CERTYFIKACJA W ZAKRESIE „COMMON CRITERIA" – WSTĘPNA KONCEPCJA BUDOWY POLSKIEGO MODELU BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Remigiusz Lewandowski

Uniwersytet Mikołaja Kopernika w Toruniu

Streszczenie: W artykule przedstawiono zagadnienie weryfikacji bezpieczeństwa systemów teleinformatycznych w oparciu o normę „common criteria". Stanowi ona obecnie międzynarodowy standard m.in. w odniesieniu do dokumentów elektronicznych. Z tego względu zarówno sama norma, jak i model certyfikacji w zakresie „common criteria" mają fundamentalne znaczenie dla bezpieczeństwa państwa, a w szczególności bezpieczeństwa identyfikacyjnego obywateli. Analiza modelu certyfikacji w zakresie „common criteria" oraz relacja tej certyfikacji z bezpieczeństwem państwa prowadzi do wniosku o konieczności stworzenia w Polsce struktur organizacyjnych zapewniających przedmiotową certyfikację. W artykule zaprezentowano propozycję krajowego modelu bezpieczeństwa teleinformatycznego w oparciu o certyfikację „common criteria". W modelu tym kluczowe funkcje pełnią Polskie Centrum Akredytacji, Agencja Bezpieczeństwa Wewnętrznego (lub Narodowe Centrum Kryptologii) oraz Centralny Ośrodek Informatyki (lub Instytut Maszyn Matematycznych).
Słowa kluczowe: bezpieczeństwo państwa, bezpieczeństwo systemów teleinformatycznych, „common criteria".

„Common Criteria" (CC) to norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych. CC udostępnia procedury umożliwiające zdefiniowanie zagrożeń oraz zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania w produkcie. Certyfikacją według normy CC zajmują się niezależne, akredytowane laboratoria badawcze na całym świecie.

Jednym z elementów procesu certyfikacji jest tzw. „profil ochrony" (PP – *protection profile*), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat potwierdzający ich faktyczną skuteczność. Proces certyfikacji może być prowadzony według różnych poziomów szczegółowości i weryfikacji formalnej (EAL – *Evaluation Assurance Level*), począwszy od EAL1 (tylko testy funkcjonalne) aż do EAL7 (formalna weryfikacja projektu oraz testy).

Zgodnie z decyzją Komisji Europejskiej z dnia 28 czerwca 2006 r. ustanawiającą specyfikacje techniczne dla norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie, „mikroprocesory zastosowane w paszportach muszą być oceniane zgodnie z odpowiednim profilem zabezpieczeń opartym na wspólnych kryteriach". Wymóg ten dotyczy również podpisu elektronicznego, na podstawie *Rozporządzenia Rady Ministrów w sprawie określenia warunków technicznych i organizacyjnych dla*

kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego. Norma CC staje się zatem powszechnym standardem w zakresie bezpieczeństwa systemów teleinformatycznych, a w praktyce status taki uzyskała w odniesieniu do systemów związanych z funkcjonowaniem administracji publicznej oraz w przypadku dokumentów elektronicznych[1]. W przypadku Polski certyfikat CC został przyznany m.in. apletowi do obsługi danych biometrycznych z BAC/EAC/SAC (SmartApp ID 3.1)[2] czy też apletowi do obsługi podpisu elektronicznego (SmartApp SIGN 2.2)[3].

Oba certyfikaty przyznane zostały przez niemiecki Bundesamt für Sicherheit in der Informationstechnik (BSI), a testy wykonały francuskie i niemieckie laboratoria. Wydaje się, że – z uwagi na znaczenie przedmiotowej certyfikacji dla bezpieczeństwa narodowego w przypadku dokumentów państwowych (np. paszportów biometrycznych) – jej realizacja powinna być domeną polskiego organu odpowiedzialnego za sferę bezpieczeństwa państwa w obszarze teleinformatyki.

Praktyka oraz literatura przedmiotu wskazują, że działalność w zakresie oceny i certyfikacji bezpieczeństwa produktów i systemów sektora ICT ma charakter strategiczny dla państwa i podlega szczególnej ochronie z jego strony (np. przed przejęciem kontroli przedsiębiorstwa prowadzącego taką działalność przez podmioty zagraniczne)[4]. Tego rodzaju ochrona może mieć np. formę prowadzonej przez państwo procedury autoryzacji inwestorów zagranicznych w odniesieniu do przedsiębiorstw działających w zakresie testowania i certyfikacji bezpieczeństwa produktów i systemów teleinformatycznych, co znalazło choćby zastosowanie we Francji[5]. Potwierdza to tezę, że kontrola państwa nad omawianym obszarem testowania i certyfikacji (także w zakresie CC) ma istotne znaczenie dla bezpieczeństwa narodowego. Dokumenty zawierające warstwę elektroniczną oraz związane z bezpieczeństwem państwa systemy teleinformatyczne wymagają odpowiedniej wiarygodności. Tworzy ją z jednej strony sam producent (w oparciu o swój profesjonalizm i odpowiednio skonstruowane procesy wewnętrzne), a z drugiej państwo – poprzez właściwe regulacje[6], w tym także dotyczące nadzoru (również organizacyjno-kapitałowego) nad działalnością certyfikacyjną w zakresie CC. Certyfikacja w zakresie CC

[1] P. Śniecikowski, PWPW *Smartapp-ID 3.1 (IFX) – rozwiązanie dla trzeciej generacji paszportów biometrycznych,* „Człowiek i Dokumenty" nr 36/2015, s. 14.

