested in practice for many years [G08a]. An *IT-Grundschutz/ISO27001* certification always includes an official ISO27001 certification, but, due to the additionally audited technical aspects, is more informative. The evaluation is performed by an external auditor certified by the German Federal Office for Information Security. In order to prove the achieved security level, *IT-Grundschutz* includes a certification methodology. There are three certification levels; the most comprehensive one is the 'ISO27001 certification based on *IT-Grundschutz,*' which incorporates the procedures and requirements of ISO27001 certification based on *IT-Grundschutz* safeguards.

The certification procedure comprises inspections of the reference documents, on-site inspection, and the generation of audit reports. For lower security level certification, *IT-Grundschutz* provides the less comprehensive and less costly 'entry level' (lowest level) and the 'continuation level' (intermediate level). The certification level is reflected in according to safeguard categories. While the entry level certification only requires the implementation of safeguards of category A, the continuation level requires A and B. The ISO27001 certificate based on *IT-Grundschutz* requires all safeguards –A, B, and C– to be implemented. The additional 'Z' safeguards present supplements that can be used in case of higher security requirements.

4.2.1 *IT-Grundschutz* procedure

We describe the procedure an institution has to perform in order to secure its information domain according to the *IT-Grundschutz* methodology [G08a, G08b].
At first, the architecture, components, and processes of the information domain must be identified and documented. This is done in the *structure analysis*. Subsequently, the *determining of protection requirements* assesses the level of protection that is appropriate for the particular objects specified in the structure analysis. All objects are analyzed in regard to the potential damage that could result from an impairment of the protective goals of confidentiality, integrity or availability. Then the protection requirement for each object of the structural analysis is classified as "normal," "high," or "very high." Next, the *selection and adaptation of safeguards* must be accomplished. In this modeling process, the prior identified objects of the information domain are associated with respective *IT-Grundschutz* modules. The modules are comprised of generic aspects (e.g., personnel, contingency planning), infrastructure (e.g., server room), IT systems (e.g., laptop), networks (e.g., WLAN), and applications (e.g., database). Each module is associated with specific safeguards suitable to protect the module from typical threats. The safeguards are classified in the categories *A (entry level)*, *B (continuation level)*, *C (certificate)* and *Z (additional)* in accordance with the targeted certification level. All safeguards must be examined and adapted to the specific scenario to ensure the appropriate function. Adaptations must be documented. The result of the procedure is an *IT-Grundschutz* model for use as a test plan for an existing information domain or as a development plan for an information domain in planning. Next, the *basic security check* is performed to provide an overview over the existing security level by comparing current state and target state. Therefore applicability and current implementation status of each selected safeguard are checked. The basic security check reveals where additional steps have to taken in order to implement the *IT-Grundschutz* safeguards.

4.2.2 Handling special requirements

For efficiency reasons, *IT-Grundschutz* uses a two-stage approach. In the first stage, a normal protection level and a typical application scenario are assumed. Here, the *IT-Grundschutz* safeguards provide an adequate security level. These safeguards can be determined quickly and efficiently allow for increases in the security level of the information domain.
However, in some scenarios, especially in an electronic election scenario, some objects might require safeguards at a higher security level. Therefore *IT-Grundschutz* provides the *supplementary security analysis* in the second stage. At first, it is applied to objects whose protection requirement was classified "high" or "very high" in regard to at least one of the protective goals of confidentiality, integrity or availability in the preceding

analysis. Secondly, a supplementary security analysis is indicated, if a very specific object cannot be modeled appropriately due to the lack of respective *IT-Grundschutz* modules. At last, objects which can be modeled with *IT-Grundschutz* modules, but which are deployed in an untypical way or in an untypical environment shall undergo a supplementary security analysis as well. *IT-Grundschutz* provides several options on how to handle such special requirements. First, the before mentioned additional 'Z'-safeguards can be implemented to achieve a higher protection level. If not sufficient, an additional *risk analysis* needs to be performed. *IT-Grundschutz/ISO27001* recommends a risk analysis approach described in [G08c]. The intention is to determine threats to the information domain that are not considered sufficiently by the regular *IT-Grundschutz* safeguards and to find appropriate safeguards. We sketch the basic steps. For all target objects the basic *IT-Grundschutz* threats are listed. Additional threats are determined by analyzing the specific protection requirements and the operating scenario for the target objects. Threat probability and potential damage are assessed. The protection level of implemented safeguards is checked. Next, measures are determined to handle the risks–risks can be reduced by additional safeguards, risks can be avoided (e.g., by restructuring business processes), risks can be transferred (e.g., by insurance policies) and under certain circumstances (e.g., low threat probability upon extremely costly safeguards), risks can be accepted and therefore remain. Such residual risks must be assessed and documented. Next a second basic security check is performed to check whether the security level has been improved. At last, *IT-Grundschutz* allows for adaptation by adding new modules to describe threats and safeguards for specific components which are not included in the *IT-Grundschutz* catalog so far. We discuss the applicability of *IT-Grundschutz/ISO27001* to the VSP scenario in Section 5.

