STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Krzysztof FAŁEK
Instytut Systemów Sterowania w Chorzowie

PROCES PROJEKTOWANIA ZABEZPIECZEŃ TELEINFORMATYCZNYCH NA PRZYKŁADZIE APLIKACJI KRYPTOGRAFICZNEJ

Streszczenie. Referat przedstawia metodykę projektowania zabezpieczeń teleinformatycznych w oparciu o normy międzynarodowe „Wspólne Kryteria do Oceny Zabezpieczeń Teleinformatycznych" (ISO/IEC 15408). Opisane zostały kolejne etapy projektowania Profilu oraz Zadania Zabezpieczeń. Zaprezentowany został również przykład Zadania Zabezpieczeń dla aplikacji do szyfrowania i podpisywania dokumentów elektronicznych SecOffice.

Słowa kluczowe: Wspólne Kryteria, Zadanie Zabezpieczeń, SecOffice, Przedmiot Oceny, Granice Przedmiotu Oceny, otoczenie zabezpieczeń, cele zabezpieczeń, wymagania na zabezpieczenia.

IT SECURITY DESIGNING PROCESS BASED ON THE COMMON CRITERIA STANDARD – EXAMPLE OF SECURITY TARGET FOR THE SECOFFICE PROGRAM

Summary. The paper presents designing methodology of IT security based on the international standard Common Criteria for IT Security Evaluation (ISO/IEC 15408). The designing steps for the Protection Profile and Security Target were described. The paper presents an example of the SecOffice's Security Target – the application used to digital signature and encryption of electronic documents.

Keywords: Common Criteria, Security Target, Target of Evaluation (TOE), SecOffice, TOE boundaries, security environment, security objectives, security requirements.

1. Wprowadzenie

W dobie szybkiego rozwoju teleinformatycznego rośnie zagrożenie utraty tajności i integralności wykorzystywanych, przechowywanych lub przesyłanych danych. Naprzeciw tym problemom wychodzą twórcy zabezpieczeń, konstruując różnego rodzaju zabezpieczenia zarówno sprzętowe, jak i programowe. Problemem jednak jest jednoznaczny sposób oceny jakości zastosowanych zabezpieczeń. Jedną z możliwości oceny jest oparcie się na silnie rozwijanych w ostatnich latach Wspólnych Kryteriach do Oceny Zabezpieczeń Teleinformatycznych [1], [2], [3] (*ang. CC-Common Criteria for Information Technology Security Evaluation*). Na podstawie Wspólnych Kryteriów Oceny jest realizowany Projekt Celowy KBN [8], którego jednym z elementów było wykonanie projektu zabezpieczeń teleinformatycznych.

Artykuł stanowi praktyczną ilustrację procesu projektowania Zadania Zabezpieczeń (*ang. ST – Security Target*) dla produktu „SecOffice" firmy Sotel, zgodnie z metodyką projektowania zabezpieczeń teleinformatycznych [4].

2. Zadanie Zabezpieczeń programu SecOffice

Zadanie Zabezpieczeń ma na celu formalne określenie wymagań na zabezpieczenia Przedmiotu Oceny (*ang. TOE – Target of Evaluation*) bez narzucania sposobu ich realizacji. Zadanie Zabezpieczeń jest związane z konkretną implementacją produktu w przeciwieństwie do Profilu Zabezpieczeń (*ang. PP - Protection Profile*), który nie wiąże się z konkretną implementacją.

2.1. Wprowadzenie do Zadania Zabezpieczeń (ST)

Pierwsza część projektu ma na celu prostą i jednoznaczną identyfikację Zadania Zabezpieczeń, słów kluczowych charakteryzujących opisywany TOE, jak również zakładany poziom uzasadnionego zaufania, dla którego prowadzone będą następne etapy procesu projektowania, znajdujące wyraz w kolejnych rozdziałach dokumentu. Oprócz identyfikacji część ta pozwala na zapoznanie w bardzo ogólny sposób z Zadaniem Zabezpieczeń oraz Przedmiotem Oceny, którego ono dotyczy.