[2] http://www.commoncriteriaportal.org/files/epfiles/0898a_pdf.pdf

[3] http://www.commoncriteriaportal.org/files/epfiles/0694a_pdf.pdf

[4] L. Olszewski, *Strategiczne sektory w rozwoju współczesnej gospodarki narodowej*, [w:] J. Blicharz, *Prawne aspekty prywatyzacji*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wrocław 2012, s. 548-549.

[5] Décret No 2005-1739.

[6] R. Lewandowski, *Wiarygodność procesów identyfikacji i transakcji a system bezpieczeństwa państwa,* „Bezpieczeństwo. Teoria i Praktyka", nr 1 (XIV)/2014, s. 46.

odnosząca się do dokumentów elektronicznych ma ponadto kluczowe znaczenie dla bezpieczeństwa identyfikacyjnego obywateli, rozumianego jako stan niezakłóconego funkcjonowania państwa w obszarze obejmującym[7]:

1) prawidłową weryfikację deklarowanej tożsamości osób,
2) weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się ona posługuje,
3) obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość lub określone uprawnienia,
4) ochronę obywateli przed kradzieżą tożsamości.

Model funkcjonowania

Zasady współpracy międzynarodowej w obszarze Common Criteria (wydawanie certyfikatów bezpieczeństwa dla wybranych produktów teleinformatycznych przez instytucje certyfikujące poszczególnych krajów w oparciu o normę ISO 15408; dalej: CC) reguluje stosowne porozumienie (*Arrangement on the Recognition of Common Criteria Certificates*[8]). Jego podstawowym celem jest zapewnienie wzajemnej uznawalności tych certyfikatów.

Członkami (stronami) Porozumienia są instytucje autoryzujące (*Certificate Authorising Participants*) z podległymi organami certyfikującymi (*Certification/Validation Bodies*, dalej: CB). Mogą one mieć formę wyłącznie instytucji lub agend rządowych. Przystąpienie do Porozumienia następuje na pisemny wniosek po spełnieniu określonych wymogów (m.in. bezstronność i niezależność od podmiotów zgłaszających wnioski o certyfikację produktów) i uzyskaniu jednomyślnej zgody dotychczasowych członków.

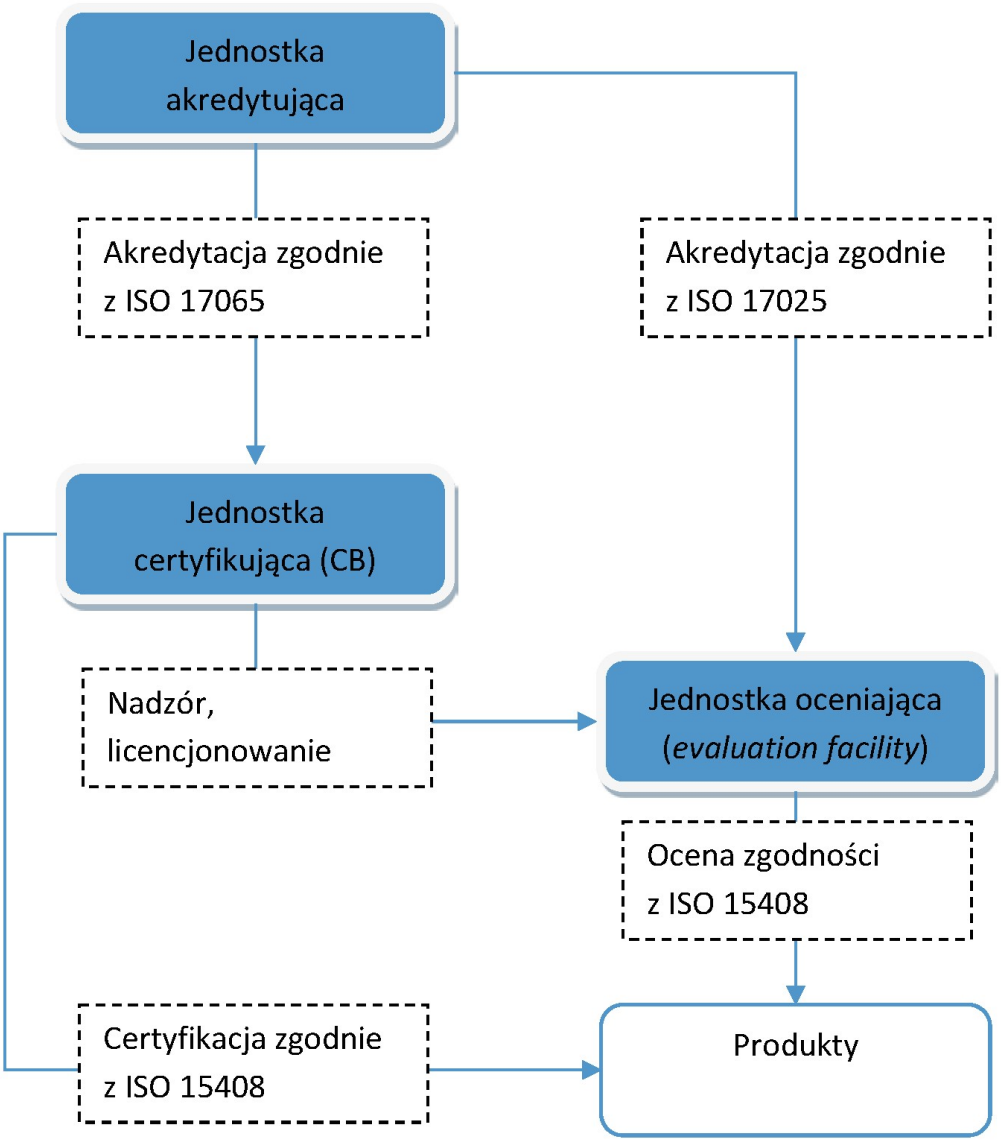
Jednym z zadań organów certyfikujących (CB) jest akredytacja zewnętrznych laboratoriów (*evaluation facility* – jednostka oceniająca) przeprowadzających testy ewaluacyjne na zgodność z CC. Laboratoria te muszą w szczególności spełniać wymogi przewidziane normą ISO 17025 (ogólne wymagania dotyczące laboratoriów badawczych i wzorcujących). Możliwe jest również przystąpienie do Porozumienia bez prawa do akredytowania laboratoriów i wystawiania certyfikatów (*Certificate Consuming Participant*).

