Holistic and Law Compatible IT Security Evaluation:

Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA

Daniela Simić-Draws, Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, Koblenz, Germany

Stephan Neumann, Center for Advanced Security Research Darmstadt, Technische Universität Darmstadt, Darmstadt, Germany

Anna Kahlert, Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Universität Kassel, Kassel, Germany, Kassel, Germany

Philipp Richter, Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Universität Kassel, Kassel, Germany, Kassel, Germany

Rüdiger Grimm, Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, Koblenz, Germany

Melanie Volkamer, Center for Advanced Security Research Darmstadt, Technische Universität Darmstadt, Darmstadt, Germany

Alexander Roßnagel, Projektgruppe verfassungsverträgliche Technikgestaltung (Provet), Universität Kassel, Kassel, Germany, Kassel, Germany

ABSTRACT

Common Criteria and ISO 27001/IT-Grundschutz are well acknowledged evaluation standards for the security of IT systems and the organisation they are embedded in. These standards take a technical point of view. In legally sensitive areas, such as processing of personal information or online voting, compliance with the legal specifications is of high importance, however, for the users' trust in an IT system and thus for the success of this system. This article shows how standards for the evaluation of IT security may be integrated with the KORA approach for law compatible technology design to the benefit of both – increasing confidence IT systems and their conformity with the law on one hand and a concrete possibility for legal requirements to be integrated into technology design from the start. The soundness of this interdisciplinary work will be presented in an exemplary application to online voting.

Keywords: *Common Criteria, Information Technology (IT) Security Evaluation, ISO 27001, IT-Grundschutz, Law Compatible Design, Online Voting*

DOI: 10.4018/jisp.2013070102

INTRODUCTION

Embedding IT in everyday life, brings not only many advantages, but also increases risks. For example, in case of malfunction economic damages or – in the worst case – damages for life and health are possible. IT security plays a key role in preventing these risks. In order to make IT security measureable and comparable, different standards for the evaluation of IT Security have been developed. As an internationally accepted standard, the Common Criteria are used for the evaluation of IT related products. This evaluation only includes security objectives, directly related to the IT product. However, security objectives concerning the product environment are also of importance when analysing IT security. A broader approach is chosen by ISO 27001/IT-Grundschutz with its organisational perspective: Here, organisation, infrastructure, applications and employees are considered. In combination they constitute the so called *information domain to be protected*. Thus ISO 27001/IT-Grundschutz aims at enforcing and evaluating a basic protection level for complete organisations. Usually, IT security evaluation standards, such as Common Criteria or ISO 27001/IT-Grundschutz consider system security from a technological and organisational point of view and do not specifically integrate legal requirements for the system in different contexts. A fixed integration of national law into internationally applicable standards would be impractical. Integrating legal evaluation of IT security is crucial, however, for systems to be designed in a law compatible way. This might lead to higher acceptance and increasing trust by users. Integration with IT security evaluation standards would provide the law with an effective option to accomplish its normative requirements in IT environments. Legal requirements should be integrated with such standards in an easy and flexible way, in order to be able to adjust them to different jurisdictions and application areas. Thus, IT security evaluation and assertion of legal requirements would both benefit from integration.

Therefore, we proceed to show how the approach for law compatible technology design KORA (Konkretisierung rechtlicher Anforderungen/ concretisation of legal requirements), Common Criteria and ISO 27001/IT-Grundschutz may be integrated into an evolving interdisciplinary approach for the design and evaluation of secure and law compatible IT systems. After presenting the state-of-the-art of related work, the article will first give an extended overview of the applied approaches and standards. Then it will be shown how these approaches and standards may be integrated into one evolving interdisciplinary approach for law compatible IT-security evaluation. We first describe possible interfaces between the presented approaches and standards and illustrate possible combinations. Afterwards, application of our concept will be shown by way of an example from online voting: ballot secrecy in remote online voting systems. Finally, a conclusion will be given on the results of the interdisciplinary work and an outlook on necessary future work.

RELATED WORK

As IT security engineers and lawyers have a different professional background, difficulties often arise when working together on a topic. Even if both strive for the same goal, they usually operate by means of different approaches and different terms or the same term indicates slightly or even totally different concepts. In order to be able to operate effectively, a mutual basis must be found. Already several works have been conducted considering the question of how to enhance security evaluation approaches with legal aspects.

Breaux et al. (Breaux & Antón, 2005a; Breaux & Antón, 2005b; Breaux & Antón, 2008; Breaux, Vail, & Antón, 2008) address the challenges of highly regulated domains, in their case the U.S. Health Insurance Portability and Accountability Act. The authors convert legal texts into formal specifications in terms of rights, obligations, and constraints, thereby resolving ambiguities. *Breaux et al.* focus their research in one direction towards software engineering. Our work, however, aims at involving legal researchers and computer scientists each in a perpetual discourse moving back and forth between all levels of the design process. Creating this interdisciplinary flexibility turns out to be of central importance so that conflicts between technical goals or conflicts between technological solutions may be solved adequately.

Beckers et al. (2012a) aim at solving problems, they identified in the works of *Breaux et al.* They present a pattern-based approach for identification and analysis of relevant legal provisions in requirement engineering. A concept for deriving software requirements from legal provisions has been presented in an additional paper in 2012 (Beckers et al., 2012b). Integrating legal requirements with technology development has, however, already been conducted successfully in a number of research projects with the legal approach for technology design KORA. In our work, we therefore aim at integrating KORA with Common Criteria and ISO 27001/IT-Grundschutz, in order to incorporate expertises and requirements from both disciplines into system development and evaluation. A first promising integration of KORA and Common Criteria has already been conducted in 2011 (Bräunlich et al., 2011), so that we are able to continue work from this point on.

KORA

KORA is an approach developed within *provet* (Projektgruppe verfassungsverträgliche Technikgestaltung/Project Group Constitution Compatible Technology Design) in order to support technology development in a legal way (Hammer et al., 1993; Idecke-Lutz, 2000; Laue, 2009; Pordesch, 2003; Roßnagel, 2008; Scholz, 2003; Schwenke, 2006; Stadler, 2006).

The approach describes how to concretise abstract legal requirements gradually towards technical design proposals by conducting an interdisciplinary discourse. KORA bridges the gap between rather abstract legal requirements and precise technical goals and thus the interdisciplinary gap between law and technological science. Legal requirements are identified and gradually refined as adequate and specific technical formulations. If this gap is not closed while developing technology, a legal evaluation of technology remains possible only afterwards. In case of illegality, the law might then be a barrier to the appliance of new technology. However, if the gap is closed successfully at an early stage, new technology can be designed in such a way as to fulfil the legal requirements right away. The results compiled with KORA are developed with the goal to fulfil legal requirements in the best possible way. Thus they may exceed minimal legal requirements, and will not easily be prone to become obsolete, if legal practice should become stricter than before.

Before applying KORA, relevant legal specifications need to be identified. They may result from European Law, the national (in our case the German) constitution or from subconstitutional national law. The legal context as well as the basis application area of technologies has to be considered to gain relevant specifications.

In order to derive design proposals from legal specifications, the KORA approach is carried out in four consecutive steps:

First, *legal requirements* are derived from the legal specifications. Legal requirements do not contain technological attributes but rather social functions. However, these social functions can be influenced by application of technology. Legal requirements have to ensure validity of the social functions of the legal specifications considering application of the specific technology. For this purpose chances and risks for the social function through appliance of the technology, are described. The legal requirements themselves are legal guidelines related to the technological systems. By complying with the legal requirements, risks should be reduced and chances improved. The requirements are described in legal terminology.