Przykład 1. Sformułowanie identyfikatorów Zadania Zabezpieczeń oraz Ogólny opis Zadania Zabezpieczeń.

Identyfikatory Zadania Zabezpieczeń (ST)

Przedmiot Oceny (TOE): SecOffice – Program do szyfrowania i podpisywania dokumentów elektronicznych.

Wersja ST: 1.0.

Słowa kluczowe: SecOffice, podpis cyfrowy, zabezpieczenie dokumentów, szyfrowanie dokumentów, kryptografia.

Poziom uzasadnionego zaufania: EAL 3.

Stosowana wersja CC: 2.1.

Deklaracja zgodności z CC: [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introdution and General Mode; August 1999 (...).

Ogólny opis Zadania Zabezpieczeń

Zadanie Zabezpieczeń zaprojektowano dla programu SecOffice. Program przeznaczony jest do zabezpieczania dokumentów elektronicznych przez ich szyfrowanie oraz podpisywanie. Dokonuje on zabezpieczenia lub weryfikacji dokumentów bezpośrednio z poziomu programów pakietu Microsoft Office (Word i Excel) bez konieczności przechodzenia do innego programu szyfrującego (...).

2.2. Opis Przedmiotu Oceny (TOE)

Punkt ten przedstawia szczegółowy opis Przedmiotu Oceny zawierający dane o rodzaju produktu, jego funkcjonalności, granicach oraz środowisku działania. Na szczególną uwagę zasługują tu granice TOE, które pozwalają określić, jakie zagrożenia i podatności dotyczą samego Przedmiotu Oceny, a jakie jego środowiska.

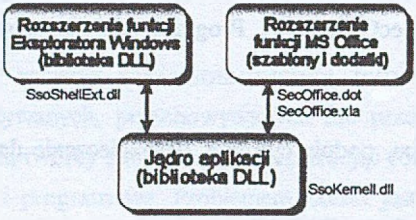
Przykład 2. Opis Przedmiotu Oceny

Rodzaj produktu

Przedmiot Oceny jest programem służącym do zabezpieczania dokumentów elektronicznych przez ich szyfrowanie oraz podpisywanie. Dzięki integracji z programami pakietu MS Office zabezpieczenie dokumentu może być wykonane bezpośrednio z poziomu tych programów. Program pozwala również na zabezpieczenie (szyfrowanie lub podpis) innych plików. Realizowane jest to poprzez integrację oprogramowania z Eksploratorem Windows, a funkcje zabezpieczeń dostępne są w menu kontekstowym dowolnego menadżera plików.

Funkcjonalność Przedmiotu Oceny (TOE)

SecOffice (Przedmiot Oceny) jest elementem pośredniczącym pomiędzy interfejsami użytkownika (aplikacje MS Office, systemowy Eksplorator Windows) a systemową biblioteką funkcji kryptograficznych (CryptoAPI).



Rys. 1. SecOffice - struktura aplikacji
Fig. 1. SecOffice – aplication structure

CryptoAPI, wchodząca w skład otoczenia TOE, udostępnia wszelkie potrzebne operacje kryptograficzne oraz operacje na certyfikatach. Dzielą się one na kilka grup, takich jak: podstawowe funkcje kryptograficzne, funkcje zarządzania certyfikatami czy funkcje do szyfrowania i odszyfrowania wiadomości (...).

