Practical IS security design in accordance with Common Criteria

Frantisek Vosejpka

frantisek.vosejpka@i.cz

S.ICZ a.s.
Hvězdova 1689/2a
Prague 4, post zip 140 00

Abstract

The usage of Common Criteria (CC) [1], as an international standard for security description of the ***products developed on the information technology base*** (IT) already is an established practice that provides common rules for ***developers***, objectifies the ***evaluator***'s work and simplifies decisions of trusted IT system ***users***. However the CC may be utilized also along with the security design of entire information system (IS), particularly those handling classified information that should be evaluated and certified by National Security Agency (NSA).

From the very beginning the new IS design and architecture should incorporate the ***security architecture*** constituting elements. Afterwards the IS risk analysis results come into the design of IS security measures. Especially complicated IS bordering more external ISs with different classification level should be composed of more IT products, that are (depending on its position in the entire IS security architecture) assigned the range of ***security functional requirements*** and ***security assurance requirements***. The IT product complying stated requirements can be picked out on the market or be developed.

The IS security design should be done in the structure stated by CC for the ***Security Target*** (ST). Besides the CC requirements it should solve the IS security environment (and, in case of handling classified information, it must follow the CZ Act. No 148/1998 coll. [2]).

The ***security functional requirements*** should be stated into the entire IS grid, where each security product has its own column. The appropriate requirement windows of already existing products with evaluated ST can be ticked off immediately.

The ***security assurance requirements*** should be stated depending on IS security mode of operation and on the requirements stated on border with other connected ISs. It should be stated separately for both, the items of Trusted Computing Base, and for the specific products related to security critical mechanisms.

The blueprint ***Security Requirements for Development*** of each newly developed security product should be printed as an extract of the IS security design.

Keywords: INFOSEC, CIS Security Design, Common Criteria, CIS Security Target

1 Introduction

The usage of Common Criteria (CC) [1], as an international standard for security description of the products developed on the information technology base (IT) already is an established practice that provides common rules for developers, objectifies the evaluator's work and simplifies decisions of trusted IT system users. However the CC may be utilized also along with the security design of entire information system (IS), particularly those handling classified information that should be evaluated and certified by National Security Agency (NSA).

