Paper

Cryptology Laboratory – its quality system and technical competence according to the ISO/IEC 17025 standard

Robert Wicik

Abstract—A laboratory is an organization which operates a quality system, has technical competence, generates valid results and its quality system and technical competence are conformed and recognized. A cryptology laboratory operates in information technology security area, where cryptographic methods of information protection play main role. Appropriate confidence, correctness and effectiveness of security services is needed and may be achieved trough development, evaluation, accreditation and certification processes performed by competent and commonly recognized organizations like: laboratories, certification and accreditation bodies. We describe in the paper the accreditation and certification structure and the IT security framework and also the role of the cryptology laboratory in this structure and framework.

Keywords*— *cryptology laboratory, certification, accreditation, quality system, ISO/IEC 17025 standard.

1. Introduction

A laboratory is an organization [1] which:

- operates a quality system – according to the ISO/IEC 17025[1] international standard;
- is technically competent – has competent personnel, sufficient equipment and appropriate test methods and procedures;
- is able to generate technically valid results;
- has conformed and recognized competence (for example) by government bodies.

A cryptology laboratory is a specific kind of laboratory which operates in information technology (IT) security area, where cryptographic methods of information protection play main role. Each IT system or a product has its own requirements [3] for maintenance of confidentiality, integrity and availability and implement a number of technical security enforcing functions to meet these requirements. Appropriate confidence, correctness and effectiveness of these functions are needed and may be achieved through development, evaluation, accreditation and certification processes performed by competent and commonly recognized organizations: laboratories, certifications bodies and accreditation bodies.

[1] "Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących", PN-EN ISO/IEC 17025, 2001 (in Polish).

The main area of activity of the Cryptology Laboratory is testing, analyzing and evaluating of cryptographic:

- systems and devices;
- transformations (ciphers, integrity functions, generators, etc.);
- protocols;
- other crypto mechanisms.

Results of these tests, analysis and evaluations are used in design and certification processes of:

- secure IT products;
- products that bring security features to general systems
- or in design and accreditation of secure IT systems.

In this paper, we explain evaluation processes and evaluation criteria of secure IT products and systems during the certification of type and the certification of conformity. We show the role in certification processes of the Cryptology Laboratory and we emphasize importance of its quality system and the set of technical procedures.

2. Product certification and system accreditation

Information technology security [4] means:

- confidentiality – prevention of the unauthorized disclosure of information;
- integrity – prevention of the unauthorized modification of information;
- availability – prevention of the unauthorized withholding of information or resources.

An IT system or product has its own requirements for maintenance security services and it implements a number of technical security enforcing functions to meet these requirements. Appropriate confidence, correctness and effec-

tiveness of these functions is needed and may be achieved through development, evaluation, accreditation and certification processes performed by competent and commonly recognized organizations like: laboratories, certification and accreditation bodies (see Fig. 1).

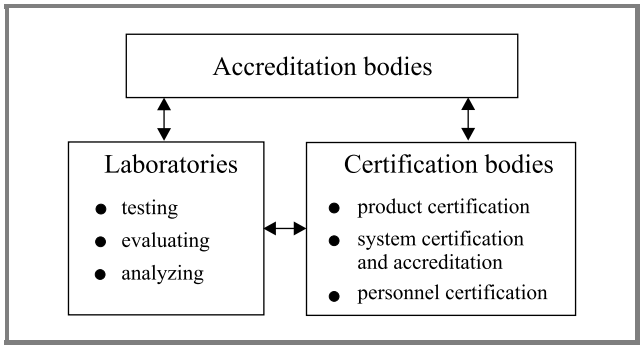

Fig. 1. Accreditation and certification structure.

Accreditation bodies recognize and verify competence of laboratories and certification bodies. It is a national organization responsible for accrediting laboratories and certification bodies according to the standards, for example to the ISO/IEC 17025 standard or another requirements. Accreditation is a procedure by which an authoritative accreditation body gives formal recognition that the laboratory or certification body is competent to carry out specific conformity assessment tasks.
Certification bodies perform a product and system certification, a system accreditation and a personnel certification. A certification body is a national organization, often the National Security Authority, responsible for administering evaluations of products and systems within that country. The certification body issue certificates (certification reports) – public documents, which are formal statements confirming the results of the evaluation and that the evaluation criteria, methods and procedures were correctly applied.
Laboratories perform testing also analyzing and evaluating of devices and systems. Accredited laboratories issue evaluation technical reports which are submitted to the certification body detailing the findings of an evaluation and forming the basis of the certification.

