Laboratorium Oceny Cyberbezpieczeństwa Instytutu Łączności – wymagania i wytyczne

Elżbieta Andrukiewicz ***Nils Tekampe***

Rozwój technologii telekomunikacyjnych zwiększa zapotrzebowanie na certyfikację bezpieczeństwa produktów i usług. W połączonych gospodarkach, w tym w szczególności w Unii Europejskiej, istotne znaczenie ma wzajemne uznawanie certyfikatów wydawanych na podstawie wiarygodnych i kompletnych ocen bezpieczeństwa. Obecnie jest to możliwe dzięki porozumieniom międzynarodowym, takim jak Common Criteria Recognition Agreement (CCRA) i Senior Officers Group Information Security – Mutual Recognition Agreement (SOG-IS MRA).

Proces certyfikacji produktu lub usługi składa się z dwóch etapów: ewaluacji (oceny), którą wykonują laboratoria oraz wydawania certyfikatów, które wykonują jednostki certyfikujące. Laboratoria przeprowadzające ewaluację muszą spełnić szereg kryteriów, określanych przez krajowe jednostki certyfikujące. W opracowaniu przeanalizowano wymagania i praktyki laboratoriów w krajach należących do porozumień międzynarodowych, zapewniających wzajemne uznawanie certyfikatów zgodnych z Common Criteria wraz z wnioskami i wytycznymi dla Laboratorium Oceny Cyberbezpieczeństwa w Instytucie Łączności.

cyberbezpieczeństwo, ocena cyberbezpieczeństwa, certyfikacja

Potrzeba certyfikacji cyberbezpieczeństwa

Certyfikat zwiększa zaufanie, że zastosowany produkt, świadczona usługa lub wdrożony proces spełnia wymagania bezpieczeństwa w całym cyklu życia, od zaprojektowania do wycofania z użytku. Oczywiście, sam system certyfikacji musi być wiarygodny, transparentny oraz wykorzystywać powszechnie uznawane normy referencyjne określające sposób tworzenia wymagań bezpieczeństwa oraz metody ewaluacji (oceny), zapewniające porównywalność i powtarzalność wyników.

Szereg regulacji, które pojawiły się w ostatnich latach w Unii Europejskiej, takich jak Dyrektywa NIS, Rozporządzenie eIDAS, Rozporządzenie PSD2, wykazało potrzebę opracowania systemu certyfikacji cyberbezpieczeństwa, ułatwiającego wzajemne uznawanie poświadczeń oraz przeciwdziałających fragmentacji Jednolitego Rynku Cyfrowego w Europejskim Obszarze Gospodarczym (EOG). Kluczową inicjatywą jest dyskutowany obecnie projekt Rozporządzenia Parlamentu Europejskiego i Rady dot. europejskich ram certyfikacji cyberbezpieczeństwa („The CyberSecurity Act").

Należy podkreślić, że posiadanie własnej, krajowej struktury laboratoriów dokonujących oceny cyberbezpieczeństwa oraz jednostki certyfikującej sytuuje kraje członkowskie w gronie aktywnych producentów certyfikatów cyberbezpieczeństwa, a nie jedynie odbiorców, którzy będą musieli uznawać certyfikaty wydane przez inne kraje z EOG.

Porównując istotne mierniki potencjału, takie jak powierzchnia, liczba ludności oraz produkt krajowy brutto, wszystkie kraje UE, które wyprzedzają Polskę w rankingach [1], mają od wielu lat działające

struktury organizacyjne umożliwiające wydawanie certyfikatów cyberbezpieczeństwa, uznawanych nie tylko w EOG, ale także globalnie.

Rozumiejąc znaczenie certyfikacji cyberbezpieczeństwa dla strategii zrównoważonego rozwoju Polski w perspektywie długookresowej, Instytut Łączności – Państwowy Instytut Badawczy zainicjował projekt pn. „Krajowy system oceny i certyfikacji bezpieczeństwa i prywatności produktów i usług ICT zgodnie z Common Criteria (KSO3C)", którego realizację rozpoczęto formalnie w marcu 2018 roku.