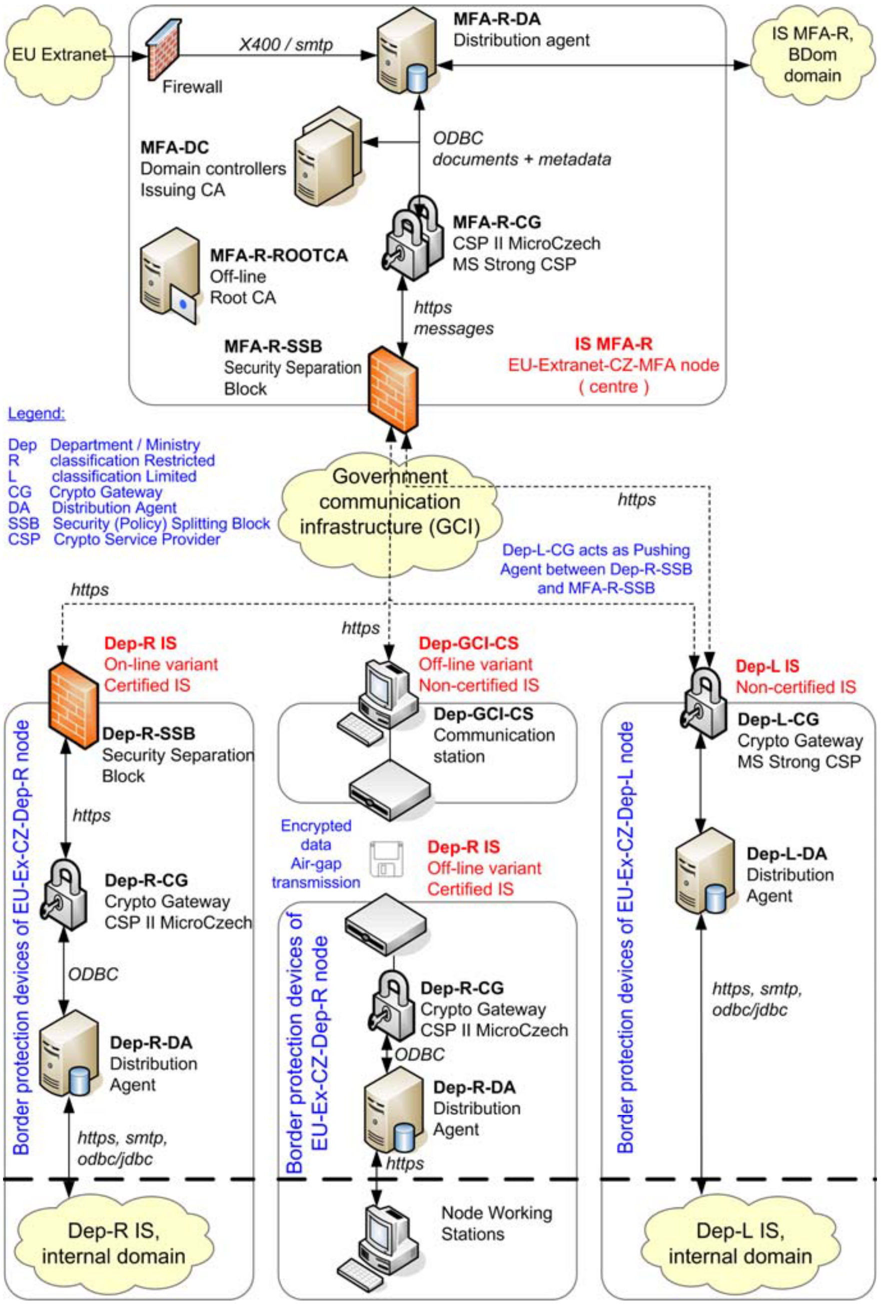
The security design of an IS handling classified information covers a somewhat larger area than stipulated by the CC for trusted IT systems. Parallel to the application of the security functional requirements and security assurance requirements stipulated by the CC, higher level security policy requirements (legislative requirements and IS security managers' requirements) must be applied. The security issue must be addressed in terms of the entire IS life cycle, including the planning, development, implementation, approval, operation, further development and withdrawing of the system. Apart from the field of computer and communication security, other security areas must also be dealt with, such as those concerned with the security of environments in which IS technologies are to be deployed and operated. They include personal security, physical security, cryptographic information protection, administrative security and organizational measures. All these measures must be evaluated and the operation of the IS approved by the Certification Authority.

- In the event that an IS handles CZ national classified information, the law shall be adhered to [2] and the Certification Authority shall be CZ NSA.
- In the event that an IS handles the EU or NATO classified information, the requirements of the given organization's INFOSEC guidelines shall be applied, and the Certification Authority shall be the relevant INFOSEC body.

2 Preliminary/Expert IS Security Design and Risk Analysis

2.1 Security Operational Requirements

The Czech EU Extranet IS design and development, presented in the DSM magazine [3], whose INFOSEC architecture is shown in the following chart, was chosen to illustrate the procedure.



The picture shows the central node (CZ MFA) linked to the EU Extranet (Brussels) and providing for the distribution of EU documents to the agencies' local nodes (Department/Ministry) and other governmental organizations. The basic requirements in terms of operational security were as follows:

- to ensure the secure sorting and distribution of classified (classified RESTRICTED) and unclassified (LIMITED - unclassified but sensitive) official documents;
- to ensure the secure transmission via WAN and secure interconnection of information systems and nodes featuring different security policies and divided into two levels of classification (certified RESTRICTED and non-certified LIMITED).

