EPJ Web of Conferences 77, 00001 (2014)
DOI: 10.1051/epjconf/20147700001

IT Security Standards and Legal Metrology – Transfer and Validation

F. Thiel [a], V. Hartmann, U. Grottker and D. Richter

Physikalisch-Technische Bundesanstalt (PTB), Abbe Str. 2-12, 10587 Berlin, Germany

Abstract: Legal Metrology's requirements can be transferred into the IT security domain applying a generic set of standardized rules provided by the Common Criteria (ISO/IEC 15408). We will outline the transfer and cross validation of such an approach. As an example serves the integration of Legal Metrology's requirements into a recently developed Common Criteria based Protection Profile for a Smart Meter Gateway designed under the leadership of the Germany's Federal Office for Information Security. The requirements on utility meters laid down in the Measuring Instruments Directive (MID) are incorporated. A verification approach to check for meeting Legal Metrology's requirements by their interpretation through Common Criteria's generic requirements is also presented.

1 Introduction

To check for conformity of measurement instruments with the requirements of the Measuring Instruments Directive 2004/22/CE (MID) [1], several helpful Guidelines have been developed [2], [3]. Currently the tailoring of essential requirements to all kinds of IT components including validation recommendations predominate, making the guides rich in detail and therefore demand a sound expert knowledge when performing individual tests.

Thus it is proposed that legal metrology shall increasingly rely on IT components that are in accordance with widely accepted technical rules and standards. This applies in particular for all-purpose components that are not exclusively used in measuring systems such as, e.g., data transmission components or operating systems. Consequentially, there is a need for procedures to reasonably handle this new approach [3].

Legal Metrology (LM) and IT Security are different domains with partly quite an unequal understanding of how the "security" aspect is rendered, e.g. the protection of sensitive data and the defined roles (s. Fig. 1).
In this contribution we will outline the transfer and cross validation of Legal Metrology's requirements for utility meters into the IT security domain, applying a generic set of rules provided by the Common Criteria (CC, ISO/IEC 15408), i.e. their integration into a recently developed *Protection Profile* for a Smart Meter Gateway designed under the leadership of the Germany's Federal Office for Information Security [7, 8].

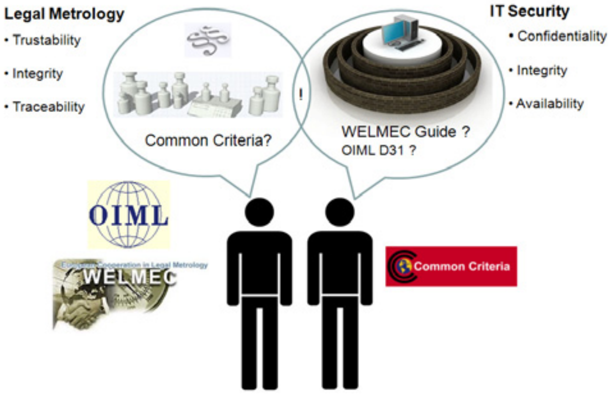

Fig. 1: Legal Metrology and IT Security: Different Domains with different understanding of and requirements for data protection.

To this end a verification method to check for meeting Legal Metrology's requirements by their interpretation through CC's generic requirements was developed and applied. As a result, the non-congruent parts were extracted. They and only they further have to be covered by metrology-specific regulations.

2 The Common Criteria Approach

In the last decade, an international standard for IT security, the so-called *Common Criteria for Information Technology Security Evaluation* (CC, ISO/IEC 15408) [8] has been developed. It provides guidance for security evaluation by providing generic requirements for major security functionalities of IT products and assurance measures to be applied to these functionalities. The

[a] Corresponding author: florian.thiel@ptb.de

Article available at http://www.epj-conferences.org or http://dx.doi.org/10.1051/epjconf/20147700001

means to adapt the generic requirements to particular application areas are the so-called *Protection Profiles*, which are pre-designed in the CC standard.
While the protection profile is a means to express the security requirements in a comparable way, another instrument of the CC standard, the so-called *Security Target*, is a means to express the security function implemented in a particular product. By matching security targets with protection profiles, the evaluation of compliance with requirements is supported.