The second step concretises the legal requirements into more detailed *legal criteria*. These criteria describe how the technology can fulfil the legal requirements without yet committing to a certain organisational, technological or legal approach. Although legal terminology is used, the criteria are approximated to technical terms.

In the third step, legal criteria are concretised into *technical design goals*. These goals describe elementary functions, which need to be fulfilled, for the technology to be considered criteria compatible. As technical design goals are described in technical terminology, a language change is taking place in this step.

Finally, in the fourth step, concrete *technical design proposals* are derived from the technical design goals by discussing feasible ways of realisation of the goals. The technical design proposals provide design recommendations for the technical system. They are performance characteristics which constitute technical functions (Hoffmann et al., 2012). Each design proposal should comply with at least one of the technical goals.

KORA is not meant primarily to evaluate existing products, though it may be used to this end, also. It is rather an approach for derivation of technical goals and design proposals from abstract legal specifications in order to enable a law compatible design of technology. Accordingly, the main advantage of KORA is the inherent possibility to transfer legal specifications into technical design proposals. For this purpose an interdisciplinary discourse is needed during all steps as well as a perpetual refitting of all steps. Therefore, results of any step can and need to serve as input to any other. This nature of KORA provides the opportunity to integrate it with other approaches at several interfaces.

A risk analysis is conducted in KORA when deriving legal requirements. This step, often carried out by legal researchers, could benefit from expert IT security risk analysis as in Common Criteria and ISO 27001/IT-Grundschutz.

COMMON CRITERIA OF PRODUCT SECURITY

The Common Criteria (CC) (ISO/IEC, 2009) is an IT security evaluation approach with a product point of view. In combination with the Common Evaluation Methodology (CEM, 2009), CC provides an internationally accepted standard for the evaluation and certification of IT security requirements.

The standard allows selecting applicable security requirements for a specific product or a group of products. This is done in the *Protection Profile (PP)*: The *Introduction* of a Protection Profile always begins with the so-called reference containing metadata: PP Title, PP version, author, date and version of the underlying CC documentation. Then, the *Target of Evaluation (TOE)* is defined and its intended functionality described in detail. A TOE may be a single product or system, but it might also consist of distributed components. The detailed specification of a TOE is at the discretion of the PP-Author. The introductory part of the PP closes with the conformance claim and the targeted *Evaluation Assurance Level (EAL)*. The security problem is separately described in the section *Security Problem Definition (SPD)*. The SPD consists of the identification of threatened assets, participating subjects and a description of potential *Threats (T)*. A distinction is made between primary and secondary assets: Protecting primary assets is the core task of the TOE. In contrast, secondary assets exist as long as the TOE exists. They are necessary for the protection of the primary assets.

The Security Problem Definition also contains the detailed formulation of *Organisational Security Policies (P)* and *Assumptions (A)*. *Organisational Security Policies* must be fulfilled by the TOE itself and the security environment the TOE is embedded in. *Assumptions*, by contrast, are related exclusively to the security environment of the TOE. The security environment does not only contain additional connected IT systems, but also surrounding processes. Therefore, *Assumptions* need not be fulfilled by the TOE itself. However, *Assumptions* are essential for the effectiveness of the TOE's *Security Functionalities (SF)*. Failure of *Assumptions* during operation of the TOE affects the TOE security. Within the Common Criteria, a specification of means to fulfil the *Assumptions* as well as their evaluation is not intended. Assumptions may for example result from threats which are assumed not to be realistic or insignificant or it may be assumed, that threats will be addressed by organisational means. The protection against threats in this last case could be evaluated by other standards. For example, the protection of a server (as a part of the operational environment of a TOE) against non-authorised access is usually formulated as an assumption.

The security problem described above can be countered by specific *Security Objectives (O/OE)*. *Security Objectives* must be formulated separately for the TOE itself (O) and the security environment (OE). These specifications prove that the *Security Objectives* are able to cover all defined aspects for the TOE and its security environment. Each security objective states explicitly the encountered threats, the considered policies and the covered assumptions. Security objectives (O) for the TOE refer to threats (T) and organizational security policies (P). Additionally, security objectives for the TOE environment (OE) refer to the abovementioned assumptions. Moreover, it has to be proven that every *Threat* and every *Policy* is addressed by at least one *Security Objective (O)*. In addition, every *Assumption* must be addressed by at least one *Security Objective for the security environment (OE)*.[1] If however no standard or evaluation method or other procedure exists, which might enforce a specific assumption, this leads to the problem, that this assumptions leads to OEs which need not be enforced: OE(ne). OE*(ne)* is no abbreviation from CC, but was introduced in this paper, in order to distinguish between assumptions, which need to be reviewed legally and those which need not be reviewed legally in the following.

As a final refinement, *Security Objectives* are translated into the standardised language of the Common Criteria. This results in a list containing *Security Functional Requirements (SFR)*. They include requirements with explicitly desired and explicitly undesired conditions of the TOE. All possible SFR are provided in the second part of the Common Criteria. They are subdivided into eleven classes and families. Every class represents a superior security aspect (e.g. FCO: Communication) and is itemized in separate families (e.g. FCO_NRO: Non-repudiation of origin). Before a *Security Objective* can be translated into an SFR, the regarding class and the specific family need to be identified. The CC provides strict guidelines on how to perform this translation. Subsequently, a table that juxtaposes *Security Objectives* and SFRs is created. It serves as proof that every *Security Objective* is covered by at least one SFR and vice versa. This proof of evidence should be formulated in natural language. Also, some SFRs depend on one or more other SFRs. It is necessary to resolve these dependencies by using a separate table. The *Protection Profile* closes with a detailed explanation of the *Security Assurance Requirements*. It gives an overview of the targeted security level and serves as basis for the PP evaluation.

Evaluation can be carried out for the validation of a *Protection Profile (PP)* or of a specific product. The latter is called a *Security Target (ST)*. If a *Protection Profile* is evaluated, its completeness as well as its consistence is checked. In order to check its completeness, it is necessary to check if the formulated threats, organizational security policies and assumptions are completely covered by security objectives (O and OE). In the case of product evaluation, the ST can be based on an existing and already evaluated PP. The formal structure of a *Protection Profile* is similar to that of a *Security Target*. The ST takes the SFRs that are defined in the PP and compares them with the actual *Security Functionalities (SF)* implemented in the product.

Using the Common Criteria for evaluation of IT security has many advantages. CC provides an objective, well-structured and well-accepted evaluation of security attributes of a product. The internationally accepted certification can serve to gain a competitive advantage. Limitations concerning organisational design and the specification of assumptions require an integrated evaluation concept, however.

ISO 27001/IT-GRUNDSCHUTZ

Originally, two major evaluation standards for security objectives for the operational environment co-existed, ISO/IEC 27001 (2005) and IT-Grundschutz (BSI, 2008a). Both have been integrated in the recent IT-Grundschutz catalogues. IT-Grundschutz actually is a realisation of ISO 27001 as an applicable approach. An IT-Grundschutz-evaluation includes an evaluation by ISO 27001.

The IT-Grundschutz has been developed by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik/BSI). The motivation behind IT-Grundschutz is to provide safeguards for protection against business processes, applications, and IT systems in a holistic approach covering organisational, personnel, infrastructural, and technical aspects, thereby providing a security level adequate for standard protection requirements. IT-Grundschutz is divided into a catalogue of building blocks, catalogues of threats, and catalogues of safeguards. Building blocks are categorized into the following classes:

- **B 1:** Overarching aspects of the information security
- **B 2:** Security of the infrastructure
- **B 3:** Security of IT systems
- **B 4:** Network Security
- **B 5:** Application Security

Building blocks contain a short description for corresponding components, procedures, and IT systems as well as an overview of threats and safeguard recommendations.