2.2 System Design Rules Applied

At first, a new IS design architecture focuses on meeting users' reasonable operational needs using IT (minimality and least-privilege principles). It is desirable that a new IS design includes from the beginning at least a preliminary/expert IS Security Architecture design, which then undergoes a risk analysis that looks into the assurance of major security objectives, including data confidentiality, accessibility and integrity, as well as availability of IS services. The risk analysis results are input into the final IS security design.

- Generally, the IS security architecture and security design are primarily concerned with the so-called Trusted Computing Base (TCB), addressing the issue of computer and communication IT security within IS. The TCB should further include other devices affecting IS security, such as integrity checks and antivirus devices (defence-in-depth principle). The TCB must comply with the security functional requirements and the security assurance requirements prescribed by the law and the CC.
- Good commercial technologies, verified in practice, which leave the security assurance to the TCB, may be used at the IS application level. The application SW is subject to common requirements, such as secure installation, reliable operation, upgrading and service packs application.

The strength of the TCB security mechanisms must respond to threats occurring in IT, as well as to the entire IS security environment level (node, domain etc.) and the level of risks associated with individual IS assets. In commercial IS, the major criterion is the cost of assuring the survival of the system after it has been exposed to threats, which is regularly a compromise between the costs of ensuring principal security objectives and the amount of damage caused by their failings. In addition, those ISs intended for the processing of classified information are required by law to establish their security mode of operation [4] related to the level of classification, and assign a minimum level of security requirements to be fulfilled.

Once these measures for the IS security environment are established and organizational steps have been taken to ensure their implementation, they may be considered eligible for the deployment of IT products identified, for example, with the Controlled Access Protection Profile (CAPP) [5], where, in the Overview, the following is stated: „*The CAPP provides for a level of protection which is appropriate for an assumed non-hostile and well managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The CAPP does not fully address the threats posed by malicious system development or administrative personnel. CAPP-conformant products are suitable for use in both commercial and government environments*".

IT devices protecting a node against attacks from other nodes of the same IS, i.e. nodes covered by the same security policy (self-protection node principle), may also be regarded as a TCB components.

More complex ISs, which may be interconnected with external IS or even with IS with a lower classification (lower security level), have, apart from the TCB, other IT constituting an IS interface/border. However, the IS border protection devices must be assessed and designed separately, in the context of the border-specific risk analysis results (border-protection principle).

3 IS Security Design

The "IS Security Design" as such must include the necessary security requirements and be eligible for evaluation. This implies the following:

- the design is made within the structure prescribed for the Security Target by the CC;
- the design must follow the risk analysis results;

- identified threats must be covered by the CC requirements and additional requirements ensuing from the higher level security policies must be laid down;
- security requirements for the individual IT of the TCB and border devices must be represented separately;
- a consistent range of security functional requirements and security assurance requirements are determined for each security technology;
- necessary IT products conforming to the set requirements may be chosen in the market or developed.

3.1 IS Description

Let us bring up again the objective of this article: to show the description of the entire IS security set-up within the “Security Target” structure in such a way as to display the CC requirements for all the TCB security-relevant components and to project the requirements of the higher level security policies (legislation). This document also seeks to show how these requirements should be interpreted with respect to the purchase or development of new IT products, and, finally, in relation to security evaluation.

The “IS Description” section should describe the purpose of the entire IS, its basic functionality, the geographic arrangement of nodes, security mode of operation, information classification levels and categories, overall IS security architecture, IS assets and minimum functionality required. In the event that connection with other IS is established, it should also describe mutual data flows, the system configuration of distributed technologies and managements’ scopes of operation. At this point, the security functions used, such as Security Audit (FAU), Identification and Authentication (FIA) and User Data Protection (FDP), may already be enumerated.

3.2 IS Security Environment

This chapter summarizes the envisaged assurance of the IS secure environment and presents a list of higher level security policies, security threats and risk analysis results. The risk analysis is carried out using the knowledge of IS architecture that has already been designed (including both existing technologies and technologies which are yet to be developed) and the environment in which the IS is to be implemented.

