Proceedings of the 2013 Federated Conference on
Computer Science and Information Systems pp. 775–780

How to Develop a Biometric System with Claimed Assurance

Andrzej Bialas
Institute of Innovative Technologies EMAG,
ul. Leopolda 31, 40-189 Katowice, Poland
Email: a.bialas@emag.pl

***Abstract*—The article concerns the process of developing biometric devices with a view to submit them for certification in compliance with ISO/IEC 15408 Common Criteria. The author points at the assurance paradigm which shows that the source of assurance is a rigorous process of the product development along with methodical and independent evaluation in an accredited laboratory. The state of the art of certified biometric devices was discussed. There was some focus put on the issue of insufficient support that the developers get in this respect. Basic processes related to the Common Criteria methodology were described (IT security development, IT product development, IT product evaluation). These processes were illustrated by the elements of security specifications of certified biometric devices. The author proposes that development patterns can be used to prepare evidence material, while specialized devices supporting development processes – to deal with basic difficulties encountered by the developers of biometric devices.**

I. Introduction

TODAY'S IT applications, especially those used in the large businesses, banking, e-government and e-health sectors require dependable identification and authentication. One of the possible group of solutions used in these applications is provided by biometrics.

Biometric authentication concerns the automatic identification of humans by their intrinsic physiological characteristics (finger images, hand/facial geometry, vascular patterns, iris, retina, etc.) or behavioural characteristics (hand writing, keystroke dynamics, etc.).

Biometrics can be used for:

- identification of a person's identity; the captured biometric sample is compared with enrolled templates contained in the database to find the matching one;
- verification of a person's identity; the captured biometric sample of the person claiming the given identity is compared with the enrolled template associated with the claimed identity and stored in the database.

Both processes, identification and verification, should be supported by the enrolment process, responsible for capturing biometric samples and storing them in a secure way. Providing mechanisms to associate an identity with a person, biometric devices are often used when quick, secure and positive authentication is needed.

Biometric devices implement the best matching technologies for the given application domains. These devices encompass hardware and software parts. The implementation of these parts is important, as it is always critical for the entire security system in which these devices work.

IT users require trustworthy biometric devices because these devices usually secure their critical applications in high risk environments. The Common Criteria (CC) [1] methodology can be used to develop trustworthy biometric devices.

The developers of biometric devices should be familiar with the Common Criteria methodology because they should be able to perform different CC-related security analyses and tests in order to prepare biometric IT products for evaluation, to elaborate evaluation evidences and to assist the evaluation process. Most of IT developers, not only biometric technology developers, have difficulties to successfully perform these tasks. For this reason some Common Criteria supporting documents and guidances (e.g. [2]) have been elaborated and consulting services are offered. One of the Common Criteria-based methodologies supporting the IT security developers in their works will be presented in this paper. It was elaborated during the CCMODE (Common Criteria compliant, Modular, Open IT security Development Environment) R&D project [3], co-financed by the EU within the European Fund of Regional Development. The objective of this project was to elaborate a CC-compliant methodology and tools to develop and manage development environments of IT security-enhanced products and systems for the purposes of their future certification. The CCMODE project resulted in the following products: knowledge, patterns (including documentation, procedures, evidences, specification means, etc.), methodology and tools which can be used by different organizations to create and manage IT development environments [4]–[5]. The contribution of this paper is to provide developers of biometric devices with the new patterns-based and software-supported assurance methodology to make this development process easier. The paper shows how the general purpose patterns and tools elaborated in the CCMODE project can be adopted for biometric devices. The paper also discusses the state of the art of the certified biometric devices pointing out sources of knowledge useful for developers.

The paper presents a short primer for the CC methodology, a range of the CC-related support offered for biometric technology developers, a review of the development process of biometric devices in the CCMODE development environment, and conclusions.

978-1-4673-4471-5/$25.00

II. Common Criteria methodology – a primer

The ISO/IEC 15408 standard Common Criteria [1] assumes that the reliability of security measures depends on how much accuracy and rigour is put into the development, testing, verification, documenting etc. of IT products. The more rigorous is this process, the more precise are the used good engineering practices, the better is the organization of the development /production /maintenance environment – the more reliable, trustworthy is the IT product. In the nomenclature of the standard, the commonly understood reliability was replaced by a more precise term – assurance. The assurance can be measured by means of Evaluation Assurance Levels (EAL) in the range from EAL1 (minimal value) to EAL7 (maximal value). The applied degree of rigour affects the cost of the product development, manufacturing and maintenance, therefore when the EAL is declared, the developer has to compromise between the product costs and the assurance level. In practice, among already evaluated 1,200 IT products, the biggest number are those on levels EAL3 and EAL4 [6]. An IT product in the CC nomenclature is called TOE – Target of Evaluation.