The big advantage of the CC approach is the comparability of evaluation results independently achieved by security evaluation bodies, besides the reference to the latest state-of-the-art of IT security. An aspect of special importance is that CC enforces the definition and clear description of assumptions and environmental conditions, under which a protection profile and a security target have been set up. Comparability is obviously only given under same assumptions and conditions.
The approach is applicable to products that may be implemented in hardware, firmware, application software or any combination of them. The evaluation process establishes a level of confidence that the security functionalities of IT products under evaluation meet the requirements. The CC is therefore useful as a guide for the development and for the evaluation of IT products, even for their procurement. The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a broad variety of IT products.
Though the approach of CC is very valuable and the only systematic and comprehensive one available, it is not a scheme that could simply be applied by the developer of a system *quasi* as an add-on to the normal specification. The levels of definition of security functions and protection profiles differ considerably from those a programmer needs. Especially for already existing complex systems like an operating system, it is necessary to interpret the security means implemented with regard to the security functions required by the protection profile.

Several evaluations of operating systems have been performed (Windows 2000 to Windows Vista, SuSE Linux, Red Hat Linux [9]) by the National Information Assurance Partnership (NIAP) [10]. Because of the complexity of the evaluation object, this was only possible by a cooperation of the evaluator with the manufacturer of the operating system.

To date, a successful application of CC-based methods in the legal metrology area is not known. This is, on the one hand, not fully explainable since the IT related requirements, as outlined above, are well structured in guides like [2] and [3] and, therefore, well prepared for a revision in terms of a protection profile. On the other hand, it is comprehensible since the way of thinking and the terminology used in metrology and IT security are quite different. It will be a challenge in the near future to bring together these two worlds for the significant benefit of the IT security of measuring instruments.

Basically, the developing process of a protection profile starts with an analysis of the threats the target of evaluation is exposed to (s. Fig. 2).

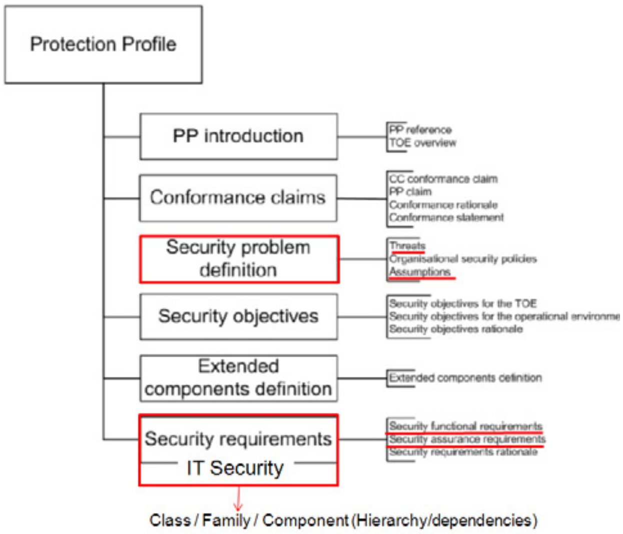
Protection Profile
PP introduction
PP reference
TOE overview
Conformance claims
CC conformance claim
PP claim
Conformance rationale
Conformance statement
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environme
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
IT Security
Security functional requirements
Security assurance requirements
Security requirements rationale
Class / Family / Component (Hierarchy/dependencies)

Fig. 2: Protection Profile contents according to the Standard ISO/IEC 15408 (Common Criteria) [8].

This comprises the identification of what is threatened as well as who or what is doing the threatening. Concerning a measuring instrument subject to legal control, matters that are threatened can be summarized as follows:

(A) the falsification of measurement values or the assignment of a measurement value to a wrong measurement.
(B) wrong measurement functions or parameters of the measuring instrument.
(C) inappropriate or missing protection means of the measuring instrument, implying that further threats such as A) or B) are facilitated.

In a standard analysis who or what is the origin of a threat, roles are defined that are performed by persons. It is presumed that some roles intend to perform threats (A) to (C). For some roles this is not assumed (e.g. an administrator of any IT installation), who enjoy more confidence. A protection profile therefore does not require the same protection means for each role.