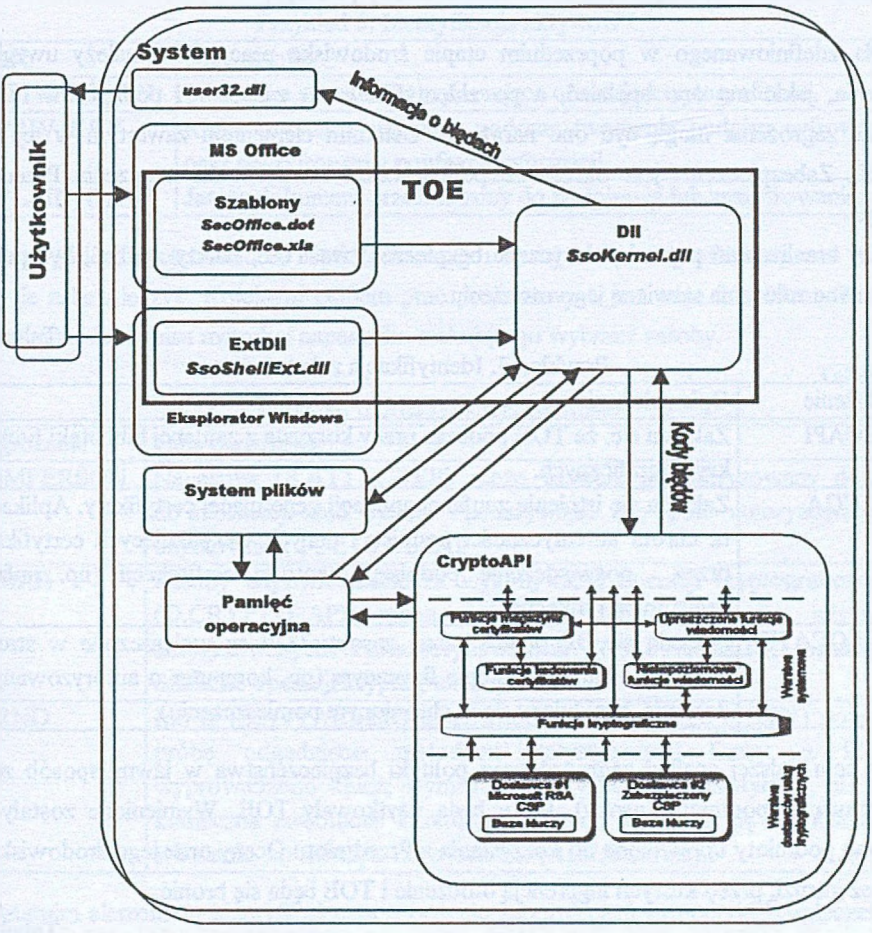
Granice TOE

Logiczne granice TOE

TOE odpowiedzialny jest za komunikację z użytkownikiem (przez rozszerzenie możliwości systemowego eksploratora, oraz aplikacji pakietu MS Office), przygotowanie danych do „obróbki kryptograficznej" (szyfrowanie, deszyfrowanie, podpisywanie, weryfikacja, wyliczenie wartości skrótu) oraz zebranie i zapisanie otrzymanych wyników. Obsługą funkcji kryptograficznych, bezpieczeństwem przechowywania certyfikatów oraz kluczy, jak również ochroną bibliotek odpowiedzialnych za operacje kryptograficzne zajmuje się system operacyjny (otoczenie TOE) (...).

Fizyczne granice TOE

W skład TOE wchodzi biblioteka SsoKernel.dll odpowiedzialna za przygotowanie danych przeznaczonych do obróbki kryptograficznej, wywołania odpowiedniej funkcji CryptoAPI oraz przekazywanie komunikatów do użytkownika (...). Pozostałe elementy związane z przepływem danych użytkownika zabezpieczone oraz nadzorowane są przez system operacyjny. W szczególności należy tu wymienić bibliotekę CryptoAPI realizującą funkcje kryptograficzne (...).