The Common Criteria methodology comprises three basic processes:

- IT security development based on different types of security analyses; a special document is worked out, called Security Target (ST), which is a set of security requirements – functional requirements describing how security measures should work and assurance requirements describing how reliable the developed products are;
- TOE development, including its documentation; this documentation, being an extension to the above mentioned ST, is evidence material prepared for the sake of the third process – security evaluation;
- IT security evaluation, carried out in an independent, accredited laboratory [6].

The standard has a wide application range as it is difficult to find an IT product without any security measures of its functions. Rigorous regulations related to the product development, along with independent evaluation, are the source of assurance for such a product.

Biometric products are security-related products requiring assurance.

III. Common Criteria Support for the Biometric Devices Developers

The developers of biometric devices can use the BSI guide [2] which is about the preparation of evidence material. The guide has a general character (concerns any IT products) and does not give any patterns to prepare the material. Therefore the developers have to use consulting services in this respect. There are few software tools which support the development of evidence material. One of them was described in [7]. The tool allows to generate a Security Target pattern which is one of over a dozen documents needed in the whole process. Some valuable practical hints about the evidence preparation and the certification itself are available in [8].

The developers of biometric devices can get some assistance from the so called Protection Profiles. These are evaluated sets of requirements for a certain class of IT products. For biometric devices only two Protection Profiles have been developed so far.

The [9] profile presents a biometric verification system in terms of [1] and defines functional and assurance requirements for such a system. Two other biometric systems, i.e. enrollment- and identification systems, are not considered in this profile. The profile focuses on the stand-alone version of the biometric device. Moreover, it does not discuss the biometric modality and related hardware. For this reason, the [9] focuses only on a software solution. This PP has EAL2 claimed. Testing is not considered (thresholds). This profile is of basic significance for the developers of biometric devices. The second PP [10] provides fingerprint spoof detection.

Up until now only three biometric devices have successfully passed the certification process [6]. The Security Target [11] presents the functionality of the Palm Secure biometric verification system, based on the structure of the veins in the palm as a unique characteristic of a human body. The Security Target [12] specifies a system that provides fingerprint spoof detection as part of a biometric system for fingerprint recognition. The ST [13] (EAL2+) specifies a distributed (server-based) authentication system based on biometric data.

IV. Development Process of Biometric Devices in the CCMODE Development Environment

In order to obtain a certificate for an IT product, including a biometric product, it is necessary to carry out the three basic processes mentioned in section 2.

4.1 IT security development process

This process encompasses activities aiming at the elaboration of the TOE security functions (TSF) meeting security functional requirements (SFR), to be implemented at the claimed EAL during the next process – TOE development. The IT security development process includes (key parts):

1. Preparation of the ST introduction.

The developer should assign the TOE type (i.e. biometric device) and provide a concise but precise description of the TOE, which can be an entire biometric device or its part only. The TOE can encompass software, hardware or both. It should be described in the ST introduction what the TOE is and what the TOE operational environment is, including the required non-TOE hardware/software/firmware in this environment. In the TOE description physical and logical scope of the TOE should be specified. The ST introduction should present the TOE usage and its major security features.

2. Conformance claims.

They specify conformance with the used CC standard version (e.g. v.3.1), with protection profiles (if applied) and with assurance packages expressing the EAL level.

3. Security problem definition (SPD).

The security problem can be expressed as the assets protection against threats (this method is recommended to apply

more reliable technical measures) or as OSP (Organizational Security Policy) rules to be fulfilled to avoid incidents (organizational measures are less appreciated than the technical ones). A good practice is to start with the identification of the TOE protected assets (they can be inside or outside the biometric TOE) and external entities interacting with the TOE (sometimes called subjects). The biometric TOE protects usually the users' assets placed outside the TOE (e.g. on servers), called primary assets. To protect these assets, it is vital to protect the TOE internal assets, e.g.: biometric reference and life records, claimed identity, configuration data, etc., (sometimes called secondary assets). The external entities can be authorized or not, can be humans or processes. Usually, the main "actors" are: administrator, user, attacker. Specifying threats, OSPs or both, some assumptions for the operational environment concerning connectivity-, personal- or organizational aspects can be added. Examples of threats are: "Using the identity of another user, an attacker may perform a brute force attack to be positively verified by the TOE.", "An attacker modifies biometric references or other security-relevant system configuration data.". An example of OSP is: "The TOE shall meet recognized national and/or international criteria for its security relevant error rates like: False Accept Rate (FAR) and False Rejection Rate (FRR)." More examples are included in [9]. The elementary items of the SPD (as well as SO, TSF) are specified by mnemonic names called generics.