4.3 Incorporating Protection Profile and *IT-Grundschutz*

We demonstrate how the proposed PP and *IT-Grundschutz/ISO27001* evaluation methodologies can be incorporated in the security concept based VSP evaluation. In our security concept template we linked respective requirements to corresponding PP objectives, meaning that these requirements are covered by the referenced objectives and therefore satisfied by PP-certified voting software. Respectively, to each requirement that has to be satisfied by the operational environment, we linked suitable *IT-Grundschutz* safeguards. To this end, we assumed a generalized VSP architecture and components and mapped them to *IT-Grundschutz* modules. Our results thereby also show how utilizing PP-certified voting software and incorporating existing *IT-Grundschutz/ISO27001* can reduce costs and efforts in the VSP evaluation. Due to space limitations, we are restricted to presenting examples from our security concept template. In the first example a PP-certified voting system would significantly reduce the extent of evaluation. We list the applicable PP objectives that are achieved by a certified voting system. For their complete description, we refer to [VV08].

BALLOT CASTING

References: VSP act § 8, VSP ordinance § 3

PP objectives: O.Abort (b), O.OneVoterOneVote (b), O.Correction (c), O.Acknowledgement (d), O.Proof (e)

The VSP must ensure that the voters

a) are able to cast an invalid vote,

b) are able to abort the voting procedure without losing elective franchise,

c) are able to correct their vote any number of times until the final voting,

d) receive a confirmation for their vote,

e) are not enabled by the voting system to show their voting decision to others.

Besides a), all aspects are completely satisfied by a PP-certified voting system. The evaluation authority only needs to ensure that a) is fulfilled.

The next example shows how PP assumptions are integrated into the security concept template and how they can be satisfied by *IT-Grundschutz* safeguards [G05].

SYSTEM TIME

References: Operational environment requirements catalog [Sc09b]

PP assumption: A.SystemTime

IT-Grundschutz safeguards: B 3.3 Network components (S 4.227 Use of a local NTP server for time synchronization), B5 Security of applications (S 5.67 Use of a time stamp service)

The VSP must make the correct time and time stamps available to the voting system, conforming to the actual time. The required exactness is defined by the election host. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

In this case, the referenced *IT-Grundschutz* safeguards satisfy the assumption. *IT-Grundschutz* safeguards can also be used to satisfy many other requirements from the security concept; e.g., "Guarantee and maintenance of operation" (see Section 3.2) can be realized by implementing the modules "B 1.3 Contingency planning concept" and "B 1.8 Handling security incidents" [G05].

However, our findings revealed that *IT-Grundschutz* safeguards cannot cover all of the requirements in the template. For example, the voter registration or secure delivery of authentication means cannot be described appropriately by *IT-Grundschutz*. Availability or integrity safeguards from the *IT-Grundschutz* might not be sufficient for all election scenarios. We explain how to proceed in the next section.

4.4 Application guideline

To apply the security concept template we recommend that the VSP performs the *IT-Grundschutz* procedure described above in order to define the specific protection requirements of its system and to analyze to what extent the *IT-Grundschutz* safeguards referenced in the template fulfill these requirements. If certain requirements cannot be covered, a supplementary security analysis and, based on its result, a risk analysis should be performed. Remaining risks identified in this analysis have to be noted in the Section "Residual security risks" in the security concept (see Section 3.2).

If the VSP already has an *IT-Grundschutz* certificate which includes the respective safeguards noted in the template, the particular requirements are satisfied and do not need to be evaluated again. Otherwise the linked safeguards serve as a recommendation on how to satisfy the requirements. However, the operational environment is no plug-in component with exactly defined functional properties; *IT-Grundschutz* safeguards must always be adjusted to the specific local conditions. Therefore the applicability of an existing *IT-Grundschutz* certificate to the security concept and the election scenario always must be checked by the evaluation authority.

If PP-certified voting software is utilized, the VSP can skip the implementation of safeguards for the requirements which are already satisfied by the certified voting software. The evaluation authority only must evaluate whether the remaining requirements have been satisfied. This reduces the costs and effort of conducting a VSP evaluation. To optimize the evaluation, voting software manufacturers could include the fulfillment of these remaining requirements for the voting software from our template to their CC certification to prove not only PP-compliance, but additional 'VSP-suitability.'