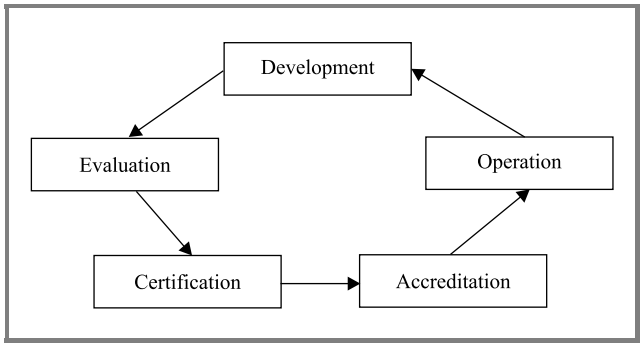

Fig. 2. IT security framework.

IT security framework covers [2]: development, evaluation, certification, accreditation and operation of a security device or system (as in Fig. 2).
In the development process an IT system or product is built.
In the evaluation process it is assessed against defined security evaluation criteria.
In the certification process it is confirmed that the results of an evaluation are valid and the evaluation criteria have been applied correctly.
In the system accreditation process it will be confirmed that the use of an IT system is acceptable within a particular environment and for a particular purpose.
In the secure operation process an accredited system is operated according to approved procedures.

3. General requirements for testing laboratories

A testing laboratory should meet requirements according to the ISO/IEC 17025 standard issued in 1999, which covers: "General requirements for the competence of testing and calibration laboratories". The standard [1] includes:

– management requirements concerning quality system and documentation;

– technical requirements concerning personnel, test methods and equipment.

This standard is applicable to all organizations performing test also laboratories where testing forms part of product certification. It is for use in developing quality, administrative and technical systems. Laboratory clients, regulatory authorities and accreditation bodies may also use it in confirming or recognizing the competence of laboratories.
Management requirements [1] for a laboratory include:

1. Organization – the description of the laboratory organization and the identification of potential conflicts of interest, when a laboratory is a part of larger organization.

2. Quality system – introduces some specific directions what must be in a quality policy statement to comply with ISO/IEC 17025 standard.

3. Document control – demonstrates how laboratory's documents are issued, identified, changed and approved.

4. Review of requests, tenders and contracts – it is to resolve any differences between the request or tender and the contract before any work commences. Each contract shall be acceptable both to the laboratory and the client.

5. Subcontracting of tests and calibrations – when the laboratory subcontracts work, this work shall be placed with a competent subcontractor (complies with ISO/IEC 17025 standard).

6. Purchasing services and supplies – the laboratory should have procedures for the selection purchasing of services and supplies that affect the quality of the tests.

7. Service to the client – describes laboratory's cooperation with the client and principles of a client's access to relevant areas of the laboratory's work.

8. Complaints – the laboratory should have procedures for the resolution of complaints received from clients.

9. Control of nonconforming testing work – there are specific requirements for dealing with nonconforming testing results and reference to corrective action in such cases.

10. Corrective action – there are specific procedures defined for cause analysis, selection and implementation of corrective action, subsequent monitoring and follow-up audits.

11. Preventive action – it should be undertaken, if improvements and potential sources of nonconformances, either technical or concerning the quality system are identified.

12. Control of records – quality and technical records from internal audits and management reviews as well as records of corrective and preventive actions.

13. Internal audits – internal auditors periodically conduct internal audits of activities of the laboratory to verify its quality system and the testing activities.

14. Management reviews – the laboratory's executive management periodically conduct a review of the laboratory's quality system and testing activities to ensure their continuing suitability and effectiveness, and to introduce necessary changes or improvements.

Technical requirements for a laboratory include [1]:

1. General – describes which factors determine the correctness and reliability of the tests performed by a laboratory.

2. Personnel – the laboratory should have competent personnel as well as plans and procedures of education and training.

3. Accommodation and environmental condition – laboratory facilities and environmental conditions should help testing and do not adversely affect the required quality of tests.

4. Test methods and method validation – the laboratory uses methods and procedures for testing which should be validated if they are not standardized.

5. Equipment – the laboratory shall possess sampling, measurement and test equipment which should be regularly calibrated or checked.

6. Measurement traceability – it is traceability to the International System of Units (SI). It is possible and desirable in some areas and not in others.