3.2.1 Assumptions for the IS Security Environment

The assumptions for the secure utilization of the IS include the security requirements essential for the IS security operation. However, they are not provided by the IS supplier and, in general, they do not fall within the full scope of operation of core IS management. The following items have been addressed:

A.PHYSICAL_SECURITY – It is assumed that physical security is built, documented and operated in accordance with the legal requirements [2]. Uncontrolled access by unauthorized individuals is prevented. The security functions must establish a level of secure environment which corresponds to the security mode and the classification level of the information being processed.

A.EQUIPMENT_PROTECT - It is assumed that HW and SW whose integrity and accessibility are crucial for the enforcement of IS security policy and, accordingly, for overall IS security, are protected from unauthorized physical modification.

A.PERSONAL_SEC - It is assumed that personal security is assured, documented and controlled by the relevant operating bodies pursuant to the legislation [2]. It is further assumed that users follow the “IS Operational Security Guidelines” and act in the interest of the security of the IS.

A.MANAGE - It is assumed that the operator officially appoints the required number of administrators for each administrative role. Substitutability is established in order to ensure that necessary operations can continue to be performed within the required time interval in the event that the relevant administrator/user is unavailable. It is also assumed that any multiplication of the roles to be performed by each individual will not be such as to compromise IS security.

A.NO_EVIL_ADM – The administrators managing the IS in different roles must be trustworthy, must not be irresponsible, must adhere to the procedures set out in the IS documentation and must not misuse their privileges and compromise the operational and data security of the IS. The activity of the central administration will ensure that the entire IS life cycle runs in compliance with the legislative requirements.

A.LAN_SEC - It is assumed that LAN cabling and devices in the system locations are situated in compliance with the physical security requirements, are not shared by other IS and will not be used to attack the IS.

A.DOCUMENT_SEC - It is assumed that the IS operator exercises administrative security in accordance with law [2].

A.UNUSUAL_EVENTS – In the event that the level of threads from the environment grows and/or the risks to the IS increase, additional organizational measures will be taken to guarantee the security of the IS as required.

3.2.2 Organizational Security Policies

The organizational security policies are a set of procedures applied by the operator to the operation in order to protect information and physical assets. These policies comply with the legal requirements and other regulations [2]. The following items have been addressed:

P.SYSTEM_HIGH – The security mode of operation places demands on the security of the environment in which the information system works. The requirements are determined by the level of classification of the confidential information being processed and the users' authorization levels. The adequate application of security functions derived from the "system high" security mode of operation is required [4].

P.RESPONSIBILITY – The users of the IS must be responsible for their activities within the IS. Their responsibilities and liabilities must be set out and they must understand them. User activities that have an impact on the security of the IS must be recorded and checked on a secure and continuous basis.

P.AUTHORISED_USERS – A person may become an IS user only if he/she needs to have access to at least some of the information in the IS in order to duly perform his/her work for the organization, meets the personal security requirements, has valid authorization to gain access to a given level and scope of classified information, has received training and has been assigned a user's account for his/her specific role by the IS administrator.

P.NEED_TO_KNOW – The Need-to-Know rule enforces the minimality principle. Access to a classified item of information may be allowed if the work to be performed requires access to such information.

P.PRIVILEGE – The IS must be capable of limiting the extent of users' authorizations, namely by dividing users according to the roles they perform and allocating only the necessary extent of authorization to such roles. The roles must be divided for individual administrative actions (Least-Privilege or Privilege-Separation principles).

P.CRYPTO – Classified data flows between the IS nodes, conducted along communication links outside the secured facility, are secured by cryptographic devices certified by the NSA for the respective classification level. The cryptographic devices are located inside the operator's secured areas and operated in compliance with the legislation.

P.BORDER_PROTECT – All the IS borders are dealt with using IS project certified by the NSA. Any other (additional) borders are dealt with separately, documented and are also subject of certification by the NSA.