Threats outlined in the building blocks are summarised in catalogues of threats. These threats (T) are classified as follows:

- **T 1:** Force majeure
- **T 2:** Organizational deficiencies
- **T 3:** Human errors
- **T 4:** Technical failure
- **T 5:** Intentional wrongdoing

For instance, T4.1 refers to *"Breakdown of energy supply"*.

Similar to the catalogue of threats, the catalogue of safeguards summarises the safeguards mentioned in the catalogue of building blocks. These safeguards (S) are categorised as follows:

- **S 1:** Infrastructure
- **S 2:** Organisation
- **S 3:** Personnel
- **S 4:** Hard- and Software
- **S 5:** Communication
- **S 6:** Emergency provisions

For instance, infrastructural safeguard S.141 describes protection against external electromagnetic radiation, technical safeguard S4.199 intends to protect against dangerous file formats. Safeguards are classified into three categories based on the targeted certification level, namely the *entry level* (A), the *intermediate level* (B), and the *ISO 27001 certification level* (Z).

The steps of the IT-Grundschutz evaluation process can be captured as follows:

The information domain to be protected is the starting point. It includes the whole organisational environment including infrastructure, applications and employees across all levels of the organisation. This information domain does not necessarily cover the entire system, but it serves as a base for the overall security implementation. During structural analysis, the current architecture of the information domain is analysed and documented.

Afterwards, protection requirements are determined. Based on the structural analysis, the degree of protection for the infrastructure, components, and processes is assessed. Therefore, infrastructure, components, and processes are investigated and potential damage resulting from a violation of confidentiality, integrity, and availability is estimated. IT-Grundschutz includes an abstract classification of protection requirements between "normal", "high" and "very high".

The next step is to model the information domain under examination with the help of building blocks in order to conduct selection and adaptation of safeguards. Therefore, building blocks are mapped onto target objects of the information domain, e.g., infrastructure, components, and processes. From a practical perspective, it proves to be best common practice to proceed in the order of the building blocks; hence from general to more concrete aspects. IT-Grundschutz modelling consists of deciding if and how the modules in each building block are adequate to model the information domain. Based on the modelling process, appropriate safeguards are determined in order to mitigate the risk of potential damage identified in the prior step. In addition to the selection of appropriate safeguards, these safeguards need to be adapted to the information domain of investigation in order to ensure the protection requirement.

In the next step, the so called basis security check, the current state of the IT infrastructure, components, and processes is identified. This state and the target state deduced from the previous steps are compared with reference to the determined protection requirements. The outcome of this phase is an overview of the relevance of previously determined safeguards in the concrete information domain. Therefore, interviews are conducted with responsible personnel about the implementation status of individual safeguards.

Finally, an extended security check is performed: Protection requirements classified “high” or “very high” call for further security analysis. Here, IT-Grundschutz integrates a comprehensive risk analysis. The risk analysis is based on IT-Grundschutz, BSI Standard 100-3 (BSI, 2008b). The goal of this analysis is to determine threats that were not sufficiently considered by the standard safeguards in the IT-Grundschutz catalogues. For these threats corresponding safeguards will then be deduced.

Finally, selected and adapted safeguards that are only partially or not implemented as well as special purpose safeguards are implemented into the information domain.

IT-Grundschutz with its comprehensive set of safeguards covers all aspects of information security management, from infrastructure, to organisation, to personnel, to hard- and software, to communication and emergency provisions. Implemented safeguards are not meant to protect legally derived assets, however, but assets deemed important by IT security experts. Furthermore, as indicated by its name, the approach has been invented to achieve a basic degree of information security, rather than an in-depth analysis of process dependencies. The modular approach of IT-Grundschutz leads to a modest level of security in a simple and cost-effective manner. Thus, IT-Grundschutz would gain from integration with KORA and Common Criteria.

INTEGRATION OF KORA, COMMON CRITERIA AND ISO 27001/IT-GRUNDSCHUTZ

During comparison of KORA, CC and ISO 27001/IT-Grundschutz, it became apparent, that an integration of these approaches would be able to eliminate certain weak points of each approach:

- KORA is an approach for derivation of technical design proposals from legal requirements. Risk analysis in KORA does not usually fully achieve the expertise and structure of IT security evaluation and could be enhanced by the procedures of CC and ISO 27001/IT-Grundschutz.
- In contrast, security requirements derived with the Common Criteria do not systematically integrate legal assets and provisions. Because the Common Criteria approach is focused on IT products, the organisational point of view is not taken into account. CC, thus, could be enhanced by both, KORA and ISO 27001/IT-Grundschutz.
- IT-Grundschutz does not systematically take into account legal aspects, either. In contrast to Common Criteria, IT-Grundschutz has a more general view on IT security, because the whole organisation is considered. The evaluation of an IT-system is not as detailed as in Common Criteria.

Thus, ISO 27001/IT-Grundschutz, also would benefit from both, KORA and CC.

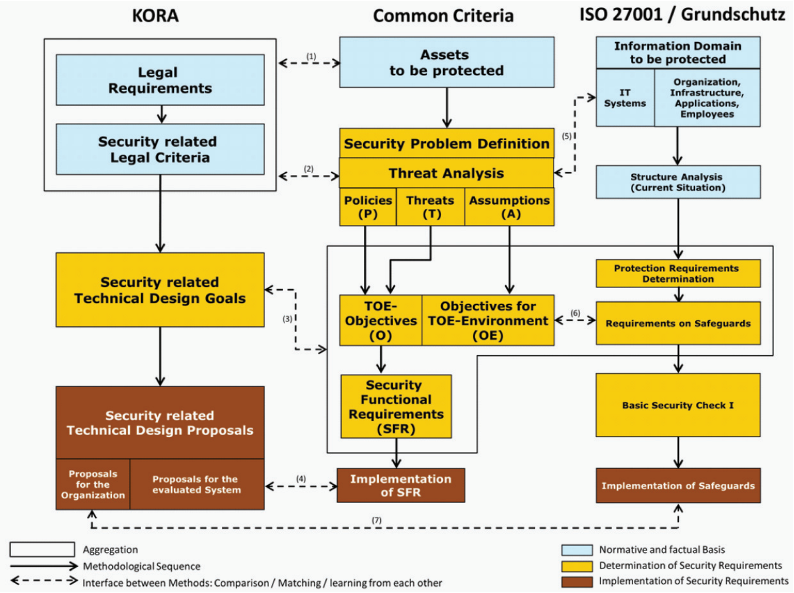
By integrating all three approaches, we aim at improving communication between legal researchers and computer scientists and at improving IT design and evaluation processes.