---

[7] R. Lewandowski, T. Goliński, *Nielegalna migracja a bezpieczeństwo identyfikacyjne*, [w:] M. Tomaszewska-Michalak, T. Tomaszewski (red.), *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warszawa 2015, s. 112.

[8] http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf

Stronami Porozumienia – w zakresie akredytowania laboratoriów i wystawiania certyfikatów – są: Australia, Kanada, Francja, Niemcy, Indie, Włochy, Japonia, Malezja, Holandia, Nowa Zelandia, Norwegia, Korea, Hiszpania, Szwecja, Turcja, Wielka Brytania oraz Stany Zjednoczone. Stronami Porozumienia – z wyłączeniem akredytowania laboratoriów i wystawiania certyfikatów – są: Austria, Czechy, Dania, Finlandia, Grecja, Izrael, Pakistan oraz Singapur[9]. Model funkcjonowania certyfikacji przedstawiono na rys. nr 1.



Rys. 1. Ogólny model certyfikacji w zakresie CC
Źródło: opracowanie własne

[9] http://www.commoncriteriaportal.org/ccra/members/

W modelu certyfikacji CC uczestniczą trzy istotne instytucje:
1) jednostka akredytująca (*accreditation body*),
2) jednostka certyfikująca (*certification body*),
3) jednostka oceniająca/laboratorium (*evaluation facility*).

Jednostka akredytująca i certyfikująca

Jednostka akredytująca odpowiada za nadzór nad krajowym systemem norm i oceny zgodności. Działalność jednostki obejmuje całość zagadnień związanych z normami ISO i nie jest ograniczona do kwestii Common Criteria. W Polsce zadania te wykonuje Polskie Centrum Akredytacji przy Ministerstwie Gospodarki.

Jednostka certyfikująca odpowiada za nadzór nad krajowym systemem Common Criteria. Powinna być akredytowana zgodnie z 17065 (Ocena zgodności – Wymagania dla jednostek certyfikujących wyroby, procesy i usługi) przez właściwą jednostkę akredytującą lub funkcjonować na podstawie przepisów prawa. Jednostka certyfikacyjna jest podmiotem wystawiającym certyfikaty Common Criteria. W Polsce brakuje tego rodzaju podmiotu. W państwach-stronach Porozumienia jednostkami certyfikującymi są na przykład:
1) Bundesamt für Sicherheit in der Informationstechnik (Niemcy),
2) National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme, działające w ramach National Security Agency (USA),
3) Norwegian Certification Authority for IT Security, działające w ramach Norwegian National Security Authority (Norwegia).