Normy referencyjne w schemacie oceny i certyfikacji cyberbezpieczeństwa

Na początku XXI wieku opracowano pierwsze normy, które zapewniają jednolite podejście do tworzenia wymagań bezpieczeństwa dla produktów teleinformatycznych powszechnego użytku oraz sposobu weryfikacji spełnienia wymagań przez te produkty. Sformalizowany i uporządkowany sposób tworzenia wymagań bezpieczeństwa teleinformatycznego pozwala na wyznaczenie żądanego poziomu bezpieczeństwa w zależności od konkretnych potrzeb. Z kolei sformalizowany i ujednolicony system weryfikacji funkcjonowania produktów w środowisku operacyjnym umożliwia określenie poziomu zaufania do poprawności i kompletności wdrożenia opisanych wymagań. Oceną bezpieczeństwa zajmują się wyspecjalizowane laboratoria, dysponujące odpowiednim wyposażeniem oraz specjalistami, którzy potrafią przeprowadzić testy i badania weryfikujące spełnienie. W praktyce duża część testów polega na przeprowadzaniu ataków na produkty i systemy w kontrolowanych warunkach laboratorium. Całość opisano w normie ISO/IEC 15408 *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych* [2], znanej pod rynkową nazwą Common Criteria. Normy serii ISO/IEC 15408 są stale rozwijane i uaktualniane w miarę rozwoju technologii teleinformatycznych oraz sposobów i środków przełamywania zabezpieczeń.

Przyjęcie jako podstawy weryfikacji bezpieczeństwa teleinformatycznego powszechnie uznawanych norm międzynarodowych umożliwiło opracowanie zunifikowanej metodyki przeprowadzania oceny bezpieczeństwa teleinformatycznego.

Zakres przedmiotowy Common Criteria

Ocenie bezpieczeństwa zgodnej z Common Criteria można poddać każdy produkt ICT pod warunkiem, że został on opracowany w taki sposób, że wymagania bezpieczeństwa są opisane zgodnie z formalnym modelem bezpieczeństwa zawartym w normie PN ISO/IEC 15408.

Z uwagi na uwarunkowania prawne i rynkowe, schematy oceny i certyfikacji znajdują zastosowanie w wielu obszarów funkcjonowania produktów teleinformatycznych, takich jak:

- infrastruktura krytyczna (programowalne sterowniki, VPN, sieci bezprzewodowe),
- infrastruktura informatyczna (IPSec, moduły kryptograficzne, systemy wykrywania wtargnięć, systemy antywirusowe),
- energetyka (inteligentne liczniki),
- administracja publiczna (paszporty, prawa jazdy),
- zdalna identyfikacja i uwierzytelnienie (podpis elektroniczny, pieczęć elektroniczna),
- opieka zdrowotna (karty lekarza i pacjenta),

- systemy transportowe (tachografy),
- specjalizowane karty dla użytkowników telefonii komórkowej (USIM),
- media (dekodery cyfrowe),
- gry on-line (elektroniczny krupier).

Warto zaznaczyć, że metodyka oceny bezpieczeństwa zgodna z Common Criteria jest też powszechna w obszarze zastosowań teleinformatyki związanych z bezpieczeństwem narodowym, bezpieczeństwem publicznym oraz w innych obszarach, w których wymagania bezpieczeństwa mają najwyższy priorytet.