Figure 1 shows the steps of each approach and the identified interfaces. In this context, the term interface indicates not a function call or a kind of adaptor. Here, it stands for the comparison and matching of process steps with the aim of enabling the involved parties – legal researchers and computer scientists – to learn from each other. Hence, possible paths through the integration mainly serve for comparison of results. Potential aggregations of single steps and identified interfaces are described in the following paragraphs:

A first aggregation summarises legal requirements and the security related legal criteria. The main difference between these two steps is the degree of detailing. Between the aggregation of the first two KORA steps and the Common Criteria approach two interfaces (1) and (2) can be inserted: (1) Assets to be protected by a TOE are often laid down in legal provisions. For example ballot secrecy as an asset is fixed by law. Also, protection of an IT asset may be demanded by law, if it is identified as important for a legal asset. (2) Formulating legal requirements and criteria includes a risk analysis and an implicit consideration, which assumption is acceptable and which is not. Hence, a comparison and transition between the aggregated legal requirements and criteria and the elements of the Security Problem Definition is possible, because their content correlates as well as the procedure to derive this content. A transition from KORA to Common Criteria here means the systematisation of aspects, the legal researcher was implicitly thinking about during formulating the requirements and criteria. A transition and comparison from CC to KORA reveals, which legal aspects the CC-author did not considerate. Also, assumptions may be reviewed legally at this interface.

Assumption, which assume, that a security aspect will be achieved with an additional evaluation approach (e.g. ISO 27001/IT-Grundschutz in case of organisational aspects) and which thus lead to OEs, that will be enforced, need not be

Figure 1. Integration of security requirements engineering and evaluation approaches


KORA
Common Criteria
ISO 27001 / Grundschutz
Legal Requirements
Security related Legal Criteria
(1)
(2)
Assets to be protected
Security Problem Definition
Threat Analysis
Policies (P)
Threats (T)
Assumptions (A)
Information Domain to be protected
IT Systems
Organization, Infrastructure, Applications, Employees
(5)
Structure Analysis (Current Situation)
Security related Technical Design Goals
(3)
TOE-Objectives (O)
Objectives for TOE-Environment (OE)
(6)
Protection Requirements Determination
Requirements on Safeguards
Security Functional Requirements (SFR)
Basic Security Check I
Security related Technical Design Proposals
Proposals for the Organization
Proposals for the evaluated System
(4)
Implementation of SFR
Implementation of Safeguards
(7)
Aggregation
Methodological Sequence
Interface between Methods: Comparison / Matching / learning from each other
Normative and factual Basis
Determination of Security Requirements
Implementation of Security Requirements

justified legally. Assumptions, which assume, that certain threats need not be considered, however, and which thus lead to OEs that need not be enforced, OE(ne), need to be reviewed legally and may be reviewed to a certain degree.

If a legal provision demands "secure" or "sufficiently secure" storage or processing of data, the question arises: How secure is secure enough? Since absolute security or absolute secrecy is not possible, a threshold must be found by which compliance with or breach of the provision, in our case Art. 38.1 GG (Grundgesetz, the German Constitution) may be measured. In a first step, a way must be found how to make security measurable at all and then a sufficient degree of security must be determined. Answers to these questions are usually not contained in legal provisions, even if they specifically address technological security.

Thus, in technology law this problem is usually managed by applying "Security Philosophies", based on expertise from engineering science (Roßnagel, 1997; Roßnagel & Neuser, 2006). Here, two general approaches may be applied: probabilistic or deterministic risk assessment.

Probabilistic assessment of risks means, that probability of damages, initiating events, dependability of security systems and probability of specific development of damages are analyzed. A probability statement alone, says nothing on the matter, if this probability is legally tolerable or not, however. Normative risk thresholds would be needed in order to determine intolerable risk a tolerable "remaining risk". As far as either no probability calculations or no normative risk threshold are at hand, probabilistic risk assessment is not usable to this end. A probabilistic risk determination for online voting has been drafted in Philipp Richter, *Wahlen im Internet rechtsgemäß gestalten* (Richter, 2012, p. 199 ff). This draft, however, has not found its way into legal provisions, as of yet, and also needs to be specified in the future.

In deterministic risk assessment, certain threats are assumed and a system is evaluated and tested with respect to protection against these threats. In this approach all measures are deemed "necessary", which are necessary in order to manage these predetermined threats. Determination of threats to be considered and determination of necessary counter measures are usually conducted based on expert knowledge gained in past damage events. Threats, not covered and the possibility of security measures failing are the tolerated "remaining risk" in this approach. Exactly this deterministic approach is applied, when a CC-assumption states, that a threat does not need to be considered.

From the legal viewpoint, the threats determined by technological experts, determine the basic conditions for the layout of security systems. In their construction, criteria from reliability engineering need to be observed. Functionality of security needs to remain intact even, if individual components of the system fail. Proof of security is provided by presenting measures taken for protection against the predetermined threats. The advantage of the deterministic approach is, that its requirements are clear and testable.

As a conclusion for a legal justification of assumptions, this means, that assumptions, which lead to OEs, that need not be enforced OE(ne) are lawful, as far as this is in good accordance with the art of IT security engineering, considering the value of the protected assets. If, however, a threat is predetermined as considerable, it must be countered with security measures. Assumptions, which need to be enforced by measures outside CC, need not be reviewed legally. Application of these principles will be shown in chapter 7.

A second aggregation combines security requirements formulated in natural language (Common Criteria Security Objectives, ISO 27001/IT-Grundschutz requirements on safeguards) and (semi)formal language (Security Functional Requirements). These can be compared with the technical design goals of KORA. It is also possible to use semi-formal expressed security objectives as an input for the KORA design goals or, vice versa, technical design goals from KORA as input for the aggregated security requirements. The interface (3) between the security related technical design goals and the aggregation relates to all elements inside the aggregation.

At the level of implementation, two interfaces have been identified: The superset of security related technical design proposals is split into two subsets – proposals for the organisation and proposals for the evaluated system. Because of their systemic focus, the proposals for the evaluated system can be matched at interface (4) with the implementation of security functional requirements (SFR) in CC. The implementation of SFR is formulated in a Common Criteria Security Target. Additionally, there will be KORA-proposals addressing organisation. Since ISO 27001/IT-Grundschutz offers its own catalogue for organisational safeguards, interface (7) allows a comparison of organisational KORA-proposals and the catalogue S 2. Conflicts between proposals are possible. In such cases, formulated proposals need to be balanced legally. This is now possible systematically by matching CC-SFR and ISO 27001/IT-Grundschutz-safeguards with KORA proposals.

Regarding Common Criteria and ISO 27001/IT-Grundschutz, *a further interface* (5) namely between security problem definition and IT-Systems – as a sub-element of the Information Domain to be protected – has been identified. Evaluation of an IT System can be conducted much more precisely in Common Criteria than in ISO27001/IT-Grundschutz. On the other hand, the IT System as Target of Evaluation (TOE) can be evaluated from a holistic organisational perspective with the help of ISO27001/IT-Grundschutz.

Common Criteria offers no possibility for an evaluation of security objectives regarding the system environment. This disadvantage has been solved *by introducing the sixth interface* (6) namely between environmental objectives and requirements on safeguards determined in the IT-Grundschutz catalogues.

The developed integration can be used in different ways – it is not necessary to use all identified interfaces at the same time: Starting with the mainly used approach, the aim is to complete the results of the main approach by comparison with the other approaches. For example, completeness of a Protection Profile can be checked. This is the application, the authors use as proof of concept in the next section. By integrating process steps of KORA, the Protection Profile could be enhanced to integrate legal requirements systematically by importing legal criteria as assets and then conducting a threat analysis. Another use case could have the aim to conduct a much more precise evaluation of the information domain component IT-Systems with the help of Common Criteria. Every possible use case can be marked as a characteristic path through the integration.