Analiza jednostek certyfikujących w państwach-stronach Porozumienia wskazuje, że co do zasady są to jednostki ulokowane w strukturach organów państwa odpowiedzialnych za jego bezpieczeństwo lub w szczególności za jego bezpieczeństwo teleinformatyczne. Porozumienie wskazuje, że „działalność jednostek certyfikujących zarówno o wielorakim charakterze, jak i o wyłącznie komercyjnym charakterze nie jest zgodna z duchem Porozumienia, który – obok zgodności z określonymi standardami – wymaga obopólnego zrozumienia i zaufania pomiędzy organizacjami rządowymi" oraz że omawiana działalność „nie może uwzględniać wielorakich oraz wyłącznie komercyjnych jednostek certyfikujących" (s. 5). Niemniej jednak w Holandii funkcję jednostki certyfikującej pełni Netherlands Scheme for Certification in the Area of IT Security (NSCIB) w ramach rządowego organu Netherlands National Communications Security Agency (NLNCSA), który omawiane zadania podzlecił podmiotowi komercyjnemu, tj. TÜV Rheinland Nederland B.V[10]. Jest to jedyny taki przypadek w wykazie jednostek certyfikujących w ramach Porozumienia.

[10] http://www.tuv.com/en/netherlands/home.jsp.

Porozumienie precyzuje szereg wymagań w odniesieniu do jednostki certyfikującej. Zgodnie z nimi:

1) Usługi jednostki certyfikującej (CB) mają być dostępne bez nienależnych finansowych lub innych warunków. Procedury, według których CB pełni działalność, będą administrowane w sposób niedyskryminujący.
2) CB ma być bezstronna. W szczególności powinna dysponować stałym personelem odpowiedzialnym przed kierownictwem wyższego szczebla, co ma umożliwić codzienną działalność prowadzoną bez nienależnego wpływu lub kontroli przez kogokolwiek mającego handlowe lub finansowe korzyści w certyfikacji/walidacji.
3) CB ma posiadać i udostępniać na żądanie:
   a) schemat czytelnie przedstawiający odpowiedzialność i strukturę sprawozdawczą organizacji,
   b) opis sposobów, za pomocą których organizacja uzyskuje wsparcie finansowe,
   c) dokumentację opisującą Schemat Oceny oraz Certyfikacji/Walidacji oraz
   d) dokumentację czytelnie wskazującą na jej status prawny.
4) Pracownicy CB mają być kompetentni w zakresie funkcji, które pełnią. Informacja o właściwych kwalifikacjach, szkoleniach i doświadczeniu każdego z pracowników ma być przechowywana i uaktualniana przez CB. Pracownikom mają zostać udostępnione czytelne, aktualne i udokumentowane instrukcje odnoszące się do ich obowiązków i odpowiedzialności.
5) CB ma utrzymywać system do kontroli całej dokumentacji związanej ze Schematem Oceny i Certyfikacji/Walidacji i zapewnić, że:
   a) aktualne wydanie odpowiedniej dokumentacji jest dostępne we wszystkich istotnych lokalizacjach;
   b) dokumenty nie są poprawiane lub zastępowane bez właściwej autoryzacji;
   c) zmiany są ogłaszane w taki sposób, że ci, którzy powinni o tym wiedzieć, są szybko informowani i mogą podjąć szybkie i efektywne działania;
   d) zastąpione dokumenty są usuwane z użytkowania z całej organizacji i jej jednostek;
   e) ci, którzy są bezpośrednio zainteresowani Schematem, są informowani o zmianach.
6) CB ma dysponować wymaganymi pomieszczeniami i udokumentowanymi procedurami, aby umożliwić przeprowadzanie w sposób właściwy Certyfikacji/Walidacji Produktu Informatycznego lub Profilu Zabezpieczeń zgodnie z CC oraz powiązanymi Metodami Oceny (to jest CEM, Dokumenty Wspierające CC).
7) CB ma zapewnić, że Jednostki Oceniające Bezpieczeństwo Informatyczne (*Evaluation Facilities*) są zgodne z wymaganiami określonymi w Porozumieniu.