Rys. 2. Sterowanie przepływem informacji w SecOffice
Fig. 2. SecOffice information flow control

Środowisko działania TOE

Środowisko TOE stanowi bezpieczny system operacyjny (za bezpieczeństwo systemu odpowiada jego administrator), który kontroluje bezpieczeństwo wszystkich istotnych elementów TOE oraz jego otoczenia i zasobów. System ten jest zainstalowany na komputerze o kontrolowanym dostępie, dzięki temu TOE wraz z zasobami i otoczeniem nie jest narażony na ataki fizyczne.

2.3. Otoczenie zabezpieczeń Przedmiotu Oceny (TOE)

Dla zdefiniowanego w poprzednim etapie środowiska pracy TOE należy uwzględnić założenia, jakie ma ono spełniać, a po zidentyfikowaniu zasobów i podmiotów określić, na jakie zagrożenia mogą być one narażone. Ostatnim elementem zawartym w tej części Zadania Zabezpieczeń jest określenie polityk bezpieczeństwa dla otoczenia Przedmiotu Oceny.

Aby zrealizować potrzeby dotyczące bezpieczeństwa TOE, należy zadbać, by spełnione były pewne założenia stawiane jego otoczeniu.

Tabela 1

Przykład 3. Identyfikacja założeń

Założenie	Opis założenia
AE.CAPI	Zakłada się, że TOE podczas pracy korzysta z zaufanej biblioteki funkcji kryptograficznych.
AU.CGA	Zakłada się istnienie zaufanej aplikacji generującej certyfikaty. Aplikacja ta chroni autentyczności podpisu i danych weryfikujących certyfikatu przez poświadczenie podpisem centrum certyfikacji (np. zaufane centrum certyfikacji).
AE.LOCATE	Zakłada się, że przetwarzane zasoby TOE są umieszczone w strefie o kontrolowanym dostępie fizycznym (np. komputer o autoryzowanym dostępie, znajdujący się w chronionym pomieszczeniu).

W celu dalszej analizy zagrożeń oraz polityki bezpieczeństwa w jawny sposób zostają przedstawione podmioty (osoby), które będą użytkowały TOE. Wymienione zostały tutaj zarówno podmioty uprawnione do korzystania z Przedmiotu Oceny oraz jego środowiska, jak również intruzi, przed których ingerencją otoczenie i TOE będą się bronić.

Tabela 2

Przykład 4. Identyfikacja podmiotów

Podmiot	Opis
S.USER	Zakłada się że każdy użytkownik systemu operacyjnego może jednocześnie korzystać z TOE.
S.ADMIN	Zakłada się istnienie co najmniej jednego użytkownika systemu operacyjnego z prawami administratora, który może dokonać instalacji TOE w systemie, zakładać nowych użytkowników (S.USER) systemu oraz nadawać im prawa.
S.ATTACKER	Zakłada się, że napastnicy posiadają wysoki poziom umiejętności, wystarczające środki i głęboką motywację do przeprowadzenia ataku.

Kolejnym elementem bezpośrednio związanym z atakami napastników są zasoby TOE. Obejmują one zarówno dokumenty opracowane przez użytkownika, jak również zasoby systemowe, niezbędne do prawidłowego działania TOE.

Tabela 3

Przykład 5. Identyfikacja aktywów

Zasób	Opis zasobu
D.CRYPTO_API	Biblioteka systemowa wykonująca operacje kryptograficzne.
D.PRIV_KEY	Klucz prywatny używany podczas tworzenia podpisu cyfrowego, oraz deszyfrowania poufnych informacji.
D.PLAIN_DATA	Jawny dokument przeznaczony do podpisania lub zaszyfrowania.

Dla wymienionych zasobów istnieją bardziej i mniej realne zagrożenia, przed którymi należy je zabezpieczyć. Kolejnym etapem prac projektowych jest więc ich zidentyfikowanie z uwzględnieniem opisu metody i napastnika atakującego wybrane zasoby.