4. Solution of this problem by setting the security objectives (SO) – for the TOE and its operational environment.

The security objectives are concise statements of the intended solution to the given SPD problem (i.e. threat, OSP, assumption solutions). The security problem can be solved partially by the TOE (specifying the TOE security objectives countering threats or enforcing OSPs) and partially by its environment (specifying the security objectives for the operational environment countering threats, enforcing OSPs or satisfying assumptions). The first case expresses the elementary TOE responsibility for security, e.g.: "The TOE shall ensure that all users can be held accountable for their security relevant actions." [9]. The second one expresses the elementary TOE operational environment responsibility for security, e.g.: "The TOE operating equipment and adequate infrastructure shall be available (e.g.: operating system, database, LAN, public telephone, and guardian)." [9]. The developer should provide a rationale that security objectives really solve the problem and are necessary. Security objectives represent an elementary security measure.

5. Working out the security requirements.

The security functional requirements specification (SFRs) is elaborated on the basis of TOE security objectives, while the security assurance requirements specification (SARs) is derived mainly from the declared EAL (please note: EALs are predefined packages of SARs). The SFRs are expressed with the use of the functional components from Part 2 of the standard [1], while the SARs are expressed by the assurance components from Part 3. Both kinds of components are grouped in families and the families – in classes representing ordered security issues. The components can be considered the semiformal specification language of Common Criteria. The informally expressed TOE security objectives are translated to the SFR components and they will be implemented in the TOE security functions. For example, the "FAU_GEN.1 Audit data generation." component presents requirements how the audit records should be created and what they should contain. The security objectives for the TOE operational environment are not translated to the components and will be expressed in technical and operational documentation of the biometric system. The set of SARs implied by the claimed EAL can be modified by adding extra components or replacing components existing in the EAL by more rigorous ones (this is expressed by EAL+). The SARs will determine the range and details of the TOE development and the TOE evaluation processes. The security requirements elaboration is finalized by their rationale. An example of SAR is "ADV_TDS.3 Basic modular design." describing the TOE decomposition into subsystems and modules.

6. Preparation of the TOE summary specification (TSS).

The TSS contains the TOE security functions (TSF) derived from the SFRs, functions which should be implemented in the considered IT product or system during the next step – the TOE development process. The best practice is to group the SFRs around the specific security functionality and assign them to the defined TSF which implements this group. The TOE summary specification provides potential consumers of the TOE with a description how the TOE satisfies all the SFRs (presenting details concerning the SFRs implementation). Examples of TSFs expressed by generics (short mnemonics) [12] are: "TSF_FFD Detecting if a finger presented on the sensor is a fake or not.", the "TSF_AUDIT Producing an audit record for every use of the security functions of the TOE.".

The IT security development process provides a set of TOE security functions, which should be implemented, at the claimed EAL. This process can be facilitated by the use of the ST pattern elaborated in the CCMODE project.

Fig. 1 presents the CCMODE Tools – documents generator window with the security target pattern. On the left side the pattern structure is shown, while the right side presents some fields to be filled in by the IT product related data. Some fields are automatically filled in by data from the project knowledge base. On the bottom part some users functions and knowledge access points are available.

Using patterns the developer focuses on the TOE security issues only, not on composing the evidence documentation compliant with Common Criteria. During this work he/she is guided by the advanced help system.

4.2 TOE development process

The TOE development process encompasses the elaboration of the evidences documentation implied by SAR components of the claimed EAL (please note Table 1 placed on page 31 in the third part of the standard [1]).