8) CB ma sporządzić dla każdej Jednostki Oceniającej Bezpieczeństwo Informatyczne właściwie udokumentowane porozumienie, obejmujące wszystkie stosowne procedury, włączając uzgodnienia zapewniające zachowanie tajemnicy Informacji Chronionych oraz Procesów Oceny i Certyfikacji/Walidacji.
9) CB ma posiadać Księgę Jakości i dokumentację przedstawiające procedury, dzięki którym jest zgodna z wymaganiami. Mają one zawierać co najmniej:
   a) politykę utrzymania jakości,
   b) zwięzły opis statusu prawnego CB,
   c) nazwiska, kwalifikacje i obowiązki kadry kierowniczej oraz pozostałych pracowników certyfikujących/walidujących,
   d) szczegóły dotyczące uzgodnień szkoleniowych dla pracowników certyfikujących/walidujących,
   e) schemat organizacyjny przedstawiający hierarchię służbową, odpowiedzialność i podział funkcji począwszy od kadry kierowniczej,
   f) szczegóły dotyczące procedur związanych z Monitoringiem Produktów IT lub Oceną Profilu Zabezpieczeń,
   g) szczegóły dotyczące procedur związanych z ochroną nadużyć Certyfikatów CC,
   h) dane identyfikacyjne kooperantów oraz szczegóły udokumentowanych procedur dotyczących oszacowania i monitorowania ich kompetencji oraz
   i) szczegóły jakichkolwiek procedur dotyczących odwołań lub ugód.
10) W zakresie dozwolonym przez prawo krajowe, statuty, rozporządzenia wykonawcze lub regulacje uczestników, CB powinna posiadać stosowne uzgodnienia dla zapewnienia poufności informacji pozyskanych w toku działalności Certyfikacji/Walidacji na wszystkich szczeblach organizacji i nie ma możliwości nieuprawnionego ujawniania Informacji Chronionych uzyskanych w toku działalności Certyfikacji/Walidacji zgodnie z tym Porozumieniem.
11) CB ma sporządzić oraz będzie uaktualniać w miarę potrzeb Listę Produktów Certyfikowanych/Walidowanych. Każdy Produkt Informatyczny lub Profil Zabezpieczeń wymieniony na liście ma być jasno zidentyfikowany. Lista ma być publicznie dostępna.
12) CB ma posiadać procedury związane z rozwiązywaniem sporów między własną jednostką, związanymi Jednostkami Oceniającymi Bezpieczeństwo Technologii Informatycznej (ITSEF) i ich Klientami.
13) CB ma przeprowadzać przeglądy zarządzania jej Schematem, tak aby zapewnić, że wypełnia cele tego Porozumienia.
14) CB ma sprawować właściwą kontrolę nad stosowaniem Certyfikatów Common Criteria. Jest zobowiązana podejmować stosowne administracyjne, proceduralne i prawne kroki w celu przeciwdziałania lub przeciwstawiania

się niewłaściwemu użyciu certyfikatów oraz dokonywać korekty fałszywych, mylnych lub niewłaściwych oświadczeń o certyfikatach lub o Schemacie Oceny i Certyfikacji/Walidacji.

15) CB ma posiadać udokumentowane procedury dotyczące wycofywania Certyfikatów Common Criteria i publikowania tych unieważnień w kolejnym wydaniu Listy Produktów Certyfikowanych/Walidowanych.

Jednostka oceniająca

Jednostka oceniająca odpowiada za ocenę (testy) produktów na zgodność z normą ISO 15408 (*Kryteria oceny zabezpieczeń informatycznych*). Prowadzenie jednostki oceniającej wymaga wcześniejszej akredytacji zgodnie z ISO 17025 (*Ogólne wymagania dotyczące laboratoriów badawczych i wzorcujących*) przez właściwą jednostkę akredytującą oraz dopuszczenia przez jednostkę certyfikującą. Na świecie są 63 takie akredytowane laboratoria[11]. W Polsce nie działa żadna jednostka oceniająca.

Wymogi dotyczące jednostki oceniającej zawarte są w normie ISO 17025. Struktura normy składa się z dwóch zasadniczych elementów:

1) rozdziału czwartego, w którym podano wymagania dla właściwego systemu zarządzania, a więc:
   a) nadzoru nad dokumentami,
   b) przeglądu zamówień ofert i umów,
   c) podwykonawstwa badań i wzorcowań,
   d) zakupu usług i dostaw,
   e) obsługi klienta i skarg,
   f) nadzorowania niezgodnych z wymaganiami badań i/lub wzorcowań,
   g) audytów wewnętrznych oraz działań korygujących i zapobiegawczych,
   h) nadzoru nad zapisami oraz przeglądu zarządzania
2) oraz rozdziału piątego, zawierającego wymagania związane z kompetencjami technicznymi laboratorium, które dotyczą:
   a) personelu (m.in. odpowiednie kompetencje i kwalifikacje; sformułowane cele dotyczące wykształcenia, szkolenia i umiejętności; ustalenia zapewniające niezależność kierownictwa i personelu od jakichkolwiek komercyjnych, finansowych lub innych nacisków i wpływów wewnętrznych i zewnętrznych, które mogłyby niekorzystnie oddziaływać na jakość ich pracy),
   b) wyposażenia (m.in. laboratorium powinno być wyposażone we wszystkie elementy niezbędne do prawidłowego przeprowadzenia badania; wyposażenie i jego oprogramowanie powinno zapewniać wymaganą dokładność oraz spełniać odpowiednie specyfikacje dotyczące badań;

[11] http://www.commoncriteriaportal.org/labs/.

każdy obiekt wyposażenia istotny dla wyników oraz oprogramowanie używane do badań powinny być jednoznacznie zidentyfikowane, laboratorium powinno mieć procedury dotyczące bezpiecznego postępowania i konserwacji wyposażenia),

c) warunków lokalowych i środowiskowych,
d) spójności pomiarowej,
e) metod badania i wzorcowania oraz ich walidacji (m.in. właściwe metody i procedury spełniające wymagania klienta, z preferencją dla metod opublikowanych w normach międzynarodowych, regionalnych lub krajowych; w przypadku metod nieznormalizowanych – konieczność wcześniejszego ich zwalidowania),
f) pobierania próbek,
g) postępowania z obiektami do badań i wzorcowań (m.in. obliczenia i przenoszenia danych powinny być w sposób systematyczny poddawane właściwym sprawdzeniom, a stosowane oprogramowanie komputerowe odpowiednio zwalidowane jako przydatne do użytku i zapewniające integralność danych; powinny być ustanowione i wdrożone procedury dotyczące ochrony danych),
h) zapewnienia jakości wyników badań i wzorcowania,
i) przedstawiania wyników.