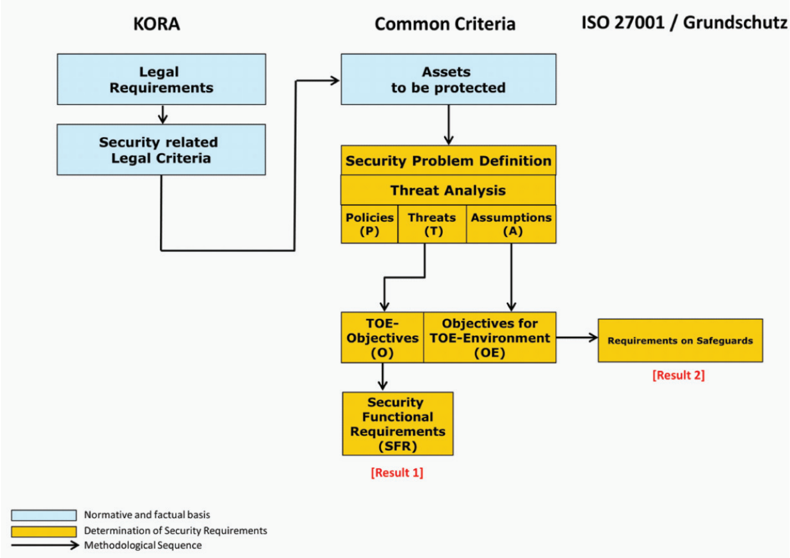
APPLICATION: BALLOT SECRECY

Since elections in general are of great importance within our social and political society, application of the integrated approach will be explained by referring to the ballot secrecy in online elections. By using the developed integration (see Figure 1) we are able to derive three legal criteria that ensure secrecy in the context of remote online voting. These legal criteria will be transferred into Common Criteria Assets in order to carry out a CC security analysis. By doing this, security objectives both for the IT System and the organisation are derived. The results can be used as a sound basis for the formulation of technical design goals (KORA) or the implementation of safeguards (ISO 27001/IT-Grundschutz). The implementation of requirements is not part of this work section, however. The traversed path through the integration is shown in Figure 2.

Ballot secrecy is one of the electoral principles named in Art. 38.1 GG. Thus, parliamentary elections have to follow this principle. Consequently, the starting point for the first step of KORA will be the principle of ballot secrecy from Article 38.1 GG.

From ballot secrecy follows the legal requirement “indeterminable choice” (Richter, 2012). Indeterminable choice addresses secrecy of the voter’s behaviour from two viewpoints.

Figure 2. Exemplary usage of the developed framework


KORA
Common Criteria
ISO 27001 / Grundschutz
Legal Requirements
Security related Legal Criteria
Assets to be protected
Security Problem Definition
Threat Analysis
Policies (P)
Threats (T)
Assumptions (A)
TOE-Objectives (O)
Objectives for TOE-Environment (OE)
Requirements on Safeguards
[Result 2]
Security Functional Requirements (SFR)
[Result 1]
Normative and factual basis
Determination of Security Requirements
Methodological Sequence

First, it must not be possible to associate the voter with his voting decision. Only the voter himself should be able to know which decision was his decision. A revelation of the voting decision by the voter is harmless if there is no provable receipt of the vote and thus the truth of the voter`s assertion cannot be confirmed. Furthermore, "indeterminable choice" means, that the voting decision, even without a link to the voter, must stay secret until the election period is over. Intermediate results must not be published during the election period, so that every voter has the same "tactical" information at the moment of voting.

In summary, the election process has to be created in such a technical way as to prevent identification of a voter`s ballot and intermediate results.

From "indeterminable choice" three legal criteria are derived: "unknown content", "unknown voter", and "data minimisation". The first legal criterion "unknown content" expresses the requirement that it must not be possible for anyone to become aware of the content of bindingly cast ballots before the end of the election period. Though the content has to be processed for counting the votes, it must remain unknown until this point in time. Hence, no one must see the ballot content apart from the voter, who cast the ballot. In case of paper based voting, unknown content is guaranteed by using ballot boxes, which are not opened until the election officially has ended. Such a protection of the ballot content has to be ensured in online voting as well. The ballot content must be protected against persons, who try to spy out the decision by looking at the display at the time of voting as well as by accessing the terminal, which is used for casting the ballot. Appropriate actions have to be taken to protect ballot secrecy even if the election takes place in private surroundings. "Unknown content" protects against illegal manipulation during casting the ballot as well as producing intermediate results.

The second criterion "unknown voter", derived from "indeterminable choice" demands unlinkability of the content of cast ballots and voters at any point in time. Until the end of the election period this is guaranteed by "unknown content" as no one must notice the content apart from the voter himself. But since it must be possible to count the election result, "unknown voter" is necessary at the latest from this point on. "Unknown voter" means, that no one may relate the content of the voting decision to the stored personal data of voters. Moreover it must be impossible for voters to prove their voting decision to anybody. Furthermore voters must be protected and prevented from generating evidence about their voting decision accidentally.

In the context of paper based elections a link between voting decision and voters is generally impossible because the ballot is thrown into the ballot box, which is permanently locked during election. Thus an attribution is not feasible after throwing the ballot into the box. Beyond that, the election documents have to be kept in safe custody and are destroyed after a predefined time period. Endless secrecy would, of course be the safest solution. It remains questionable, however, if such an endless secrecy can be guaranteed in the context of online voting. It is difficult to delete IT data completely and furthermore the connection between ballot and voter cannot be cut as easy as in paper based elections. Also, cutting the connection between voters and their ballots permanently at an early stage may rule out technical concepts for the voter to verify the correct processing of his ballot afterwards. "Unknown voter" is a concretisation of ballot secrecy and thus provides protection of the free and equal ballot (Morlok, 2006). The protective function referring to the equal ballot ends when the election is finished (Richter, 2012). To guarantee free elections, coercion based on the knowledge of the voting decision must be impossible at the current election as well as at future elections. Therefore, "unknown voter" should be guaranteed at least as long as voters live. Consequently it would be possible to keep the connection between the voter and his ballot for controlling the election. To avoid third persons from revealing this connection, an anonymisation, which would reliably resist attacks within the time period of a human life, would be a satisfying implementation from the legal viewpoint.

"Unknown content" and "unknown voter" have been presented as concepts, applicable at different points in time, "unknown content" before, "unknown voter" after the voting phase. This concept follows the approach, that "unknown content" and "unknown voter" must never be broken at the same time. However, for "unknown voter" to be sound after the voting phase, supposedly, measures must be taken long before this point in time (see also data minimisation below).

The third legal criterion derived from the requirement "indeterminable choice" is "data minimisation". The principle of data minimisation is laid down in § 3a of the German Data Protection Act (BDSG). It was created in the "Census" decision of the Federal Constitutional Court (BVerfGE, 1983). No IT system shall collect and process more personal data than necessary for its designated purpose. Because it is difficult to control personal data once they are collected and processed by modern IT systems, data minimisation often is the only way to protect the right to informational self-determination at all (Roßnagel, 2011). It is certainly the safest way, because data that are not available cannot be misused. The principle of data minimisation is realized by a technical and organizational configuration of data processing equipment that uses as few personal data as possible (Roßnagel, 2011). In our context, data minimisation strengthens ballot secrecy and the legal requirement of "indeterminable choice", because the less personal data are collected in the context of an election, the more difficult it becomes to link ballots to voters. Consequently, data minimisation is tightly linked to the criterion "unknown voter" and an important aspect of protecting ballot secrecy.