The evidence material can have different forms:

- documentation, for example: configuration management plan, manuals for the maintenance personnel or for the administrator, security policy of an institution that develops the product, configuration list, procedure of the system installation, delivery procedure, testing documentation, plan of penetration tests, and many other documents of that type which, with respect to their contents, always resulting from proper SAR requirements;
- documented results of independent research or observations conducted by the evaluators, e.g. a report concerning the analysis of the TOE vulnerability and TOE development environment, report from independent testing of the TOE, report from the inspection of the TOE development environment, or a ranking list of risk cases identified in the development environment;
- behaviour or activities of people who play certain roles in the TOE life cycle, for example the roles resulting from a certain procedure (accepting the product of system before it is delivered to the client, etc.); an example of such evidence can be a protocol, note or the so called records, i.e. traces of different operations (activity reports, logs – either electronic or not) recorded in the management system.
- security target or protection profile.

This process of the TOE development includes:

1. Preparation of the ADV (Development) assurance class evidences (architecture, interfaces, design, implementation).
2. Preparation of the ALC (Life cycle support) assurance class evidences (configuration management, product delivery, development process security, used tools).
3. Working out the test documentation (ATE class), including tests specification, their depth and coverage.
4. Working out the TOE guidance documents (AGD class), i.e. manuals and procedures.
5. Vulnerability analysis support (AVA class).

The result of this process are evaluation evidences for the given IT product and the EAL claimed for it.

4.3 IT security evaluation process

The IT security evaluation is performed by an independent security lab accredited according to the existing national evaluation scheme. The basic tool is the security evaluation methodology CEM [14]. The certificates are published in the Common Criteria portal [6].

IT security development and TOE development processes can be conducted in a traditional way – from the basics with the help of consultants, or they can be carried out on the basis of patterns and supporting tools. The developed evidence material prepared with the use of tools is more coherent – thanks to that there are fewer problems during the evaluation.