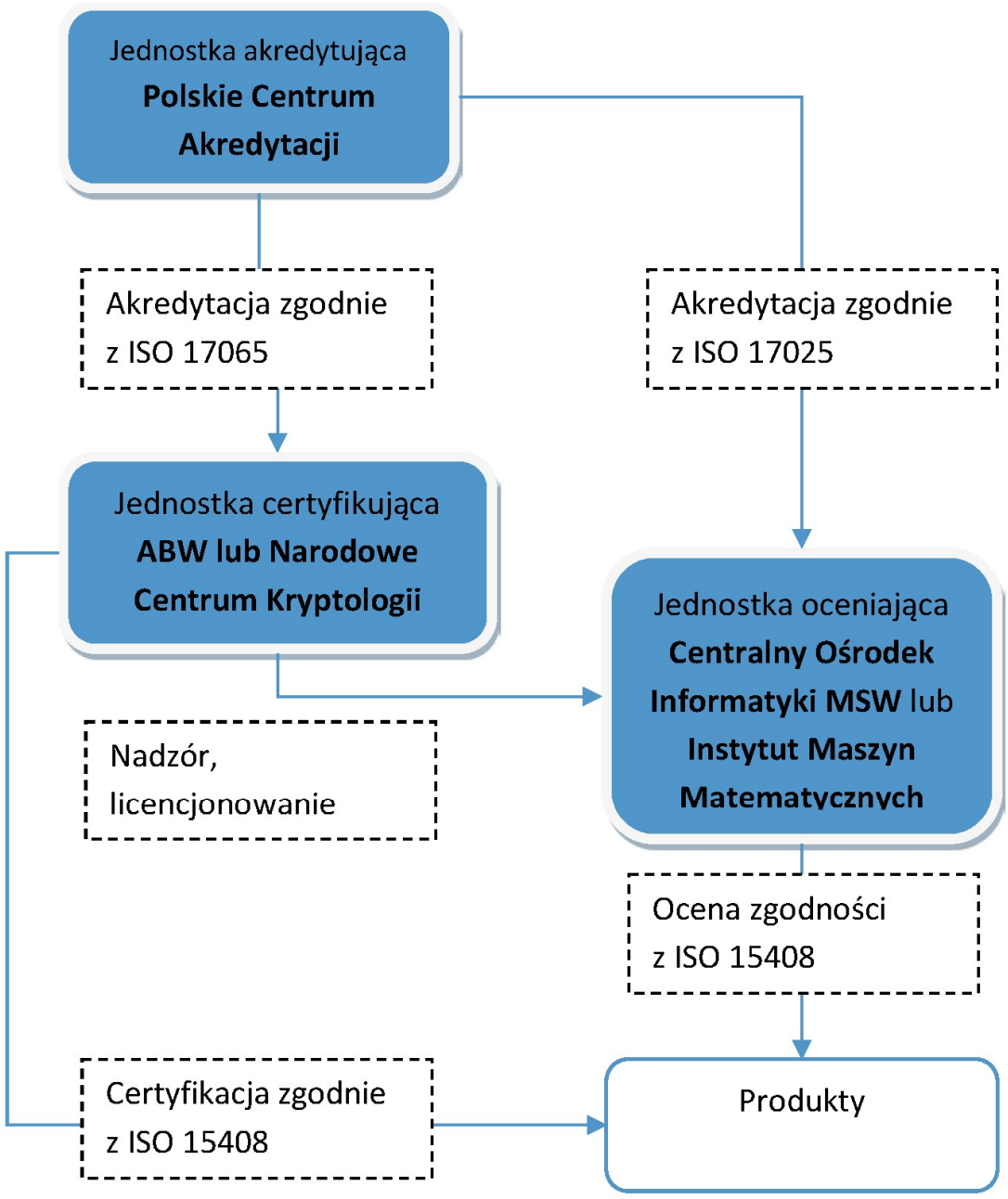
Rozdziały 4 i 5 odnoszą się do wymagań, jakie musi spełnić laboratorium, by uzyskać akredytację. Laboratorium, które wdrożyło ISO 17025, jest w stanie zapewnić, że wykonywane przez nie badania i wzorcowania są zgodne z systemem jakości, a otrzymywane wyniki są miarodajne, charakteryzują się rzetelnością i dokładnością.