Wzajemne uznawanie certyfikatów zgodnych z Common Criteria

Normy referencyjne umożliwiają uzyskanie spójności, powtarzalności i porównywalności wyników oceny bezpieczeństwa. Efektem pozytywnego przejścia oceny bezpieczeństwa może stać się wydanie certyfikatu zgodności z normą. Jednak sama certyfikacja stanowiąca formalne potwierdzenie zgodności z normami referencyjnymi znajduje się poza zakresem przedmiotowym tych norm. Do tego celu jest potrzebna struktura organizacyjna funkcjonująca według ustalonych zasad i w taki sposób, aby w pierwszym rzędzie użytkownicy danego produktu mogli zaufać przeprowadzonej ocenie, mając niewielką lub wręcz żadną wiedzę o tym, jak ta ocena była przeprowadzona, a następnie, aby takie zaufanie mogło być wyrażone przez cały rynek. W tym drugim przypadku chodzi o stworzenie warunków do wzajemnego uznawania certyfikatów wydanych przez inną strukturę organizacyjną. Oczywistym jest, że kluczowym czynnikiem utrzymania zaufania oraz uznawania wydawanych certyfikatów jest gwarancja jakości i wiarygodności procesów oceny i certyfikacji bezpieczeństwa.

Kolejnym czynnikiem dodatkowo komplikującym związek między procesem oceny a certyfikatem jest poziom uzasadnienia pewności oceny bezpieczeństwa. Jest to informacja, która w istotny sposób wpływa na zastosowanie produktu. Przykładowo, inny poziom wiarygodności oceny bezpieczeństwa można zastosować do układu scalonego montowanego w legitymacji studenckiej, a inny – tego samego nieraz układu – w paszportach. Normy referencyjne określają kryteria pomiaru zaufania do oceny, definiując kryteria dla 7 poziomów uzasadnienia pewności (*Evaluation Assurance Level* – EAL), od najniższego (EAL1) do najwyższego (EAL7). Kryteria dla poziomów uzasadnienia pewności oceny odnoszą się do rygoru, zakresu i szczegółowości testów. Niemniej jednak, o ile na niższych poziomach kryteria te można uznać za dokładne, to na wyższych zależą coraz bardziej od indywidualnie stosowanych technik i sposobów przeprowadzania odpowiednich testów, co często wymyka się jakiejkolwiek standaryzacji.

Wszystkie powyższe uwarunkowania wskazują na konieczność zbudowania struktury organizacyjnej, określającej nie tylko normy referencyjne, ale też funkcjonującej zgodnie z dodatkowymi regułami i procedurami, co zwykle jest określane jako schemat oceny i certyfikacji. Te reguły i procedury dotyczą zarówno jednostek certyfikujących, jak i laboratoriów dokonujących oceny bezpieczeństwa. Poziom uzasadnienia pewności dla wzajemnego uznawania certyfikatów może stanowić istotny czynnik zakresu przedmiotowego, dla którego wzajemne uznanie jest weryfikowalne i zunifikowane.

Mechanizm wzajemnego uznawania certyfikatów, zgodnych z Common Criteria, który w dużej mierze jest powielony w projekcie Rozporządzenia dot. europejskich ram certyfikacji cyberbezpieczeństwa, został wprowadzony w dwóch porozumieniach międzynarodowych tj. *Common Criteria Recognition Arrangement* (CCRA) [3] oraz *Senior Officers Group Information Security – Mutual Recognition Agreement* (SOG-IS MRA) [4].

CCRA było pierwszym porozumieniem w sprawie międzynarodowego uznawania certyfikatów wydawanych zgodnie z Common Criteria.

Celem CCRA jest zapewnienie, że oceny są wykonywane na podstawie spójnych reguł i norm, z wysokim poziomem wiarygodności, w celu poprawy dostępności ocenianych produktów i profili ochrony①, tak aby wyeliminować zbędne oceny oraz zapewnić ciągłą poprawę wydajności i efektywności kosztowej ocen.

W ramach CCRA funkcjonuje struktura zarządcza w postaci *Common Criteria Management Board* (CCMB), złożona z wysokich rangą przedstawicieli każdego z sygnatariuszy. Głównym celem CCMB jest nadzór nad wdrożeniem Porozumienia oraz tworzenie wytycznych dla systemów krajowych schematów oceny i certyfikacji. CCMB decyduje też o przyjmowaniu nowych członków.