Tabela 4

Przykład 6. Identyfikacja zagrożeń

Zagrożenie	Opis zagrożenia
T.IMPERSON	Napastnik (S.ATTACKER) może uzyskać nieautoryzowany dostęp do informacji lub zasobu podszywając się pod autoryzowanego użytkownika TOE (S.USER).
T.MAL	Zasoby odpowiedzialne za wykonywanie operacji kryptograficznych (D.CRYPTO_API) mogą zostać zmodyfikowane przez intruzów autoryzowanych i nieautoryzowanych (S.ATTACKER), osłabiając działanie operacji kryptograficznych.
T.RND	Intruz (S.ATTACKER) może zdobyć klucz (D.PRIV_KEY) poprzez próbę odgadnięcia metodami statystycznymi liczby, z której wyprowadzono klucz; wymagana jest wiedza matematyczna, nie jest konieczna znajomość Przedmiotu Oceny; wyklucza się bezpośrednie włamanie, co zabezpiecza otoczenie (AE.LOCATE).

Ostatnim elementem identyfikującym otoczenie zabezpieczeń są polityki bezpieczeństwa, które mają za zadanie ustalenie zbioru reguł i procedur wspomagających zapewnienie bezpieczeństwa zasobów podczas eksploatacji TOE.

Tabela 5

Przykład 7. Identyfikacja polityk bezpieczeństwa

Polityka bezp.	Opis polityki bezpieczeństwa
P.ADMIN	Osoby odpowiedzialne za administrowanie systemem (S.ADMIN) zapewnią kontrolę dostępu do systemu operacyjnego (otoczenie TOE).
P.PASS	Użytkownicy TOE, jak również pozostali użytkownicy systemu operacyjnego (otoczenie TOE) zapewnią bezpieczne przechowywanie haseł dostępu do systemu.
P.USE	Osoby odpowiedzialne za TOE zapewnią, iż będzie on dostarczany, instalowany, zarządzany i obsługiwany w sposób gwarantujący utrzymanie bezpieczeństwa.

2.4. Cele zabezpieczenia

Zagrożenia wymagają postawienia celów wskazujących, w jakim stopniu potrzeby bezpieczeństwa zostaną zaspokojone przez Przedmiot Oceny (TOE), a w jakim przez jego otoczenie.

Cele zabezpieczenia TOE określają aspekty bezpieczeństwa przeciwstawiające się zagrożeniom (nie narzucając sposobu ich realizacji) przez sam Przedmiot Oceny.

Tabela 6

Przykład 8. Cele zabezpieczenia TOE

Cel zabezpieczenia	Opis celu zabezpieczenia
OT.CERTVAL	TOE zapewni środki kontroli ważności używanych certyfikatów.
OT.ENCRYPT	TOE zapewni środki do ochrony poufności informacji.
OT.INTEGRITY_ DATA	TOE zapewni środki do wykrywania utraty integralności informacji.

Cele zabezpieczenia otoczenia identyfikują środki przeciwstawiania się zagrożeniom oraz wspieranie polityk bezpieczeństwa, które nie są realizowane przez samo TOE, lecz przez środowisko teleinformatyczne lub pozatechniczne środki proceduralne.

Tabela 7

Przykład 9. Cele zabezpieczenia otoczenia TOE

Cel zabezpieczenia	Opis celu zabezpieczenia
OE.CRYPTSEC	Otoczenie TOE zapewni środki do wykonania bezpiecznych operacji kryptograficznych (włączając w to bezpieczeństwo przechowywanych kluczy prywatnych – D.PRIV_KEY) (zaufana biblioteka funkcji kryptograficznych).
OE.HRDACC	Otoczenie TOE zostanie zabezpieczone przed fizycznym dostępem (zamknięte pomieszczenie).
OT.INTEGRITY_ TOE	Otoczenie TOE umożliwi wykrycie utraty integralności TOE (podmiana elementów funkcjonalnych wchodzących w skład TOE).