Badania i wzorcowania, jakie wykonują laboratoria, stanowią kombinację metod znormalizowanych i nieznormalizowanych oraz własnych – opracowanych przez te jednostki. Zgodnie z normą ISO 17025 laboratorium powinno wykonywać badania i wzorcowania, posługując się do tego celu wykwalifikowanym personelem, sprawną aparaturą badawczą oraz udokumentowanymi procedurami, a także podejmować właściwe metody badań i wzorcowań spełniające wymagania klienta.

Implementacja modelu w Polsce

Implementacja modelu w zakresie certyfikacji CC wymaga nadania odpowiednich uprawnień w tym zakresie wybranym instytucjom i wypracowania koniecznych kompetencji. Biorąc pod uwagę istniejące w Polsce instytucje odpowiedzialne za omawiane sfery, zaproponować można model, w którym funkcję jednostki akredytującej pełni – zgodnie z aktualnymi kompetencjami – Polskie Centrum Akredytacji, rolę jednostki certyfikującej pełni Agencja Bezpieczeństwa Wewnętrznego lub Narodowe

Centrum Kryptologii, zaś rolę jednostki oceniającej Centralny Ośrodek Informatyki MSW. Na rys. 2 przedstawiono omawiany model w warunkach polskich.



Rys. 2. Projekt modelu certyfikacji w zakresie CC w warunkach polskich
Źródło: opracowanie własne

Polskie Centrum Akredytacji jest krajową jednostką akredytującą upoważnioną do akredytacji jednostek oceniających zgodność na podstawie ustawy z dnia 30 sierpnia 2002 r. o systemie oceny zgodności[12]. Zadania przewidziane zatem w modelu przedstawionym na schemacie 2 wynikają z ustawowych oraz statutowych zadań PCA.

[12] http://www.pca.gov.pl/?page=status_prawny.

Jednym z obszarów aktywności Agencji Bezpieczeństwa Wewnętrznego jest działalność profilaktyczna, której celem jest zapewnienie ochrony szczególnie wrażliwym sferom funkcjonowania państwa i gospodarki. Obejmuje ona także m.in. systemy certyfikowania, w tym w zakresie bezpieczeństwa przemysłowego.

Natomiast zgodnie ze statutem, do zadań Narodowego Centrum Kryptologii w szczególności należy[13]:

1) realizacja zadań związanych z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem oraz ochroną narodowych technologii kryptologicznych;
2) osiągnięcie oraz utrzymanie potencjału i kompetencji w zakresie:
   a) budowy urządzeń i narzędzi kryptograficznych służących do przetwarzania informacji niejawnych oraz innych posiadających zdolności kryptograficzne,
   b) wytworzenia rozwiązań do pełnej ochrony i zabezpieczenia informacji i przekazu wraz z możliwością przygotowania zasad wdrożenia i produkcji.

Wydaje się zatem, że zarówno ABW, jak i NCR są instytucjami predestynowanymi do realizacji funkcji jednostki certyfikującej w zakresie CC i posiadają odpowiednie kompetencje w tym zakresie.

Do statutowych zadań Centralnego Ośrodka Informatyki MSW (COI) należy m.in.: odpłatne wykonywanie usług na rzecz innych podmiotów[14], w tym:

1) jednostek administracji publicznej w zakresie utrzymania, serwisu, budowy, rozwoju i eksploatacji systemów informatycznych i teleinformatycznych,
2) wykonywanie innych zadań z zakresu informatyki, telekomunikacji i teleinformatyki oraz zarządzania informacją na rzecz osób trzecich, na podstawie odrębnych umów.

COI mogłoby zatem zapewnić realizację usług w zakresie oceny (testów) produktów na zgodność z normą ISO 15408. Należy jednak zaznaczyć, że zgodnie z normą ISO 15408, „organizator powinien mieć ustalenia zapewniające niezależność kierownictwa i personelu od komercyjnych, finansowych lub innych wewnętrznych i zewnętrznych nacisków, które mogłyby niekorzystnie oddziaływać na jakość ich pracy". Alternatywę dla COI w obszarze oceny (testów) produktów na zgodność z normą ISO 15408 (tj. funkcji jednostki oceniającej) może stanowić Instytut Maszyn Matematycznych (IMM). Do statutowych zadań IMM należy m.in. prowadzenie badań naukowych i prac rozwojowych w zakresie[15]:

---

[13] http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-121-zarzadzenie-nr-10mon-z-dnia-29-kwietnia-2013-r-w-sprawie-utworzenia-i-nadania-statutu-panstwowej-jednostce-budzetowej-narodowe-centrum/.

[14] http://coi.ssdip.bip.gov.pl/statut/376_statut-centralnego-osrodka-informatyki.html.

[15] www.imm.org.pl/imm/plik/pliki-do-pobrania-statut2011_nn33.pdf.

1) badań oraz analizy technologii i technik informatycznych,
2) innowacyjnych technologii informatycznych stosowanych w zarządzaniu informacją,
3) oprogramowania przeznaczonego dla administracji państwowej,
4) unifikacji i normalizacji.