In countries where metrology is legally controlled, the roles and threats to be assumed are defined by law, to some extent. In general, only the surveillance officer and no other person has privileges. When a measuring instrument is in use, it has to be protected against threats by anyone else.

3 Protection Profile for a Smart Meter Gateway

Recent activities in Germany to implement a commodity network - a Smart Grid for electricity, gas, water and heat/cold, which aims to ensure a more sustainable, economic and secure supply of energy - are based on the implementation of utility meters with augmented functionality, the Smart Meter System. Such utility meters with augmented functionality are demanded on the European level by the Directive 2009/72/EC [11] and nationally by the Energy Industry Act (EnWG) [12].

To secure the infrastructure against several kinds of threats of physical and/or logical occurrence, and to ensure privacy of personalized data, a Gateway with specific properties is demanded and will be implemented between wide area and local networks (s. Fig. 3).

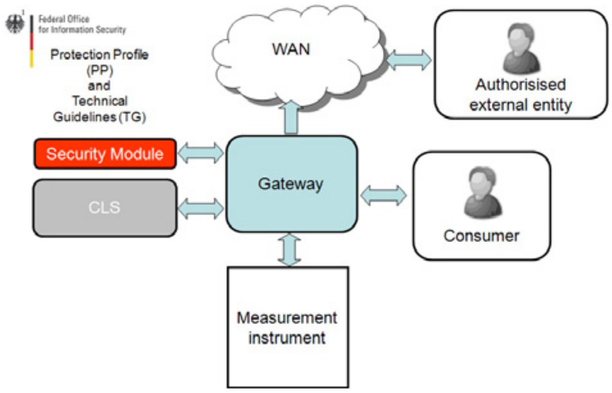
Federal Office for Information Security
Protection Profile (PP) and Technical Guidelines (TG)
Security Module
CLS
WAN
Gateway
Authorised external entity
Consumer
Measurement instrument

Fig. 3: The Gateway of a Smart Metering System in it’s environnement.

This Gateway has to meet both, the requirements of a recently developed Protection Profile (PP) [13] designed under the leadership of the Germany’s Federal Office for Information Security (BSI), applying the generic set of rules provided by the Common Criteria (CC) [8], and the legal regulations for measurement devices with their own guidelines to treat software and IT components in measurement systems, the OIML D-31, WELMEC Guide 7.2 and national Legal Metrology’s requirements the PTB-A50.7 [2], [3], [4], [5].

Furthermore a Technical Guideline (TG) also designed under the leadership of the Germany’s Federal Office for Information Security (BSI) defines interoperability properties and test requirements [14].

In such a multidisciplinary approach, the basis for mutual comprehension is a similar “language”.

Therefore, we propose that Legal Metrology’s requirements, laid down, e.g. by OIML, WELMEC or nationally should be transferred into an international standard.

To this end, a transfer of national Legal Metrology’s requirements for utility meters, the PTB requirements PTB-A50.7 [4], into the IT security domain, i.e. their integration into the PP, needs to be performed by utilizing the evaluation toolbox provided by the latter domain, the CC’s generic requirements.

A reversed approach, the derivation of modified configuration rules for the validation of standard Operating Systems in legal Metrology ([6], [7]) was already developed and successfully applied by our group by merging of edited configuration rules, extracted from a CC-based security evaluation, with software requirements for Legal Metrology (s. Fig. 4).

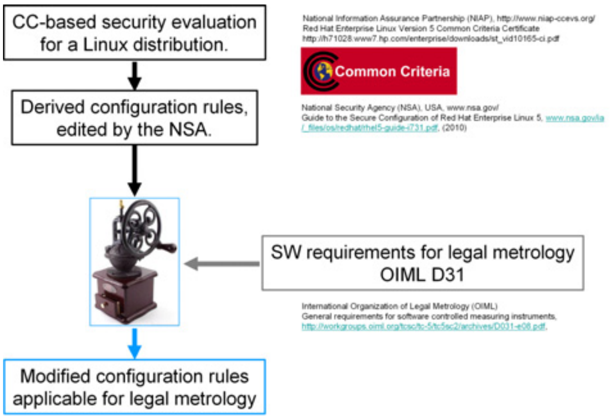
CC-based security evaluation for a Linux distribution.
National Information Assurance Partnership (NIAP), http://www.niap-ccevs.org/
Red Hat Enterprise Linux Version 5 Common Criteria Certificate
http://h71028.www7.hp.com/enterprise/downloads/st_vid10165-ci.pdf
Common Criteria
Derived configuration rules, edited by the NSA.
National Security Agency (NSA), USA, www.nsa.gov/
Guide to the Secure Configuration of Red Hat Enterprise Linux 5, www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf, (2010)
SW requirements for legal metrology OIML D31
International Organization of Legal Metrology (OIML)
General requirements for software controlled measuring instruments,
http://workgroups.oiml.org/tcsc/tc-5/tc5sc2/archives/D031-e08.pdf.
Modified configuration rules applicable for legal metrology