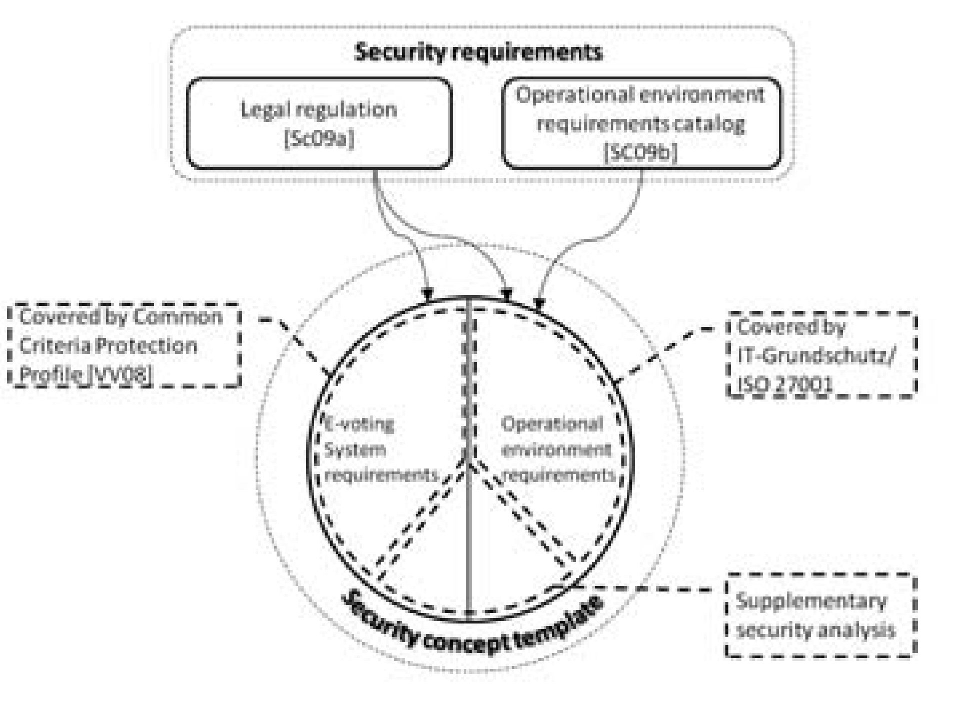
Security requirements
Legal regulation [Sc09a]
Operational environment requirements catalog [SC09b]
Covered by Common Criteria Protection Profile [VV08]
Covered by IT-Grundschutz/ ISO 27001
E-voting System requirements
Operational environment requirements
Supplementary security analysis
Security concept template

Figure 1: Application of evaluation methodologies

We illustrate our evaluation approach and the incorporation of the PP and *IT-Grundschutz/ISO27001* as well as the legal framework and the security concept template in Figure 1.

5 Discussion and Conclusion

We discuss the pros and cons of *IT-Grundschutz/ISO27001* and its applicability to the VSP scenario. Alternative certification methodologies like pure ISO27001 are mostly based on a general risk analysis approach. Threats and safeguards have to be determined from scratch. These are complex and costly tasks. In *IT-Grundschutz*, these steps are already integrated in every module of the *IT-Grundschutz* catalog. The large number of *IT-Grundschutz* safeguards simplifies implementation and can support the design process of VSPs. Hence, *IT-Grundschutz* evaluation is practicable. This supports the VSP approach. Basically, these safeguards ensure a normal security level for typical threats. This might not be sufficient for particular e-voting scenarios. However, *IT-Grundschutz* provides supplementary security analysis and risk analysis to adapt to special scenarios with higher protection requirements. Moreover new specific e-voting modules may be added to the *IT-Grundschutz* catalog. Consequently *IT-Grundschutz* seems applicable to the e-voting scenario and is a good choice for the certification of the operational environment of VSPs. Moreover, since many computer centers or similar IT service providers already have *IT-Grundschutz* certificates, it facilitates their evaluation in case they want to provide electronic voting services as VSPs.

However, in the case of already existing *IT-Grundschutz/ISO27001* certification the implemented safeguards need to be checked during the VSP evaluation for their suitability in the e-voting scenario. The effort should be determined and assessed in practical tests. Furthermore *IT-Grundschutz* is mostly used in Germany. This might reduce acceptance abroad. However, since the legal framework for VSPs is built for the German context, this does not affect the integration of *IT-Grundschutz* in the security concept evaluation.

The applicability of the PP to the VSP scenario is obvious. To develop a state-of-the-art evaluation approach, we need to incorporate this important evaluation concept for voting software. Admittedly, the PP is intended only for non-political election scenarios with low attack potential. However, it represents a foundation of requirements all other election scenarios build upon. Furthermore, since the legal framework for VSPs includes non-political elections as well, the PP perfectly fits into the VSP scenario. Regarding the incorporation of the PP into the VSP evaluation, this is an improvement on both sides; from the VSP perspective, using PP-certified voting software significantly facilitates the VSP evaluation. From the PP perspective, our VSP evaluation approach closes the gap of the PP evaluation because now the VSP is certified to achieve all open PP assumptions towards the operational environment. Thereby an overall evaluation is achieved. A VSP certified according to the security concept template complies with the legal framework, it represents the required operational environment for voting systems certified according to the PP, and it achieves the state-of-the-art in operational environment security as demanded in [Sc09b]. We point out that our combined evaluation approach of voting system and operational environment might be adapted to other e-voting scenarios outside the VSP context. However the existing legal framework, the security concept and the centralized design make the VSP scenario an ideal basis.