P.ANTIVIR – Antivirus protection for both servers and stations must be exercised at each IS node. The users shall follow organizational instructions concerning antivirus checks (safe conduct).

P.RELIABLE_HW – Choice of HW, backup level, UPS, maintenance and other actions must provide the necessary degree of IS reliability.

P.TRUST_APL_SW – The application SW may only be modified with the consent of the IS security administrator and pursuant to the procedures set out by the operational guidelines. The installation media must originate from a trusted source.

P.PHYSICAL_SEC – Physical security is built, documented and operated by the relevant departmental bodies in accordance with the legislation. Uncontrolled access by unauthorized individuals shall be prevented. The security functions must establish a level of secure environment which corresponds to the operational security mode and the level of classified information.

P. PERSONAL_SEC – Personal security is assured, documented and controlled by the organization in accordance with the legislation. The IS Management shall apply it to user accounts administration.

P. DOCUMENT_SEC – The document security shall be maintained in accordance with the legislation.

P.INCIDENT_REACT – The IS documentation must define requirements, mechanisms and procedures for the detection of and response to security incidents. A.UNUSUAL_EVENTS must be fulfilled**.**

P.INSTALLATION – The IS must adhere to all the procedures pertaining to the installation and configuration of the parameters of all the IS components (including OS and other security components, functionality of security functions and application SW).

P.IMPLEMENT_VERIF – The IS management shall assure that following P.INSTALLATION the IT security and environment implementation is verified, ensuring that security requirements, procedures and security functionality have been fulfilled prior to the commencement of operation classified information. The application of this policy makes it possible to carry out documented acceptance of IT prior to the start-up, after breakdowns and security incidents being rectified, and to verify the security situation on a regular basis.

P.IS_LIFE_CYCLE – Security must be assured at all stages of the IS life cycle, including the environment of IS operator, user and supplier.

3.2.3 Threats to Security

This section presents the risk analysis results:

- List of physical and information assets indicating their levels of classification and/or their financial value. Levels of threats to main security objectives, i.e. to Confidentiality (Classification), Integrity and Accessibility, are indicated for each asset. It is also added who is responsible for each asset.
- Threats and threat agents, which, according to the risk analysis, represent a potential breach of some of the assets or the IS security requirements. They are threats to IT and IS services, threats from an external network and threats from the IS environment. The threats may be presented in general terms or broken down into specific ones.
- List of vulnerabilities indicating weaknesses or the absence of security mechanisms which should protect IS assets from threats. Depending on the degree of risks specified below, the vulnerabilities must be covered by counter-measures; the operator must accept any residual risks.

3.3 Security Objectives

Security Objectives (O) are defined for the security functions of an IS and for the IS environment. The security objectives, categorized either for the IS information technologies or for the IS environment, make provision for the set goal to face the threats identified and comply with the organizational security policies identified. All the identified threats and organizational security policies are accounted for in one of the categories below.

3.3.1 IT Security Objectives

As opposed to the CC, where the definition of security objectives is only described for the IT of the IS internal section (IS column in the chart), the IS featuring borders between distant nodes and borders with other IS should also include border security objectives (column "Border" in the chart).

Security Objective	Description	IS	Border
O.I&A	The IS security function must provide for the user's unique Identification and Authentication prior to granting access.	Yes	Yes
O.RESIDUAL_INFO	The IS security function must ensure that no sensitive information is contained on any secured medium at the time of its being released from the system.	Yes	
O.DOMAIN_SEPARATION	This security objective is necessary to face the T.UNAUTHORISED_MODIFICATION threat. It ensures resistance to interference, modification or destruction by any unauthorized external agent. It ensures the appropriate operation administration. Domain policies must be defined.		Yes
O.INFORMATION_FLOW	This security objective is necessary to face the T.INCORRECT_CLASS, T.CLASS_LEVEL threats and to support the P.MANDATORY_ACCESS policy assuring that no information of a higher level of classification is transferred from the higher-level domain to the lower-level domain. It also provides for classification levels being correctly allocated within the IS.		Yes