Podsumowanie

Obywatele, urzędy administracji publicznej oraz podmioty gospodarcze na co dzień korzystają z usług i produktów informatycznych, które wiążą się z bezpieczeństwem identyfikacyjnym, bezpieczeństwem transakcji czy szerzej – bezpieczeństwem państwa. Dotyczy to choćby podpisu elektronicznego, ale również coraz szerszej gamy dokumentów elektronicznych. Paszport biometryczny i karta pobytu to przykłady takich dokumentów funkcjonujących w Polsce. Projektowane są również kolejne dokumenty, jak elektroniczna karta ubezpieczenia zdrowotnego, karta specjalisty medycznego czy karta specjalisty administracyjnego. Nie ma także odwrotu od koncepcji elektronicznego dowodu osobistego (choć odrębnym zagadnieniem pozostaje zasadność emisji karty ubezpieczenia zdrowotnego, podczas gdy funkcjonalność tę może realizować właśnie dowód osobisty). Z uwagi na wielkość naszego państwa i skalę zastosowania omawianych rozwiązań informatycznych (w tym dokumentów elektronicznych) zasadne jest utworzenie własnego krajowego systemu certyfikacji w zakresie Common Criteria. Raz jeszcze podkreślić należy, że ocena i certyfikacja bezpieczeństwa produktów i systemów sektora teleinformatycznego mają charakter strategiczny z punktu widzenia bezpieczeństwa państwa. Korzystanie z obcych jednostek certyfikujących może osłabiać to bezpieczeństwo i generować dla państwa oraz obywateli ryzyko. Zaproponowane w artykule rozwiązania implementacyjne stanowią próbę odpowiedzi na to wyzwanie.

LITERATURA:

1. R. Lewandowski, *Wiarygodność procesów identyfikacji i transakcji a system bezpieczeństwa państwa*, „Bezpieczeństwo. Teoria i Praktyka", nr 1 (XIV)/2014.
2. R. Lewandowski, T. Goliński, *Nielegalna migracja a bezpieczeństwo identyfikacyjne*, [w:] M. Tomaszewska-Michalak, T. Tomaszewski (red.), *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, Stowarzyszenie Absolwentów Wydziału Prawa i Administracji UW, Warszawa 2015.
3. L. Olszewski, *Strategiczne sektory w rozwoju współczesnej gospodarki narodowej*, [w:] J. Blicharz, *Prawne aspekty prywatyzacji*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wrocław 2012.
4. P. Śniecikowski, *PWPW Smartapp-ID 3.1 (IFX) – rozwiązanie dla trzeciej generacji paszportów biometrycznych*, „Człowiek i Dokumenty" nr 36/2015.
5. Décret Nº 2005-1739.

6. http://www.commoncriteriaportal.org/files/epfiles/0898a_pdf.pdf (pobrano: 1.06.2015).
7. http://www.commoncriteriaportal.org/files/epfiles/0694a_pdf.pdf (pobrano: 1.06.2015).
8. http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-121-zarzadzenie-nr-10mon-z-dnia-29-kwietnia-2013-r-w-sprawie-utworzenia-i-nadania-statutu-panstwowej-jednostce-budzetowej-narodowe-centrum/ (pobrano: 1.06.2015).
9. http://coi.ssdip.bip.gov.pl/statut/376_statut-centralnego-osrodka-informatyki.html (pobrano: 1.06.2015).
10. www.imm.org.pl/imm/plik/pliki-do-pobrania-statut2011_nn33.pdf (pobrano: 1.06.2015).
11. http://www.tuv.com/en/netherlands/home.jsp (pobrano: 1.06.2015).
12. http://www.commoncriteriaportal.org/labs/ (pobrano: 1.06.2015).
13. http://www.pca.gov.pl/?page=status_prawny (pobrano: 1.06.2015). (pobrano: 1.06.2015).
14. http://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20--%20Ratified%20September%208%202014.pdf (pobrano: 1.06.2015).
15. http://www.commoncriteriaportal.org/ccra/members/ (pobrano: 1.06.2015).

THE COMMON CRITERIA CERTIFICATION AS AN INITIAL CONCEPT FOR CONSTRUCTION OF THE POLISH INFORMATIONAL SECURITY MODEL

Abstract: The paper presents the issue of verification of IT security on the basis of the Common Criteria standard. This standard is currently internationally recognized among others in the field of electronic documents. For this reason both the standard and the Common Criteria certification model are critical for the national security and especially the identification security of citizens. The analysis of the Common Criteria certification model as well as the relationship between this certification and the national security lead to the conclusion that in Poland it is necessary to establish organizational structures which will provide the said certification. A draft of the domestic IT security model, based on the Common Criteria certification, is presented in the paper. In this model the key functions are played by the Polish Centre for Accreditation, the Internal Security Agency (or the National Centre for Cryptology) and the Central IT Establishment (or the Institute of Mathematical Machines).
Keywords: national security, IT security, Common Criteria.