Fig. 4: Synergetic approach to merge the CC-based security evaluation of an Operating System with software requirements for legal metrology (OIML D31) [7].

With these experiences we aimed to develop and apply a verification method to check for congruency of national legal regulations by their interpretation through IT security experts using CC’s generic requirements.

Before going into the description of the methodology, let’s spend a view words about the national metrological requirements laid down in the document PTB A50-7.

4 National metrological requirements which render 2004/22/EC.

The national metrological requirements, laid down in the document PTB A50-7 and define the requirements on electronic and software steered measurement instruments and auxiliary devices for electricity, gas, water and heat (utility meters, i.e. commodity meters). It renders a realization of the general requirements laid down in the MID and is compatible to WELMEC Guide (7.2) “Software” [3].

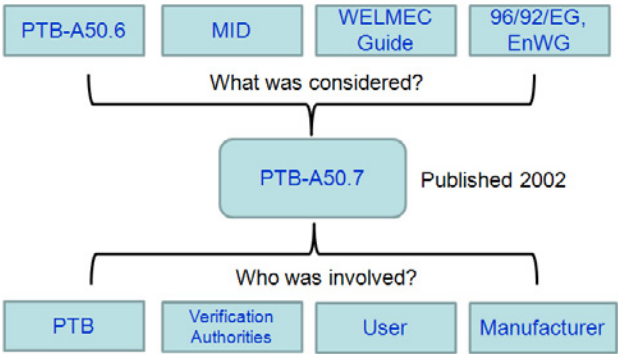

Fig. 5:.Genesis of the national requirements document PTB-A50.7.

It can be assumed as a form of standardization document, a regulative construction and testing directive. See figure 5 for a pictorial description of what was considered and who was involved in the genesis of the PTB-A50.7.

It is the aim of our approach to check for the coverage of the security requirements of PTB-A50.7 by the PP.

5 VALIDATION METHODOLOGY

We developed and applied a verification method to check for the coverage, i.e. congruency, of national legal regulations by their interpretation through IT security experts using CC's generic requirements.
In a first step we, i.e. Metrologists, identified distinguishable classes of elements within the PTB A50.7 (s. Fig. 6).

Class 1: Security elements.
Criterion: Security relevant elements, which should be covered by the PP.

Class2: Security elements, which should be covered by Technical Guideline
Criterion: Definition of Interoperability, properties and test requirements

Class3: Elements of PTB- A50.8 (a special successor of PTB-A50.7 for smart meter gateways)
Criterion: Metrological relevant elements which are not covered by aforementioned security-related classes 1 and 2.

Class 4: Obsolete elements.
Criterion: e.g. out-dated technology, etc.

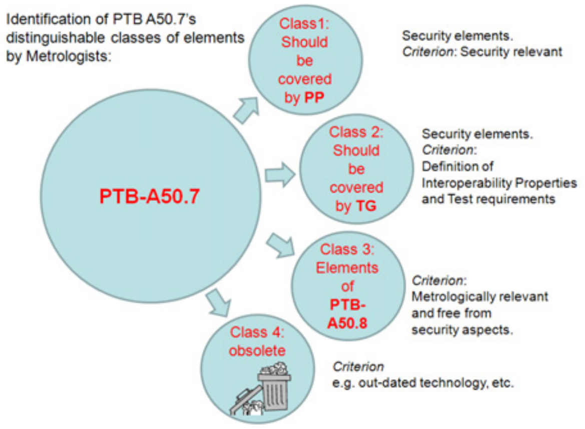
Identification of PTB A50.7's distinguishable classes of elements by Metrologists:
PTB-A50.7
Class1: Should be covered by PP
Security elements.
Criterion: Security relevant
Class 2: Should be covered by TG
Security elements.
Criterion: Definition of Interoperability Properties and Test requirements
Class 3: Elements of PTB-A50.8
Criterion: Metrologically relevant and free from security aspects.
Class 4: obsolete
Criterion e.g. out-dated technology, etc.