Security Objective	Description	IS	Border
SELF_PROTECT_ NODE	The IS security function must ensure that the network nodes and domains are separated from the others and thus provide for the local management's unequivocal competence and responsibility for the node security.		Yes
O.DEFENCE_IN_ DEPTH	The IS security function must ensure that the individual IS components are reasonably protected against threats from within the system itself. They must provide protection against an attack carried out via the network and in the event that data from external media are entering. The user is held responsible for the use of these security functions.	Yes	Yes
O.ANTIVIR	Centrally administered antivirus protection for both servers and stations must be in place. The virus chains db are updated on a regular basis and at short time intervals to ensure that antivirus protection is capable of detecting a large portion of threats to which this area may be exposed.	Yes	Yes

3.3.2 Non-IT Security Objectives

Those objectives not constituting a part of the IT Security Objectives but related to the appropriate IT implementation and activities of the IT administrators are referred to as Non-IT Security Objectives. Some examples are given in the following chart.

Security Objective	Description
O.INSTALLATION	Procedures for delivery, installation, administration and operation pursuant to the IT security objectives must be established. …
O.VERIFICATION	The IS administration will ensure that security implementation is verified to assure that security requirements, procedures and security functionality are fulfilled prior to the approval to operate classified information. …
O.IS_LIVE_CYCLE	The IS life cycle stages and rules are established for both the IS operator and supplier's environments. …
O.TRUST_APL_SW	The rules for the selection of application SW are established. Only trusted application SW, free from malicious codes and causing no failures, will be installed.
etc.	

3.3.3 Objectives of IS Security Environment

The security objectives referred to in the previous two chapters are complete, but they assume the fulfilment of the Objectives of Security Environment, marked **OE**. In particular, they involve support from the organization's higher management and security awareness on the part of users in all roles, as well as their experience. They also involve emergency events and incidents of the "force majeure" type. Examples are given in the following chart.

Security Objective	Description
OE.PHYSICAL_SEC	All the personnel responsible for the IS must ensure that the security-critical components of the IS are protected against a physical attack which might breach the IT security objectives. Physical access to the areas with the IS components must be restricted to authorized personnel, namely by measures of physical security and/or by organizational measures compliant with the security requirements [2].
OE.PERSONAL_SEC	The personal security requirements must be met [2].
OE.DOCUMENT_SEC	Departmental administrative security is pursued according to [2].
OE.NO_EVIL_USERS	The administrators in all the IS roles must be trustworthy, must not be irresponsible, must be adequately trained, must adhere to the procedures set out in the IS documentation and must not misuse their privileges and compromise the operational and data security of the IS. Inadvertent mistakes may be expected to occur nevertheless.

Security Objective	Description
OE.INCIDENT_REACT	Rules are in place to guide response to security incidents and emergencies.
etc.	

3.4 IS Security Requirements

3.4.1 IS Security Functional Requirements

In order to fulfil the security objectives for IT, the IT must have implemented the "IT Security Functional Requirements", adopted from the Common Criteria [1], Part 2. The so-called added IT security requirements, such as antivirus protection, are incorporated.

CC ID	Functional component
Security audit (FAU)	
FAU_GEN.1	... see CC
FAU_GEN.2	... see CC
etc.	
Extended functional requirements (FEX)	
FEX_RPL.1	Secure data replication between the distributed IS components
FEX_VAR.1	Warning to the user about the legal implications of unauthorized system use
FEX_ANV.1	Antivirus protection
etc.	

3.4.2 IS Internal Security Environment Requirements

In order to ensure the security objectives for the secure node environment, the "IS Internal Security Environment Requirements", added beyond the scope of the CC [1], must also be implemented for the benefit of the IS.