Next, we cross over from KORA to CC by transferring the legal criteria ("unknown content", "unknown voter" and "data minimisation") into Common Criteria Assets. By using the Common Criteria for carrying out a security analysis, only asset-related requirements are derived. Following, for each criterion a range of potential threats (T) and assumptions (A) are formulated. Then, starting from the identified threats a set of objectives (O) protecting the assets from these threats is listed. Similarly, objectives for the environment (OE) are listed. They should be able to enforce the identified assumptions. In the last step, the objectives (O) are formulated as SFRs to achieve a standardised description of requirements. The set of SFR is the first result of the proof of concept (see Figure 1: "Result 1") and could be used as a basis for the formulation of technical design goals (KORA step 3). In contrast, the identified OE are aligned with catalogue S2 (Organization) of the IT-Grundschutz. A set of suitable requirements on safeguards is the second result of the proof of concept (see Figure 2: "Result 2"). This set can be used as a basis for the formulation of organisation-related technical design proposals (KORA step 4).

Threat Analysis and Derivation of Assumptions: Unknown Content

In the context of online elections of private associations, the criterion "unknown content" is exposed to a variety of threats. The following threats have been derived by the use of attack trees.

- **T.FakeSW:** An attacker is able to disseminate manipulated client-side voting software in order to spy out the voter's submissions.
- **T.InsecurePlatform:** An attacker runs malware on the vote-casting device, which reads the vote in order to compromise the secrecy of the vote.
- **T.ProofVote:** A malicious voter is able to use information sent to/ displayed on/sent from his vote casting device to construct a proof of his vote.
- **T.SpyOutScreen:** A third person is observing the voters' screen while the voter is casting his vote.
- **T.SpyOutMsg:** An attacker is able to spy out the network communication e.g. to read cast votes.
- **T.FakeServer:** An attacker is able to imitate the voting server. By doing this, all voting related communication is redirected to this fake server.
- **T.TamperServer:** An attacker gets access to the voting server and uses stored information in order to compromise "unknown content".

Security Objectives and Assumptions are now derived from **T.SpyOutMsg** and **T.TamperServer,** which were selected as examples. Both threats are checked, whether they can be transferred to assumptions. This step will be attended legally, so that an additional feedback between IT security and law takes place at this interface, as described above. Such threats, which cannot be transferred to assumptions, are – according to the Common Criteria approach – formulated as security objectives.

In a first approach, **T.SpyOutMsg** was transferred to an assumption.

A.SecureCommunication: The voting system protects the confidentiality of the communication links between voting client and voting server.

This assumption is not legally acceptable, however, in our exemplary application to parliamentary elections and the highly valuable principle of ballot secrecy. It simply assumes protection of a confidential communication between voting client and voting server. It is not declared in this assumption, how protection of ballot secrecy might be enforced. An attacker would not have to spend great effort to refute the assumption. The communication between the voting client and the voting server can be attacked easily by affecting the WLAN router. Thus an attacker can get information about the voter and his ballot. Particular measures must be shown, which will protect ballot secrecy against the predetermined threat **T.SpyOutMsg**.

As it has been found that it is not acceptable to just assume, that the voting system will protect against **T.SpyOutMsg**, the threat must be managed according to the Common Criteria approach: A corresponding security objective must be formulated, which is able to protect the TOE against this threat.

O.SecureCommunication: The TOE uses secure communication paths to protect votes transmitted between TOE-client and TOE-server from reading.

Now, translation of informal security objectives to semi-formal SFR takes place: The security objective **O.SecureCommunication** can be explained by the following Common

Criteria components (ISO/IEC Part 3, 2009): FDP_UCT.1 combined with FTP_TRP.1 ensures that the vote is not transmitted in plaintext. By doing this, it is not possible to match between voter and vote. The component FPR_UNL.1 ensures, that the number and/or size of transmitted votes do not allow any conclusion on the content of the ballot (e.g. number of marks, invalidated vote). The used functional components – excluding the necessary dependent components – are listed below in Box 1.

T.TamperServer has been transferred to an assumption, also:

A.ServerSoftware: The voting servers' software prevents the intruder from accessing the server without having the corresponding access rights. The software is always up-to-date.

This assumption leads to a security objective for the environment (OE) of the system: OE.ServerSoftware.

ISO 27001/IT-Grundschutz provides several safeguards to implement the OE of regular updates of the voting server:

- **M 2.157:** Selection of adequate anti-virus software
- **M 2.158:** Reporting malware infection
- **M 2.174:** Secure operation of the server
- **M 2.273:** Regular installation of security critical software updates and patches.

Since A.Server.Software is covered as OE.Server.Software by ISO 27001/IT-Grundschutz, it needs not be reviewed legally.

Threat Analysis and Derivation of Assumptions: Unknown Voter

Because the criterion "unknown voter" needs to be observed from latest the stage of vote counting in our concept, all identified threats affect the voting server.

- **T.Access:** An intruder is capable of accessing the voting server(s) in a way that he might establish a link between the voter and her vote.
- **T.Manipulate:** An intruder might manipulate the voting server (at any point in time) in a way that he might establish a link between the voter and her vote (at any point in time).
- **T.Official:** An election official might access the data of the voting server in a way that allows him to establish the link between a voter and her vote.

Box 1. Common Criteria components used to implement the security objective O.SecureCommunication

FDP_UCT.1 Basic data exchange confidentiality
Hierarchical to: No other components.
Dependencies: FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or FDP_IFC.1
FDP_UCT.1.1 The TSF shall enforce the SFP for voting actions to transmit and receive votes.
FTP_TRP.1 Trusted path
Hierarchical to: No other components
Dependencies: No dependencies
FTP_TRP.1.1 The Server-TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of the voter and TOE-server and protection of the communicated vote from disclosure.
FTP_TRP.1.2 The Server-TSF shall permit a voter as remote user to initiate communication via the trusted path.
FTP_TRP.1.3 The Server-TSF shall require the use of the trusted path for the transmission of the vote.
FPR_UNL.1 Unlinkability
Hierarchical to: No other components
Dependencies: No dependencies
FPR_UNL.1.1 The TSF shall ensure that all users are unable to determine whether the operation "casting vote" is related to: the length of the transmitted vote corresponds to the number and/or position of selected nominations; invalidity of the vote.

- **T.ProofVoter:** A voter might label her vote in a way that allows the adversary accessing the (official) election data to establish a link between a voter and her vote.

Again, two threats will be used as examples.

T.Access was transferred to an assumption:

A.SecureServer: The voting server is secure in such a way that unauthorized persons do not have the possibility to access the system.

This assumption is not acceptable legally as it does not declare how unauthorized persons will be prevented from accessing the system. "Unknown voter" as part of the highly valuable ballot secrecy in parliamentary elections, has to be guaranteed by implementing concrete protective measures. Because the assumption **A.SecureServer** is not legally acceptable, an objective which is able to protect against **T.Access** has to be formulated:

O.AccessControl: The TOE uses access control mechanisms to protect the server against unauthorized accessing.

O.AccessControl can be explained directly by the following Common Criteria components: FDP_ACC, FDP_ACF, presented in Box 2. It is worth emphasizing that these and the following components have been taken from the Common Criteria catalogue without adaption. The reason for this is, that adapted SFRs have been formulated exemplarily for O.SecureCommunication yet. Another reason for this strategy is, that the following SFRs need a specific implementation. But that is not present.

T.Official has been transferred to an assumption, too:

A.Official: An official is allowed to access just a subset of stored data, so he is not able to establish a link between voter and vote.

The assumption includes a particular proposal how "unknown voter" can be protected. Exactly, this proposal can be effectively implemented by the ISO/IT-Grundschutz as outlined below. Hence, A.Official is an acceptable assumption as it is transformed into OE.Official.