In this paper we presented a security concept template for VSPs and a corresponding evaluation methodology. By incorporating existing evaluation methodologies into the security concept evaluation, we presented a realistic approach which reduces the costs and effort of an evaluation. Concluding our work helps to enable the VSP concept and improves e-voting evaluation by combining the evaluation of voting systems and operational environment.

Bibliography

[Co04] Council of Europe. 2004. Legal, operational and technical standards for e-voting, Recommendation Rec(2004)11, Council of Europe Publishing, Strasbourg.

[G01] German Ordinance on Electronic Signatures (Signaturverordnung). 2001. http://bundesrecht.juris.de/sigv_2001/index.html/.

[G05] German Federal Office for Information Security. IT–Grundschutz Catalogues. 2005. http://www.bsi.de/english/gshb/download/it-grundschutz-kataloge_2005_pdf_en.zip/.

[G08a] German Federal Office for Information Security. 2008. BSI-Standard 100-1 Information Security Management Systems (ISMS), Version 1.5.

[G08b] German Federal Office for Information Security. 2008. BSI-Standard 100-2 IT-Grundschutz Methodology, Version 2.0.

[G08c] German Federal Office for Information Security. 2008. BSI-Standard 100-3 Risk analysis based on IT-Grundschutz, Version 2.5.

[G08d] German Federal Office for Information Security. 2008. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Prüfschema für ISO 27001-Audits.

[Ha92] Hammer, V., Pordesch, U., Roßnagel, A.:. 1992. KORA - eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme, Arbeitspapier 100. provet, Darmstadt.

[Ha94] Hammer, V., Pordesch, U., Roßnagel, A., Schneider, M.J. 1994. Vorlaufende Gestaltung von Telekooperationstechnik - am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235. Sankt Augustin.

[Id00] Idecke-Lux. 2000. Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz. Nomos. Baden-Baden.

[Is08] ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems Requirements Specification, ISO/IEC JTC1/SC27, 2008.

[KRS08] Kersten, H., Reuter, J., Schröder, K.-W. 2008. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg, Wiesbaden.

[La08] Langer, L., Schmidt, A., Buchmann, J. 2008. Secure and Practical Online Elections via Voting Service Provider. In *Proceedings of ICEG 2008*, 255-262. ACI.

[RJ07] Reinhard, K.; Jung, W. 2007. Compliance of POLYAS with the BSI Protection Profile–Basic Requirements for Remote Electronic Voting Systems. In*VOTE-ID*, Lecture Notes in Computer Science vol. 4896, ed. A. Alkassar and M. Volkamer, 62–75. Springer.

[Re07] Republic and Canton of Geneva State Chancellery. Report by the Geneva government to the Geneva parliament on the internet voting project. 2007. http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf/.

[Sc09a] Schmidt, A., Heinson, D., Langer, L., Opitz-Talidou, Z., Richter, P., Volkamer, M., Buchmann, J. 2009. Developing a legal framework for remote electronic voting. In *Proceedings of VOTE-ID 2009 Second international conference on E-voting and Identity, Luxembourg, LNCS 5767*, 92-105. Springer.

[Sc09b] Schmidt, A., Volkamer, M., Langer, L., Buchmann, J. 2009. Towards the impact of the operational environment on the security of e-voting. In *Proceedings of INFORMATIK 2009, LNI 154*, 1814-1826. GI.

[Tr09] Tranchard, S. 2009. The State of Geneva designs a secure Internet voting system. In *ISO Focus* 6:38-39.

[VKG07] Volkamer, M., Krimmer, R., Grimm, R. 2007. Independent Audits of Remote Electronic Voting - Developing a Common Criteria Protection Profile. In *Proceedings of Elektronische Demokratie in Österreich - EDEM '07*, 115-126. Vienna: OCG Verlag.

[VV08] Volkamer, M., Vogt, R. 2008. Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte. Common Criteria Protection Profile BSI-PP-0037. https://www.bsi.bund.de/cln_156/ContentBSI/Themen/ZertifizierungundAkkreditierung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0037/.

[WVM07] Weldemariam, K., Villafiorita, A., Mattioli, A. 2007. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In *Proceedings of the F*irst C*onference on E-Voting and Identity (VOTE-ID), LNCS 4896.*