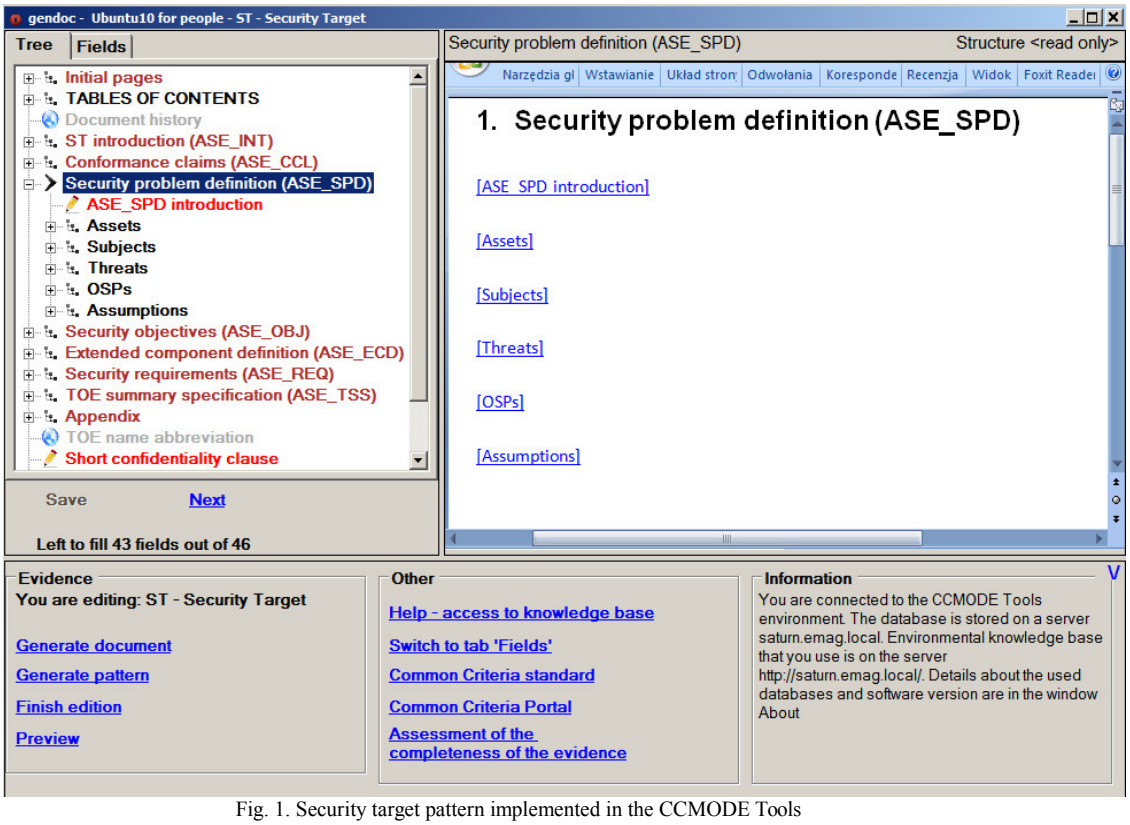

Fig. 1. Security target pattern implemented in the CCMODE Tools

V. Computer aided development of IT products

IT developers, including biometric devices developers, are focused on their products, use technology-specific language and have difficulties to express the results of their work in the Common Criteria specific terms. This standard specifies a set of detailed requirements (SARs) and the developers have troubles how to produce evidences meeting these SARs. They expect assistance by experts or patterns of evidences. Thanks to these patterns they focus only on the product-related issues, not on composing the evidences. Within the CCMODE project such patterns were elaborated as Microsoft Word templates for all assurance components [3]–[4], [15]–[16]. Additional advantages were achieved thanks to the software support of the Common Criteria related processes. The CCMODE Tools for developers [5] was elaborated as a result of the CCMODE project. The Tools encompass:

- project manager module, responsible for initialization of projects and their management in the life-cycle models,
- configuration management module, responsible for the configuration management according to the CC requirements on different EALs,
- Microsoft Word-based GENDOC module designed to work out evidences,
- Sparx System Enterprise Architect (EA)-based module for security analyses and the ST/PP elaboration,
- Subversion (SV)-based module responsible for versioning the project artifacts (including evidences),
- Redmine-based module for TOE design bug tracking and the ALC_FLR implementation,
- Testlink-based module for test development and management (ATE),
- project self-assessment module (CEM compatible),
- auditing module allowing to assess the conformance with different standards,
- knowledge base module for the project management,
- standard-related knowledge.

CCMODE Tools support traditional CC-related projects as well as the site certification concept [17].

VI. Conclusions

The paper presents general guidance for the biometric technology developers with respect to the Common Criteria standard requirements. This standard allows to develop biometric devices with the claimed measurable assurance. The assurance is based on the rigorous methodical development and independent evaluation by an accredited body. The paper provides biometric technology developers with concise information about three basic Common Criteria processes.

The paper draws the readers' attention to certain barriers in the dissemination of certified products, including biometric products. The major barriers are the lack of knowledge and skills among the developers in the use of the Common Criteria standard, high costs of the products development, lack of supporting tools and patterns that would facilitate the use of the CC methodology. The barriers result in the fact that in some IT domains the number of certified products is low. This concerns biometric technologies too.

In the huge number of certified IT products (more than 1,200) only 3 are biometric devices and only 2 protection profiles of biometric products were elaborated and evaluated. The developers point at difficulties in the preparation of evidence material [8]. To help IT developers in this activity, a set of evidence patterns was elaborated and all CC-related development and evaluation processes were computer supported (CCMODE Tools). It is extremely important to have access to knowledge which enables to carry out projects. Therefore the set of tools is supported by an extensive knowledge base.

The CCMODE project focused on the computer support of the CC-related projects management, CC-related security analyses, and pattern-based development of the evaluation evidences. More information about using this tool is placed in [5], [18]. The developers of biometric products who are free from going deep into the nuances of the Common Criteria standard and do not have to prepare the structure and layout of their evidence material from the basics, would be certain to say that their work is easier.

Computer support of the security development process according to the Common Criteria standard is the value provided by the CCMODE project. This is particularly due to the following:

- central management of the project with respect to: roles, development tools (UML, SDK, calibration tools, personalization tools, CAE/CAD, etc.), life cycle models,
- providing CCMODE Tools with the tools to manage the versions and configuration of the product, documentation, faults, tests, security measures of the development environment, and with the tools to conduct analyses, make security models, and carry out audits for compliance and security evaluation,
- providing the developers with proper-structure patterns supported by precise guidelines from the data base about what kind of information should be put in particular fields; these fields are partially filled in automatically with data from the project knowledge base.

These activities are undertaken to facilitiate the developers' work, lower the cost and shorten the time of new products development. This is particularly important in niche-market domains of the standard application, where there are not many products developed. Biometric technology is such a domain.

CCMODE Tools and the accompanying patterns were validated on the basis of several projects concerning software systems and intelligent sensors [4]–[5], [19]–[22]. The paper is an encouragement to take up validation in the field of biometrics. This work should start with the extension of the data base with a subset of generics describing assets, subjects, threats, OSPs, assumptions, security objectives, and

functions that would allow to make and analyze security models of biometric devices.

References

[1] Common Criteria for IT security evaluation, part 1-3. v. 3.1. 2009.