ISO 27001/IT-Grundschutz provides several safeguards to implement OE.Official:

- **M 2.8:** Specification of access rights
- **M 2.63:** Setting up access rights

Threat Analysis and Derivation of Assumptions: Data Minimisation

The legal criterion "data minimisation" relates to the collection, usage and archiving of data

Box 2. Common Criteria components used to implement the security objective O.AccessControl:

FDP_ACC.1 Subset access control
Hierarchical to: No other components
Dependencies: FDP_ACF.1
FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*]on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].
FDP_ACF.1 Security attributes based access control
Hierarchical to: No other components
Dependencies: FDP_ACC.1, FMT_MSA.3
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
FDP_ACF.1.4 the TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

stored during the voting process. The threat analysis differentiates between the stage before, during and after counting:

- **T.Register:** An indiscreet registration system collects more personal data of a voter than is necessary for the proof of the right of the applicant to vote.
- **T.ComLog:** An indiscreet communication system which transfers the vote from the voting client to the voting server collects log data that links the vote-id to personal information about the voter.
- **T.CastLog:** An indiscreet voting server logs the communication process of casting a vote and collects data that links the vote-id to personal information about the voter, e.g. the IP address.
- **T.AuthToken:** A careless voting system that enforces the principle of "one person – one vote" with the help of an internal authentication token does not delete the token after the vote is successfully cast.
- **T.Archive:** An indiscreet voting system stores more personal data for a longer time than necessary (long-term proof of counting).
- **T.DataDeletion:** The data stored in the voting system could be restored by an attacker after deletion.

Again, two threats will be used as examples.

T.Register has been transferred to an assumption:

A.MinimalRegister: The registration system collects only such data that are sufficient to tell an authorised voter from an unauthorised voter, including the ability to identify voters already having cast their vote. An example for a measure to fulfil this requirement is the pseudonym of an eID card, combined with the regional information like "regional citizen". An example for disregarding this assumption is the collection of name, date of birth, residence and time of voting.

The principle of data minimisation does not allow collecting more data than necessary. Thus, collected data must be essential for the election system to function. In this case, the assumption specifies particular measures to minimize personal data within the system. The assumption leads to OE.MinimalRegister. For this OE, however, ISO 27001/IT-Grundschutz provides no safeguards for implementation. At this point, there is a need to extend the IT-Grundschutz catalogue M2 or apply an additional standard.

T.ComLog has been transferred to an assumption:

A.AnonymousTransfer: The communication system transferring the vote from voting client to voting server makes the sender anonymous. For example it is part of a Mix system, or it runs through a trustworthy third party unlinking the relationship between sender and recipient. Only encrypted votes are transferred through the communication system.

Just assuming these characteristics of the system is not acceptable, legally, as well as from IT-Security, however. Concrete measures protecting against T.ComLog must be established. Therefore, a security objective needs to be formulated, considering reliability.

O.NoComLog: The TOE must consist of a minimum of three components (Voting-client, Ballot-Box-Server, Registration Server) generating and storing different types of data. This system design should avoid the combination of data in such a way that at link between individual voters and their votes can't be established.

At this point, the translation of O.NoComLog into SFRs should take place. But for this O., the Common Criteria provides no components, which are matching for distributed data storage. At this point, there is – similar to A.MinimalRegister – a need to extend the Common Criteria catalogue of functional components. A further possibility to handle that problem could be under consideration of the organizational view.

SFRs as well as ISO 27001/IT-Grundschutz safeguards listed above can serve as an input for the formulation of technical design goals according to the KORA approach. This step is not part of this paper, however.

The traversed path through the approaches as shown above is only one possible way, to combine the approaches. Dependent on the intended aim, different paths are possible.

CONCLUSION AND DISCUSSION

Approaches for deriving IT security requirements exist in different research disciplines. In general, they are used only within the specialized disciplines. An integrated interdisciplinary use of different approaches is not common practice at all, although this would improve development and evaluation of IT products, as weaknesses of one approach could be compensated by another approach.

As we have shown, every approach described in this article has its advantages and disadvantages. The legal approach KORA is mainly focusing on deriving technical requirements and design proposals to provide the development of technology in accordance with legal provisions. Aspects of IT security are only considered insofar as they are necessary for this goal. A risk analysis is conducted in KORA, but can be enhanced by specialized IT security approaches. Common Criteria is first and foremost a security evaluation and certification approach, which is internationally accepted. The aim is to gain a selection of applicable security requirements for a specific product or a group of products. A legal consideration of assets, security objectives or acceptability of assumptions does not take place, however. ISO 27001/IT-Grundschutz provides standard security measures for IT products. Since it includes a number of organizational aspects, it has a rather general view of the IT product. A detailed evaluation of the product itself, as in CC, is not intended. ISO 27001/IT-Grundschutz does not legally consider assets or security measures, either.

Since we have identified interfaces for an integration of these approaches, we found out, that integration of the approaches leads to a benefit as drawbacks of each approach can be eliminated. Future work should especially analyse, if and how far our approach could be conducted in other application fields. A very cautious assumption on our part would be that an approach like KORA – and thus also the combination with CC and ISO 27001/ IT-Grundschutz – could be used (maybe with alterations) in other legal systems, also. This would mean that a combined approach of IT Security and law compatibility as shown in this article might be applicable internationally. Also different paths through the integration must be tested in the future. Furthermore, the integration could be specified with respect to the legal justification of Evaluation Assurance levels in CC and protection levels in ISO 27001/ IT-Grundschutz. It should also be pointed out that the integration requires legal and computer experts' interpretation. So it should be analysed, to what extend the methods' integration might be formalised further in order to reduce the need for interpretation and to make it more applicable on an operational level for.

REFERENCES

Beckers, K., Faßbender, S., Küster, J.-C., & Schmidt, H. (2012a). A pattern-based method for identifying and analyzing laws. In B. Regnell & D. Damian (Eds.), *Proceedings of the International Working Conference on Requirements Engineering: Foundation for Software Quality 2012:* Volume 7195 Lecture Notes in Computer Science (pp. 256-262). Wiesbaden, Germany: Springer.

Beckers, K., Faßbender, S., & Schmidt, H. (2012b). An integrated method for pattern-based elicitation of legal requirements applied to a cloud computing example. In *Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES 2012)* (pp. 463-472). IEEE Computer Society.

Bräunlich. K., Richter. P., Grimm, R., & Roßnagel, A. (2011). Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA – Anwendungsbeispiel: Wahlgeheimnis. *Datenschutz und Datensicherheit*, 129-135.

Breaux, T., & Antón, A. (2005a). Analyzing goal semantics for rights, permission, and obligations. In *Proceedings of the 13th IEEE International Conference on Requirements Engineering (RE `05).* (pp. 177-186). IEEE Computer Society.

Breaux, T., & Antón, A. (2005b). Deriving semantic models from privacy policies. In *POLICY '05 Proceedings of the Sixth IEEE International Workshop on Policies for Distributed Systems and Networks* (pp. 67-76). IEEE Computer Society.

Breaux, T., & Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. *Transactions on Software Engineering*, *34*(1), 5–20. doi:10.1109/TSE.2007.70746

Breaux, T., Vail, M., & Antón, A. (2008). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In B. Paech & C. Rolland (Eds.) *Requirements Engineering, 14th IEEE International Conference* (pp. 46-55). Wiesbaden, Germany: Springer.