Class ID	Functional component
Physical Security (FPH)	
FPH_SAR.1	Assets being placed in a security area
FPH_SAR.2	Central servers and interface devices being separated from users
FPH_SAR.3	Cryptographic devices being separated from the other assets
Personnel Security (FPE)	
FPE_CLE.1	Personal Clearance Certificate
FPE_ASS.1	Need-to-Know assignment
FPE_ASS.2	Assignment for the role in IS management
FPE_ASS.3	External Organisation and Contractor assignment
Document Security (FDS)	
etc.	
Border Protection (FBP)	
etc.	
Organisational Measures (FOR)	
etc.	

3.5 IS Security Assurance Requirements

The security assurance requirements should be established differently for each IT product:

- **TCB** - EAL3 will suffice for IT in an IS with "system-high" security mode of operation;
- **Antivir** – is part of the TCB. However, products within this range are not covered by the CC and are selected on the basis of practical operational experience, i.e. reliability and good performance in terms of prevention, detection and remediation of consequences caused by an attack.
- **Border** – EAL is required for border security devices and components which support border functionality inside IS (e.g. determining and evaluating document classification), depending on the level of the IS being interconnected. EAL4 is required for interconnection of ISs classified as RESTRICTED and LIMITED.

- **Crypto** – a) Cryptographic protection of classified information requires an NSA certificate.
b) A commercial device or SW will suffice for cryptographic protection of the LIMITED information. However, EAL3 for applications using this crypto-mechanism and an approval from NSA are required.

4 IS SPECIFICATION SUMMARY

4.1 IS Security Functions

4.1.1 Locations of Security Mechanisms on IS HW components

The security mechanisms implementing the set security functional requirements are located on IS HW components in such a way as to perform the security architecture functions specified at the beginning of this document. The locations are shown in the following chart (see also the picture above):

Computer	Domain	W2K	Anitivirus	Audit tool	DA Special SW	CG Special SW	Crypro device	SSB Special SW
Working Station (WS)	All	X	X					
DC Server	All	X						
Apl and DB Servers	All	X	X	X				
DA Server	All	X			X			
R-CG Server	RESTRICTED	X	X			X	X	
L-CG Server	LIMITED	X	X			X		
SSB	All							X
CS - Communication station	GSI (WAN)	X	X					

X – Security mechanism (W2K, Antivirus, …) is located on the computer.

4.1.2 Allocation of Functional Requirements to Security Mechanisms

The following chart shows the functional requirements (CC Identification) allocated to the security mechanisms. It should be noted that the secure environment requirements are set out in detail for the RESTRICTED domain only. The level of measures for the assurance of a secure environment for the LIMITED domain is only determined by the list of prescribed security functional requirements and the implementation is left to the internal Security Policies of the governmental organizations responsible for operation.

CC ID or Extended ID	W2K *1)	Anitivirus	Audit tool	DA Special SW	CG Special SW	Crypro device	SSB Special SW	Envirnmt (Restricted)
FAU_GEN.1	X	X		X	X	X	X	X
FAU_GEN.2	X			X	X		X	
FAU_SAA.2	X		X					
etc.								
FEX_RPL.1	X							
FEX_VAR.1	X							
FEX_ANV.1		X						
etc.								
FPH_SAR.1								X
FPH_SAR.2								X
FPH_SAR.3								X
etc.								

CC ID or Extended ID	W2K *1)	Anitivirus	Audit tool	DA Special SW	CG Special SW	Crypro device	SSB Special SW	Envirnmt (Restricted)
FPE_CLE.1								X
FPE_ASS.1								X
FPE_ASS.2								X
etc.								

*1) W2K is a commercial product, thus CC IDs for this column are adopted from Security Target [7].

4.1.3 Trusted Computing Base Functions

The methods and mechanisms for the implementation of the above-specified functional requirements should be described in this extensive section. The following partial implementation of the W2K Security Functional Requirements is only given here as a SPECIMEN.