Fig. 6: Methodology: Differentiation of PTB A50.7 requirements into Classes

The subsequent procedure can be summarized as follows (s. Fig. 7):

- Find the requirements in the national requirements PTB-A 50.7 to be part of the PP/TG.
- Identify the chosen adapted generic requirements from the CC with all dependencies and hierarchies to cover the PTB-A 50.7's requirements.
- Compare the meaning of the CC generic requirements with the meaning of legal metrology's requirements.
- Identify conspicuous elements (match and mismatch)!

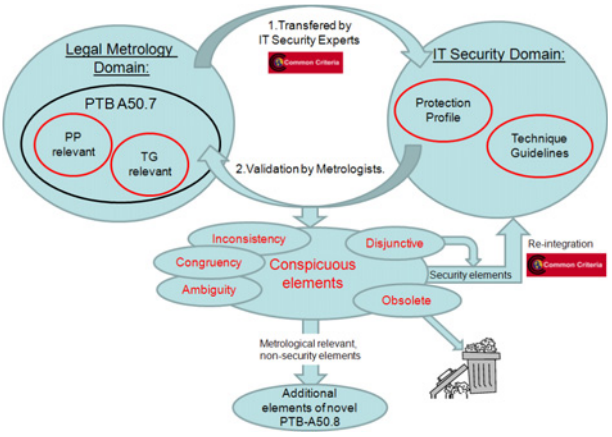

Fig. 7: Congruency Analysis Scheme

In such an analysis the following conspicuous elements are expected:

- Security relevant elements which should be reintegrated using CC.
- Metrologically relevant, non-security elements which are part of additional requirements, to be formulated in a new "regulative container", the PTB-A50.8

Expected Cases of conspicuous elements:

1. No coverage (Disjunctive)
2. Obsolete
3. Contrary (Inconsistent)
4. Ambiguities (non- bijectiv)
5. Congruency (under-, over-coverage)

Disjunctive elements, i.e. requirements not, or only partly congruent to the CC, are distinguished into security and non-security relevant items. These are either reintegrated into the PP or should be considered as part of the Technical Guidelines (TG), which define the vicinity of the Gateway and adequate testing measures, whereas the latter will be part of a new regulative "container", the PTB-A50.8 (s. Fig. 7).

6 GENERAL FINDINGS

First of all it can be stated that we found no additional obsolete elements. We did not find further completely disjunctive elements, which mean that the reintegration process could be omitted.

Since the legal metrology regulations (LMR) are rich in details, they are inherently much more tailored to metrology. Therefore the chosen CC equivalent is often much too general which could lead to **ambiguities**!

On the other hand the PP is inherently much stricter than the LMR regarding security aspects.
This may lead to:
a.) Over-coverage: PP requirements are stronger than LMR, or
b.) Under-coverage: PP restricts the LMR.

Case a.) has been detected with our method whereas no indication for case b.) has been detected.

Further **inconsistencies** *between* PP and LMR were detected, and we found **redundancies** in the LMR where different parts reference to the same part of the annexes.

<u>Therefore we can conclude that</u>

⇒ A re-integration of conspicuous elements is not necessary.
⇒ Bijectivity is not provided by the transformation due to possible **ambiguities**.

Hence, it follows that PTB-A50.7 and therefore the European Directive, the MID, cannot be reconstructed from the PP *in toto*.

Since ambiguities are the most severe problems arising in such a transfer approach, we consider it helpful to give an example:

The national requirement, which renders the requirements of the European Directive 2004/22/EC, the MID, demands:

All billing relevant measured values and parameters have to be visualisable <u>every time</u> without <u>special efforts</u>.