2.5. Wymagania na zabezpieczenie IT

Kolejną częścią projektowania zadania zabezpieczeń jest identyfikacja wymagań na zabezpieczenie teleinformatyczne. Są one podzielone na wymagania dotyczące samego Przedmiotu Oceny, jak również te dotyczące jego środowiska, którym nie może przeciwstawić się sam Przedmiot Oceny.

Wymagania na zabezpieczenie TOE składają się z części dotyczącej jego funkcjonalności oraz części uzasadniającej zaufanie do zabezpieczeń. Wymagania funkcjonalne są formalnym przedstawieniem metod realizacji wyznaczonych celów, natomiast wymagania na uzasadnienie

zaufania definiują warunki, które musi spełnić TOE, aby uznać go za zgodny z wybranym poziomem uzasadnionego zaufania. Wyrażone są one za pomocą odpowiednich komponentów [2], [3].

Tabela 8

Przykład 10. Wymagania na uzasadnienie zaufania do zabezpieczenia TOE

Klasa	Komponenty uzasadnienia zaufania
ACM	ACM_CAP.3, ACM_SCP.1
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1

Przykład 11. Wymagania na zabezpieczenie otoczenia teleinformatycznego

RE.HRDACC - Otoczenie powinno być zabezpieczone przed fizycznym dostępem do TOE i jego otoczenia teleinformatycznego przez nieupoważnione osoby.

RE.CRYPTSEC - Otoczenie TOE dostarczy zestawu bezpiecznych funkcji kryptograficznych, w oparciu o które TOE wykonuje operacje na zasobach.

2.6. Zwięzła specyfikacja TOE

Celem tej części zadania zabezpieczeń jest przedstawienie charakterystycznych dla TOE rozwiązań spełniających potrzeby zabezpieczeń funkcjonalnych oraz uzasadniających zaufanie.

Przykład 12. Funkcje zabezpieczające TOE

F.INTEGR_DATA - Sprawdzenie integralności danych

Dane, które mają być kontrolowane, zostają podpisane. Następnie, ażeby sprawdzić autentyczność danych, wywoływana jest funkcja, w wyniku której użytkownik dokonujący sprawdzenia integralności informowany jest o tym, czy podpis znajdujący się w pliku jest identyczny z tym obliczonym podczas weryfikacji. (...).

F. AUTENTH_DATA - Zapewnienie poufności informacji

W celu zapewnienia poufności chronione informacje są szyfrowane. Ponowne ujawnienie danych możliwe jest po ich odszyfrowaniu. Proces szyfrowania i odszyfrowania realizowany jest przez systemową bibliotekę funkcji kryptograficznych (...).

2.7. Uzasadnienie Zadania Zabezpieczeń

Kolejnym elementem projektu jest wykazanie, że Przedmiot Oceny dostarczy odpowiednich środków zapewniających bezpieczeństwo teleinformatyczne.

2.7.1. Uzasadnienie celów zabezpieczenia w Zadaniu Zabezpieczeń

Słuszności zastosowanych celów zabezpieczenia w świetle przewidywanych zagrożeń, wyznaczonych polityk bezpieczeństwa oraz założeń postawionych otoczeniu TOE można przedstawić za pomocą tabeli z odwołaniami skrośnymi z nieformalnym uzasadnieniem zależności w niej przedstawionych.

2.7.2. Uzasadnienie wymagań funkcjonalnych na zabezpieczenie

Celem tego etapu uzasadnienia jest wykazanie, że wymagania na zabezpieczenia są odpowiednie do spełnienia postawionych celów zabezpieczenia TOE oraz jego otoczenia. Uzasadnienie użycia komponentów funkcjonalnych powinno być też poparte przedstawieniem wzajemnej spójności i wspierania się celów oraz wymagań TOE i jego otoczenia.