4.1.3.1 W2K Security Functional Requirements

The critical security functions with the required EAL4+ level of guarantees for their appropriate functionality, documented by a certificate [6] pursuant to the CC [1], are ensured by the Microsoft Windows 2000 operating system with prescribed secure setup. The setting and checking are carried out by the security policies manager. The following security policy templates are used:

- CC_HiSec_W2K_DC.inf
- CC_HiSec_W2K_Domain.inf
- CC_HiSec_W2K_Professional.inf
- CC_HiSec_W2K_Server.inf

…

4.2 Measures for realization of IS Security Assurance Requirements

When mapping the "IS Security Assurance Requirements" for their incorporation into the measures, the procedure followed was analogous to that used in Item 4.1.

- The EAL3 requirements are applied to W2K and to the IS environment. In fact, W2K complies with EAL4 Augmented [6].
- The EAL4 requirements are applied to the DA, CG and SSB special software.
- The additional requirements are applied to a certified crypto-device (AEX_CCD.1) and a commercial crypto device (AEX_COM.1).

5 Rationale

The rationale demonstrates the completeness of the security target implementation. It documents the following:

- all the threats and organizational policies have been covered by at least one IT, non-IT or environment security target, and these are sufficient to deal with them;
- all the security targets (for IT, non-IT and environment) have been covered by the security functional requirements and the security assurance requirements;
- the security functional requirements and the security assurance requirements are capable of covering the requirements for overall IS security. The rationale includes the following components: commercial certified and non-certified components, newly developed components and those for the cryptographic protection of classified and unclassified but sensitive information.

The last section provides a review of vulnerable points and the level of residual threats which they are exposed to.

6 Selection and Development of Products for IS Implementation

IS implementation requires products which comply with the above specified Security Functional Requirements and Security Assurance Requirements. It is necessary to demonstrate that these requirements have been complied with. The possibilities are as follows:

- Selection of commercial products – the set Security Target and a Certificate issued by a reputable evaluation organization must be presented. As applicable, the certificate is not required for products with lower demands for guarantees. In the case of reliable products verified by practice it will be sufficient to document the implementation and to conduct credible tests of desirable security functionality (with NSA approval at all times).
- Development of new products – is carried out on the basis of written document "Requirements for Product Development", which summarizes the requirements for the aforementioned design.

Commercial and newly developed products do not necessarily have to have their own certificates. The certification authority (NSA) issues a certificate (it means approval to operate) for the entire IS on the basis of the test results and the evaluation of all the IS security components.

7 Conclusions

The solution presented in this article suggests one of the possible procedures in using the Common Criteria when designing a complex IS. The procedure introduced makes it possible to break down the overall security requirements into partial domains and technologies and shows the way to the development of much-needed secure IT products.

The previously published CZ IS EU Extranet chart was used as an example and the tables presented (assumptions, policies, targets, measures, etc.) include mere examples and are far from covering the entire solution. The detailed elaboration should follow the document structure included in the CC, Annex C (normative) Specification of Security Targets [1].

The document includes no classified information.

8 References

[1] Common Criteria for Information Technology Security Evaluation, CCIB-99-031 Version 2.1, August 1999, Incorporated with interpretations as of 2002-02-28 (published as ISO/IEC 15408, 1999, Evaluation Criteria for IT Security)

[2] CZ Act No 148/1998 Coll. Security of classified information, CZ NSA 1998

[3] Brusel za námi, Brusel před námi – part I and II, RNDr. Jiří Kopačka, Data Security Management journal, No 3/2004, 5/2004, web: www.dsm.tate.cz

[4] Regulation No 56/1999 Coll. - Security of information systems that handle classified information, its certification and attributes of certificates, CZ NSA

[5] Controlled Access Protection Profile version 1.d, National Security Agency, NSA Oct 1999

[6] "Common Criteria Certificate", issued by NIAP for MS Windows 2000 Professional, Server, and Advanced Server with Service Pack 3 and Hotfix Q326886, for Compaq Proliant and Dell platforms, EAL4 Augmented; Identified with CAPP [5]. The W2K Security Target [7] has also been subject of certification

[7] Windows 2000 Security Target, ST Version 2.0, 18 October 2002. It has been a component of W2K certification [6]