7. Sampling – it is a procedure whereby a part of a substance, material or product is taken to provide for testing.

8. Handling of test items – the laboratory shall have procedures for the transportation, receipt, handling, protection, storage and retention of test items to protect the interests of the laboratory and the client.

9. Assuring quality of test results – the laboratory shall have quality control procedures for monitoring the validity of tests undertaken.

10. Reporting the results – the results of each test carried out by the laboratory shall be reported in the test report accurately, clearly, unambiguously and objectively and shall include all the information requested by the client and necessary for the interpretation of the test results.

Many factors determine the correctness and reliability of the tests performed by a laboratory. These factors include contributions from: human factors, accommodation and environmental conditions, test methods and method validation, equipment, measurement traceability, sampling and handling of test items. The laboratory shall take account of these factors in developing test methods and procedures, in the training and qualification of personnel and the selection of the equipment it uses.

4. Documentation of a laboratory

There are quality and technical documentations maintained in the laboratory. Laboratory's documentation should:

- be prepared according to the requirements included in the ISO/IEC 17025 standard;
- strict correspond with the real laboratory's activities;
- be updated, approved, legible, and accessible for the laboratory's personnel.

Documentation of the laboratory should include:

- The Quality Manual,
- The Management Procedures Manual,
- The Technical Procedures Manual,
- Test Instructions,
- other documents and records describing every important properties and activities of the laboratory.

Basic laboratory's document is "The Quality Manual". In the quality manual there are defined the laboratory's quality system policies and objectives. The quality manual outlines the structure of the documentation used in the quality system of the laboratory. The quality manual includes or makes references to the supporting management procedures and technical procedures. The roles and responsibilities of quality and technical management as well as the rest of the personnel are defined in the quality manual.
"The Management Procedures Manual" is created if such procedures are not included in the quality manual. This manual covers supporting procedures of managing quality system and not covers technical (sampling and testing) procedures. Some aspects and data of laboratory's quality system can be covered by other documents, for example: rights and responsibilities of the laboratory's personnel and the organization and management structure.
"The Technical Procedures Manual" consists of laboratory-developed procedures which describe non-standard methods, laboratory-designed/developed methods, amplifications and modifications of standard methods. Developed methods and procedures should have been validated before use. Validation is the confirmation by examination and the provision of objective evidence that the particular requirements for a specific intended use are fulfilled. Each developed procedure should include records with results obtained form validation process.
"The Test Instructions" are supplements to the technical procedures. Test instructions are issued, if technical procedures insufficiently describe testing methods. A test instruction describes in details each steps to perform a technical procedure, such as: preparing samples, checking equipment, preparing workspace, performing tests, recording observations and results, other details needed to perform testing procedure.
Other documents and records maintained in the laboratory:

- definitions and terminology;
- a organization scheme of the laboratory;
- personal cards (function descriptions, duties, responsibilities);
- training (annual plans and programs of trainings);
- client complaints (register of complains, laboratory's judgments);
- approved suppliers (cards, problems, reviews);
- measuring equipment (register of equipment and their service, repairs, checks and calibrations);
- audits (schedule, programmes and reports);
- internal problems and correction actions;
- projects (proposals, realizations, approvals and introductions of documents of quality and testing system).

5. Test methods and procedures of the Cryptology Laboratory

The main area of activity of the Cryptology Laboratory is testing, analyzing and evaluating of cryptographic:

- systems and devices;
- transformations (ciphers, integrity functions, generators, etc.);
- protocols and other crypto mechanisms.

Results of these tests, analysis and evaluations are used in design and certification processes of:

- secure information technology products,
- products that bring security features to general systems;

or in design and accreditation of:

- secure information technology systems.

In the cryptology area, there are dominating non standard methods, which base on the common recognized evaluation criteria of ciphers, devices and systems. There are well known (or not) methods for determining crypto security parameters and features, which can by applicable as laboratory developed methods and procedures.
The cryptology laboratory can perform methods and procedures for:

- type certification;
- certification of conformity for objects or systems;
- evaluation of parameters for ciphers and other crypto transformations, binary sequences, etc.