Tabela 9

Przykład 13. Wspieranie celów i wymagań funkcjonalnych w TOE i jego otoczeniu

Cel zabezpieczenia		Realizowany przez	
TOE	wspomagany przez otoczenie	komponent	wspomagany przez wymaganie dotyczące otoczenia
OT.ENCRYPT	OE.CRYPTSEC OE.NON_REP OE.INTEGRITY_TOE	FDP_UCT.1	RE.CRYPTSEC RE.NON_REP RE.INTEGRITY_TOE
OT.CERTVAL	OE.CRYPTSEC	FMT_MTD.1	RE.CRYPTSEC

2.7.3. Uzasadnienie użycia komponentów uzasadniających zaufanie i zwięzłej specyfikacji Przedmiotu Oceny

Ostatnim etapem występującym w Zadaniu Zabezpieczeń jest wykazanie, że użyte komponenty uzasadniające zaufanie są wystarczające, nie nadmiarowe i osiągalne, oraz uzasadniające zwięzłą specyfikację TOE. Pokazuje ono, że funkcje zabezpieczające TOE i środki uzasadniające zaufanie są odpowiednie do spełnienia wymagań funkcjonalnych TOE.

Tabela 10

Przykład 14. Uzasadnienie zwięzłej specyfikacji Przedmiotu Oceny

Funkcja bezpieczeństwa	Wymagania funkcjonalne
F.INTEGR_DATA	FDP_DAU.2 FDP_SDI.1 FDP_UIT.1
F. AUTENTH_DATA	FDP_UCT.1

3. Wnioski i uwagi końcowe

Przedstawiony artykuł jest skrótem przykładu tworzenia zabezpieczeń teleinformatycznych w oparciu o Wspólne Kryteria. Dokument ST przygotowany na podstawie przytoczonych norm może zostać oceniony, a następnie można dokonywać jednoznacznego porównania wykonanego produktu z innymi produktami o tym samym przeznaczeniu. Wynik oceny może też być podstawą do wystąpienia o certyfikat dla danego produktu. Stosowanie Wspólnych Kryteriów ma na celu ujednolicenie sposobów projektowania i oceny zabezpieczeń oraz wydawania certyfikatów w różnych krajach, co byłoby niemożliwe przy użyciu odrębnych norm lokalnych [5], [6], [7].

LITERATURA

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, v.2.1, August 1999.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, v.2.1, August 1999.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v.2.1, August 1999.
4. ISO/IEC PDTR 15446, Information technology – Security techniques – Guide for the production of protection profiles and security targets, v.0.9, January 2000.
5. Information Technology Security Evaluation Criteria (ITSEC), EGKS-EWG-EAG, Bruessel, Juni 1991.
6. Trusted Computer System Evaluation Criteria „Orange Book"/Federal Criteria for IT Security (TCSEC/FC).
7. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).
8. Praca zbiorowa pod red. Białasa A.: Metodyka projektowania zabezpieczeń teleinformatycznych, Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, Instytut Systemów Sterowania, Chorzów 2002.

Recenzent: Dr inż. Adam Ziąbiński

Wpłynęło do Redakcji 5 kwietnia 2003 r.

Abstract

The paper presents using of methodology of IT security based on the "Common Criteria for IT Security Evaluation" (ISO/IEC 15408), on an example of SecOffice – application for digital signature and encryption of electronic documents (figure 1 present structure of the application). The article presents following steps of creating Security Target document. The first step is the Target of Evaluation and its environment identification (tables 1-5). In the next step a definition of security objectives should be done (example in tables 6, 7). The last step is a justification of used requirements in the context of objectives and threats (example in tables 8 - 10). Important part of ST is the TOE description. It helps to determine TOE and its environment boundaries, what shows figure 2. The document created in compliance with described standards may be evaluated. Evaluation results can be used for comparison of products intended for the same purposes and can be the basis for certificate process request for any product. Using of Common Criteria uniforming means of evaluation and certification in different countries.

Adres

Krzysztof FAŁEK: Instytut Systemów Sterowania, ul. Długa 1-3, 41-506 Chorzów, Polska, kfalek@iss.pl .