The chosen fix Common Criteria functions in the Protection Profile (FAU_SAR / CON.1.1 and FAU_SAR / CON.1.2) demand:

- *The TSF (target security function) shall provide only authorized consumers […] with <u>the capability to read</u> […] from the consumer audit records.*

- *The TSF shall provide the audit records in a manner <u>suitable for the user</u> to interpret the information.*

The Directive 2004/22/EC formulates very concrete the demands on time and effort (*every time*, *without special effort*). Whereas, in comparison, the chosen Common Criteria functions are very general, since <*every time*> is rendered by <*capability to read*>, and <*without special effort*> by <*suitable for the user*>, which makes the arising ambiguity challenge most obvious.

This result motivates an additional declaration to the PP, i.e., to preserve all general requirements of Legal Metrology for the development of Gateways based on different technologies and/or manufacturers.

Therefore we propose an supplement to the Technical Guideline or, which is more applicable, PTB-A50.8 requirements for metrological **and** metrologically refined security relevant elements.

7 CONCLUSIONS

Disjunctive elements, i.e. requirements not, or only partly congruent to the Common Criteria, are distinguished into security and non-security relevant items. These are either reintegrated into the Protection Profile or should be considered as part of the Technical Guidelines, which define the vicinity of the Gateway and adequate testing measures, whereas the latter will be part of a new regulative "container", the PTB-A50.8, the special successor of PTB-A50.7 for smart meter gateways.

Although the results are restricted to this particular scenario, this approach principally proves the feasibility of a reliable transfer of specific European and national legal requirements into an international evaluation methodology scheme for IT security. The Common Criteria proved also to be an international "language" to describe Legal Metrology's specific national security aspects allowing their objective international comparison.

This example underlines the necessity and usefulness of using well established, internationally excepted standards and rules for Legal Metrology. It further indicates in what direction the future development of IT related requirements should be brought forward in order to manage the more and more sophisticated IT components and simultaneously not to overburden authorities of Legal Metrology.

8 ACKNOWLEDGEMENT

The authors are grateful to the colleagues of the department 8.5 *Metrological Information Technology* of Physikalisch-Technische Bundesanstalt for helpful discussion and critical remarks.

References

[1] Directive 2004/22/EC of the European Parliament and of the Council on Measuring Instruments ("The Measuring Instruments Directive"), (2004).

[2] Organisation Internationale de Métrologie Légale (OIML), *General requirements for software controlled measuring instruments*, OIML D-31, (2008)

[3] WELMEC Guide 7.2: Software Guide (Measuring Instruments Directive 2004/22/EC), available for download at www.welmec.org.

[4] PTB-Anforderungen an elektronische und software- gesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, PTB-A 50.7, http://www.ptb.de/de/org/q/q3/q31/ptb-a/pa50-7.pdf, (2002)

[5] F. Thiel, U. Grottker, D. Richter, *Exploitation of Internationally accepted IT Security standards for Legal Metrology*, Milestones in Metrology, 4th Edition, 9-11 May, Venice, Italy, (2012)

[6] F. Thiel, U. Grottker, D. Richter, *The Challenge for Legal Metrology of Operating Systems Embedded in Measuring Instruments*, OIML BULLETIN, 52 (LII), pp. 7-16, ISSN 0473-2812, (2011)

[7] F. Thiel, D. Richter and U. Grottker, *A Testing Scheme for Operating Systems in Measurement Systems for Legal Metrology*, Actes des Conférences du Congrès International de Métrologie, Paris, France, Collège Français de Métrologie (CFM), (2011)

[8] Common Criteria for Information Technology, Version 3.1, Revision 3, (2009), http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

[9] NIAP Validated Products List, http://www.niap-ccevs.org/vpl/

[10] National Information Assurance Partnership (NIAP), http://www.niap-ccevs.org/

[11] Internal Market in Electricity Directive 2009/72/EC , (2009)

[12] Energy Industry Act (EnWG), Federal Ministry of Economics and Energy, (2013)

[13] Federal Office for Information Security (BSI), *Protection Profile for the Gateway of a Smart Metering System -V 1.02.00* final release- , (2013)

[14] Federal Office for Information Security (BSI), *BSI TR-03109 SMART ENERGY*, (2013)