Type certification bases on the national law and regulations and on the established criteria, for example on the Information Technology Security Evaluation Criteria – ITSEC [2] or Common Criteria for Information Technology Security Evaluation – CC [3]. Methods and procedures for type certification describes major actions taken during this process. Such methods and procedures can cover evaluations of crypto transformations and mechanisms used in an assessed object.
Technical procedures for type certification can cover procedures such as:

- Inspection of the documentation – includes methods for determining whether the documentation of evaluated object is complete, precisely and exhaustively describes all aspects, which are essential for certification and for the goals, which was put in.
- Checking correctness of implementation – includes methods for determining whether the security enforcing functions are correctly implemented in the evaluated object.

- Effectiveness analyzing – includes methods for determining whether the security measures implemented in the evaluated object are effective against the identified threats.
- Vulnerabilities analyzing – includes methods for determining how recommended countermeasures prevent evaluated object from successfully attacking using construction, operational and exploitable vulnerabilities detected in the object.
- Other technical procedures written according to the established criteria (ITSEC, CC, etc.).

Certification of conformity authenticate that evaluation object is consistent with type of object, which obtained type certificate. Certification of conformity process can cover all of objects or samples taken from production line. Technical procedures for certification of conformity make use of documentation and prototype objects, which were basis of the type certification. Each assessed object can require new procedures developed on the start of certification process.

Technical procedures for certification of conformity can cover procedures such as:

- Examination of conformity for the software – includes methods for determining whether the tested software is compatible with prototype of this software.
- Examination of conformity for the device – includes methods for determining whether the tested object is compatible with prototype of the object, for which certificate of type was issued.

Technical procedures for evaluation of crypto-transformation can cover procedures such as:

- Randomness testing of binary sequences produced by stream ciphers, block ciphers, hash functions, etc.
- Independence testing of pairs of binary sequences produced by stream ciphers, block ciphers, hash functions, etc.
- Avalanche testing of block ciphers and other crypto transformations, for example S-boxes.
- Nonlinearity testing of crypto transformations, for example S-boxes.

5.1. Randomness testing

Binary sequences produced by ciphers should be statistically random in order to achieve high security level of cryptographic system. We examine randomness of sequences using statistical tests [8, 10]. These tests use statistics of binary samples and also chi-square and normal distributions. We use following statistical tests: frequency test, serial test, poker tests, runs test and autocorrelation test. During statistical testing of binary sequence we count appropriate statistics for each test. Obtained statistics we split into classes, which identify them from the best to the worst.

In the Cryptology Laboratory we have a technical procedure, which describes in details how to get samples of binary sequence, how to perform statistical testing of samples and how to interpret results of testing. This procedure uses laboratory-developed software, which implement statistical tests used in the method. The procedure and software are validated in the laboratory that gives expected results of testing. We use this procedure for testing binary sequences taken from:

– random and pseudorandom generators;

– stream and block ciphers;

– password and key generators;

– other cryptographic functions, where randomness is crucial.

5.2. Independence testing

Independence testing is similar to randomness testing but concern pairs of binary sequences. Binary sequences produced by ciphers should be statistically independent and we examine independence of pairs of them using statistical tests [9, 10]. These tests use statistics of pairs of binary samples and also chi-square and normal distributions. We examine independence of a pair of binary sequences using three statistical tests for appropriate bit-length pairs. For each test we count suitable statistics. Obtained statistics we split into classes, which identify statistics from the best to the worst.
In the Cryptology Laboratory we have a technical procedure, which describes in details how to get samples of pairs of binary sequence, how to perform statistical testing of samples and how to interpret results of testing. This procedure uses laboratory-developed software, which implement statistical tests used in the method. The procedure and software are validated in the laboratory that gives expected results of testing.

5.3. Avalanche testing

There are a few criteria of avalanche testing. The basic are: avalanche effect and strict avalanche criterion (SAC). Full avalanche effect and full SAC should appear after a few rounds in a properly constructed block cipher. Full avalanche effect will occur in the cipher, if the average number of changed bits in cryptograms is equal to the half-length of ciphered block, as a result of any bit of plain text or key changes. The cipher will fulfil the strict avalanche criterion, if the average probability of bit changing in cryptograms is equal to 0.5, as a result of any bit of plain text or key changes.
In the Cryptology Laboratory we implemented software calculating avalanche effect and strict avalanche effect which occur in the evaluated block cipher. This software is used by procedures which describes in details how to prepare cipher for testing, how to perform testing of avalanche effects in the cipher and how to interpret results of testing.

The procedure and software are validated in the laboratory that gives expected results of testing. We use this procedure for testing block ciphers and other cryptographic functions, where avalanche effects are crucial.