Bundesamt für Sicherheit in der Informationstechnik. (2008a). *IT-Grundschutz Methodology, BSI Standard 100-2 (Version 2.0 Mai 2008)*. Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. (2008b). *Risk anaylsis based on IT-Grundschutz, BSI Standard 100-3 (Version 2008)*. Bundesamt für Sicherheit in der Informationstechnik.

CEM (2009). *Common methodology for information technology security evaluation (Version 3.1 Revision 3, 2009).*

German Federal Constitutional Court (BVerfGE, 1983). *Decisions of the German Federal Constitutional Court, 65*, 1 (43).

Hammer, V., Pordesch, U., & Roßnagel, A. (1993). *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten*. Berlin Heidelberg, Germany: Springer. doi:10.1007/978-3-642-78109-4

Hoffmann, A., Schulz, T., Hoffmann, H., Jandt, S., Roßnagel, A., & Leimeister, J. (2012). Towards the use of software requirement patterns for legal requirements. In Svensson et al. (Eds.) *2nd International Requirements Engineering Efficiency Workshop (REEW) at REFSQ 2012* (ICB-Research Report No. 52). (pp. 50-61). Essen, Germany: Universität Uni Duisburg-Essen.

Idecke-Lux, S. (2000). *Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz*. Baden-Baden, Germany: Nomos.

ISO/IEC. (2005). *ISO/IEC 27001: Information technology – Security techniques -- Specification for an Information Security Management System*. Geneva, Switzerland: ISO/IEC.

ISO/IEC. (2009). *ISO/IEC 15408: Common criteria for information technology security evaluation, Part 1 – 3 (Version 3.1, Revision 3)*. Geneva, Switzerland: ISO/IEC.

Laue, P. (2009). *Vorgangsbearbeitung in der öffentlichen Verwaltung*. Kassel, Germany: Kassel University Press.

Morlok, M. (2006). Art. 38 GG. In Dreier (Ed.), Grundgesetz-Kommentar. Tübingen, Germany: Mohr Siebeck.

Pordesch, U. (2003). *Die elektronische Form und das Präsentationsproblem*. Baden-Baden, Germany: Nomos.

Richter, P. (2012). *Wahlen im Internet rechtsgemäß gestalten*. Baden-Baden, Germany: Nomos. doi:10.5771/9783845243450

Roßnagel, A. (1997). Der Nachweis von Sicherheit im Anlagenrecht - Am Beispiel von deterministischen und probabilistischen Sicherheitsnachweisen im Atomrecht. *Die Öffentliche Verwaltung*, 801 – 810.

Roßnagel, A. (2008). Rechtswissenschaftliche Gestaltung von Informationstechnik. In H. Kortzfleisch, & O. Bohl (Eds.), *Wissen, Vernetzung, Virtualisierung* (pp. 381–390). Köln, Germany: Josef Eul Verlag.

Roßnagel, A. (2011). Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes? In M. Eifert, & W. Hoffmann-Riem (Eds.), *Innovation, Recht und öffentliche Kommunikation (Sonderdruck) – Innovation und Recht IV* (pp. 41–66). Duncker & Humboldt.

Roßnagel, A., & Neuser, U. (2006). Die rechtliche Festlegung von Risikogrenzwerten. *Zeitschrift für Umwelt- und Planungsrecht,* 125-131.

Scholz, P. (2003). *Datenschutz beim Interneteinkauf – Gefährdungen – Anforderungen – Gestaltungen*. Baden-Baden, Germany: Nomos.

Schwenke, M. (2006). *Individualisierung und Datenschutz– Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung*. Wiesbaden, Germany: Deutscher Universitäts-Verlag.

Stadler, T. (2006). *Mobiles Bezahlen – Die rechtsverträgliche Gestaltung mobiler Bezahlverfahren in Deutschland*. Baden-Baden, Germany: Nomos.

Daniela Simić-Draws is research assistant at the University of Koblenz-Landau at the research group IT Risk Management since 2011. First, she was involved in the project Formal Modeling of online voting with methods of computer science and legal since (ModIWA II). Currently she is giving lectures and is preparing her doctoral thesis. Her doctoral research is supervised by Prof. Dr. Rüdiger Grimm and focuses on the development of a security analysis based on business processes. Daniela Simić-Draws gained both her Bachelor's and a Master's Degree in Information Management from the University of Koblenz. In her Master's Thesis, she carried out a security analysis of a signature-based home banking technique.

Stephan Neumann has been a research assistant in the SecUSo group at the Department of Computer Science of Technische Universität Darmstadt, Germany since October 2011. He works on the project Formal Modeling of online voting with methods of computer science and legal science (ModIWa II). His doctoral research is supervised by Prof. Dr. Melanie Volkamer and focuses on theoretical and practical technical aspects of remote electronic voting schemes. He has been a reviewer for several journals and conferences. Stephan Neumann holds a Bachelor's and Master's degree in Computer Science from the University of Saarland, Germany, where he finished his Master's thesis on the integration of the cryptographic security analysis and the algebraic-logic security proof of PACE.

Anna Kahlert is research assistant at the University of Kassel within the Project Group Constitutionally Compatible Technology Design (provet). She is working for the project Formal Modeling of online voting with methods of computer science and legal science since 2011 and is preparing her doctoral thesis about the legal regulation of remote electronic voting. From 2009 until 2011 Anna Kahlert completed a legal traineeship at the Higher Regional Court in Frankfurt am Main, where she graduated the Second State Examination in Law. Before, she studied law at the University of Mannheim with focus on public commercial law, telecommunications- and media law and passed the First State Examination in Law in 2009.

Philipp Richter studied at the Faculty of Law of the Humboldt University in Berlin, where he also acquired both State Examinas and spent most of his legal clerkship. During his clerkship he took stages with two data protection agencies: Berlin and Toronto, Canada. After his second State Examina in May 2009, he came to University of Kassel and joined the "Project Group Constitution Compatible Technology Design" (provet), headed by Prof. Dr. Alexander Roßnagel. He worked for two years on a research project concerning internet voting and also presented his doctoral thesis on this topic, which he defended in March 2012. He then proceeded to work on another research project concerning privacy on the internet until beginning of 2013. Currently he is teaching, doing legal research and publishing in the areas of electronic voting, data protection and evolving information technologies.

Rüdiger Grimm is Professor and head of the Research Group IT Risk Management in the Department of Information Systems Research at the University of Koblenz-Landau. He teaches and conducts research on foundations and applications of IT security.

Melanie Volkamer has been an Assistant Professor at the Department of Computer Science of Technische Universität Darmstadt, Germany, since February 2012. She heads the research group "SecUSo - Security, Usability and Society". Before this appointment, she was a postdoctoral researcher in the group of Prof. Buchmann at the Technische Universität Darmstadt. She has *been an advisory board member of many e-voting projects and initiatives. In particular, she acted as an OSCE election observer at the first parliamentary remote electronic election in Estonia in 2007. Furthermore, she was invited by the German Federal Constitutional Court as a technical expert for e-voting in 2008. She has presented her research at numerous conferences and to many organizations like the Council of Europe. She obtained her PhD from the University of Koblenz in October 2008, and her Diploma from the University of Saarland in 2004.*

Alexander Roßnagel holds the chair for public law with the focus on law regarding technology and environmental protection at Kassel University. Among other functions he is heading the Project Group for Constitutionally Compatible Technology Design (provet), where interdisciplinary research projects regarding legal questions of communication and information technologies are carried out. He is Director among others of the Interdisciplinary Research Center for Information System Design (ITeG) at Kassel University, and Contributing Professor at the Center for Advanced Security Research Darmstadt (CASED).