[2] Guidelines for Developer Documentation according to Common Criteria Version 3.1, Bundesamt für Sicherheit in der Informationstechnik, 2007.

[3] CCMODE (Common Criteria compliant, Modular, Open IT security Development Environment) Project. http://www.commoncriteria.pl/ (Accessed 18 May 2013).

[4] Białas A. (Ed.), "Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria", Wydawnictwo Instytutu Technik Innowacyjnych EMAG, UE POIG 1.3.1, Katowice 2011 r. (in Polish).

[5] Białas A. (Ed.), "Komputerowe wspomaganie procesu rozwoju produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa", Wydawnictwo Instytutu Technik Innowacyjnych EMAG, UE POIG 1.3.1, Katowice 2012 r. (in Polish).

[6] Common Criteria Portal, http://www.commoncriteriaportal.org/ (Accessed 18 May 2013).

[7] Daisuke Horie, Kenichi Yajima, Noor Azimah, Yuichi Goto, and Jingde Cheng, "GEST: A Generator of ISO/IEC 15408 Security Target Templates", In R. Lee, G. Hu, H. Miao (Eds.): Computer and Information Science 2009, SCI 208, Springer-Verlag Berlin Heidelberg 2009, http://link.springer.com/chapter/10.1007%2F978-3-642-01209-9_14#page-1 (Accessed 18 May 2013), pp. 149–158.

[8] Higaki W.H.: "Successful Common Criteria Evaluation. A Practical Guide for Vendors". Copyright 2010 by Wesley Hisao Higaki, Lexington, KY 2011.

[9] Biometric Verification Mechanisms Protection Profile, BVMPP v1.3, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2008.

[10] Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies, FSDPP_OSP v1.7, Bundesamt für Sicherheit in der Informationstechnik, Bonn 2009.

[11] Security Target for PalmSecure Fujitsu Limited, BSI-DSZ-CC-0511, 2008.

[12] MorphoSmart Optic 301 Public Security Target, Safran Morpho, 2013.

[13] AuthenTest Server, Authenware, 2010 (in Spanish).

[14] CEM v3.1, Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, 2009.

[15] Bialas, A., "Patterns Improving the Common Criteria Compliant IT Security Development Process". In: Zamojski W., Kacprzyk J., Mazurkiewicz J., Sugier J., Walkowiak T. (Eds.): Dependable Computer Systems; Advances in Intelligent and Soft Computing, Vol. 97, 2011, Springer-Verlag: Berlin Heidelberg, pp. 1-16.

[16] Bialas A., "Patterns-based development of IT security evaluation evidences", The 11th Int. Common Criteria Conference, Antalya, 21-23 September 2010 (published in an electronic version), http://www.11iccc.org.tr/presentations.asp (Accessed 10 Feb 2013).

[17] Rogowski D., Nowak P.: "Pattern based support for Site Certification". W. Zamojski et. al. (Eds.): Complex Systems and Dependability, Advances in Intelligent and Soft Computing (AISC) 170, pp. 179-193. Springer-Verlag Berlin Heidelberg 2012.

[18] Rogowski D., "Software Implementation of Common Criteria Related Design Patterns" Proceedings of the 2013 Federated Conference onComputer Science and Information Systems (FedCSIS), pp. 1147–1152, ISBN 978-1-4673-4471-5 (Web), IEEE Catalog Number: CFP1385N-ART (Web).

[19] Białas A., Security-related design patterns for intelligent sensors requiring measurable assurance, *Electrical Review (Przegląd Elektrotechniczny)*, ISSN 0033-2097, vol. 85 (R.85), Number 7/2009, pp. 92-99, Sigma-NOT, Warsaw (2009)

[20] Białas A., Ontological approach to the motion sensor security development, *Electrical Review (Przegląd Elektrotechniczny)*, ISSN 0033-2097, vol. 85 (R.85), Number 11/2009, pp. 36-44, Sigma-NOT, Warsaw (2009)

[21] Bialas, A. Common Criteria Related Security Design Patterns—Validation on the Intelligent Sensor Example Designed for Mine Environment. *Sensors* 2010, 10, 4456-4496, http://www.mdpi.com/1424-8220/10/5/4456

[22] Bialas, A. Common Criteria Related Security Design Patterns for Intelligent Sensors—Knowledge Engineering-Based Implementation. *Sensors* 2011, 11, 8085-8114, http://www.mdpi.com/1424-8220/11/8/8085/