5.4. Nonlinearity testing

Nonlinearity is a basic criterion in achieving resistance of ciphers to cryptanalysis. We can calculate nonlinearity for Boolean functions and for complex functions composed of Boolean functions. Nonlinearity of a function is the Hamming distance to the nearest affine function (it is called classical nonlinearity) or to the nearest function, which have linear structure (it is called strict avalanche criterion). Cryptographically strong functions should have high nonlinearity – it means – large distance to cryptographically weak affine functions and function with linear structure.
In the Cryptology Laboratory we implemented software and a procedure for nonlinearity testing. We use this procedure for testing: elements of block ciphers (for example S-boxes), Boolean functions (used in S-boxes and stream ciphers) and other cryptographic functions, where nonlinearity is crucial.

5.5. Examination of conformity

In the Cryptology Laboratory we have testing procedures used in certification of conformity processes of cryptographic devices and software. We examine evaluated object, whether it is consistent with type of the object, which obtained type certificate. We process all of the objects or samples taken from production line. Results of our testing are basis for issuing certificate of conformity for examined objects by certification authority. Security devices and software with such certificates (and with certificate of type) can be used in IT security systems which process sensitive information (if obtain accreditation certificate).
Each assessed types of objects can require new procedures developed on the start of certification process.

6. Summary

Products and systems used for processing sensitive and classified information should be evaluated, certificated and accredited by competent and common recognized organizations like laboratories and certifications bodies. Certification bodies conduct certification processes, commission laboratory's testing, evaluations and analysis, and on this basis issue certificates for products and systems. Laboratories and certification bodies should operate according to the standards and be recognized by accreditation bodies.
The Cryptology Department has been operating in the Military Communication Institute for many years. The Cryptology Laboratory operates within the whole Cryptology Department using the quality system according to the ISO/IEC 17025 standard. The Cryptology Laboratory bases on the resources of the Cryptology Department, its personnel, knowledge and experience. The quality system according to the ISO/IEC 17025 standard was introduced in the Cryptology Laboratory in 2002. The Cryptology Laboratory is now recognized by the Products Certification Unit of the Military Security Authority.
Main object of interest of the Cryptology Laboratory is testing, analyzing and evaluating military crypto devices and systems. The Cryptology Laboratory performs works commissioned and financed by producers and vendors of cryptographic devices and systems. Results of the Cryptology Laboratory works are used in the certification and accreditation processes performed by the Products Certification Unit.

References

[1] "General requirements for the competence of testing and calibration laboratories", ISO/IEC 17025 Standard, 1999.

[2] "ITSEC (and ITSEM) – Information Technology Security Evaluation Criteria (and Methodology)", United Europe Commission, 1991–1993.

[3] "CC (and CEM) – Common Criteria (and Evaluation Methodology) for Information Technology Security Evaluation", ISO/IEC 15408 Standard, 1999.

[4] "UK Scheme Publications – UK IT Security Evaluation and Certification Scheme", Certification Body – CESG, Cheltenham, UK, 1999–2002.

[5] "Quality Manual and Procedures Manuals of Cryptology Laboratory", Military Communication Institute, Zegrze, 2002–2004.

[6] J. Pieprzyk, T. Hardjono, and J. Seberry, *Fundamentals of Computer Security*. Berlin: Springer-Verlag, 2003.

[7] A. Menezes , P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton Florida: CRC Press, 1996.

[8] R. Wicik, "Properties of a block cipher based on extended Feistel network with large S-boxes", in *Proc. Conf. RCMCIS'2000*, Zegrze, Poland, 2000.

[9] R. Wicik, "The statistical test for determining independence of pseudorandom bit sequences used in cryptographic systems", in *Proc. Conf. RCMCIS'01*, Zegrze, Poland, 2001.

[10] M. Borowski and R. Wicik, "How to speed up a stream cipher", in *Proc. Conf. RCMCIS'02*, Zegrze, Poland, 2002.

Robert Wicik was born in Iłża, Poland, in 1970. He received the M.Sc. degree in computer science and the Ph.D. degree in telecommunications – cryptographic data security from the Military University of Technology, Warsaw, Poland, in 1994 and 2000, respectively. He has been working in the Military Communication Institute since 1994. His main interests include cryptology and data security. He has been leading the Cryptology Laboratory since 2002.
e-mail: wicik@wil.waw.pl
Military Communication Institute
05-130 Zegrze, Poland