Wymagania związane z harmonijnym stosowaniem Common Criteria są opracowywane przez dwie inne grupy tj. *Common Criteria Development Board* (CCDB) oraz *Common Criteria Maintenance Board* (CCDB).

CCDB zarządza programem prac technicznych w zakresie utrzymania i ciągłego rozwoju Common Criteria②oraz uzgadnia szczegółowe sposoby stosowania norm do ocen bezpieczeństwa przeprowadzanych w krajowych schematach państw – członków porozumienia, w celu zapewnienia harmonizacji procesów ewaluacji i certyfikacji. Natomiast głównym zadaniem CCMB jest przetwarzanie wniosków o zmianę (*Change Proposals*) w sposobach funkcjonowania schematów krajowych, w tym metodykach ocen bezpieczeństwa, np. wynikających ze zmian w normach referencyjnych.

CCRA nakłada na jednostki certyfikujące obowiązek zapewnienia skutecznego nadzoru nad zgodnością laboratorium oceniającego z kryteriami określonymi w Porozumieniu. Natomiast dla laboratorium dokonującego oceny bezpieczeństwa, funkcjonowanie w krajowym schemacie oceny bezpieczeństwa państwa będącego członkiem CCRA wiąże się z dodatkowymi wymaganiami dotyczącymi szczegółowych technik, praktyk i procedur.

SOG-IS jako struktura organizacyjna funkcjonuje na podstawie decyzji Rady UE z 31 marca 1992 r. (92/242/EWG) w zakresie bezpieczeństwa systemów informatycznych, a następnie zalecenia Rady z 7 kwietnia 1995 r. (1995/144/WE) w sprawie wspólnych kryteriów oceny bezpieczeństwa technologii informatycznych.

Porozumienie między członkami SOG-IS ws. wzajemnego uznawania certyfikatów obejmuje państwa będące europejskimi członkami CCRA. Zakres przedmiotowy umowy o wzajemnym uznawaniu certyfikatów w SOG-IS jest jednak rozszerzeniem CCRA, które zostało zdefiniowane w następujący sposób:

- do poziomu uzasadnienia pewności EAL4 zakres przedmiotowy CCRA i SOG-IS MRA jest identyczny (tzn. certyfikaty uznawane w ramach CCRA są uznawane też w SOG-IS MRA i odwrotnie),

① Protection Profiles (PP) – specyfikacje techniczne zawierające wymagania bezpieczeństwa dla określonego typu produktu ICT.

② Należy wspomnieć, że prace nad nową wersją norm referencyjnych Common Criteria są obecnie prowadzone w całości w ramach ISO, a CCDB ma status organizacji wspierającej. Poprzednie wersje norm powstawały w CCDB.

- uznanie certyfikatów na poziomie uzasadnienia pewności powyżej EAL4 dotyczy określonych obszarów technicznych i wymaga zatwierdzenia programu przez komitet zarządzający SOG-IS. (tzn. certyfikaty wydane w tym zakresie są uznawane tylko przez państwa-członków porozumienia SOG-IS).

Komitet Zarządzający SOG-IS określił szczegółowe wymagania w dwóch domenach technicznych [5], w których są wzajemnie uznawane certyfikaty w ramach SOG-IS aż do poziomu EAL7, tzn. urządzenia sprzętowe ze skrzynkami bezpieczeństwa (np. terminale płatnicze, moduły pojazdu z tachografami, liczniki inteligentne) oraz karty inteligentne lub podobne urządzenia (np. USIM, urządzenia składania bezpiecznego podpisu elektronicznego, układy TPM, karty płatnicze).

Aby osiągnąć wyższy poziom uznania certyfikatów w ramach porozumienia SOG-IS, konieczne było opracowanie i opublikowanie zestawu dokumentów uzupełniających w stosunku do CCRA. Dokumenty te tworzą Wspólną Bibliotekę Interpretacji (*Joint Interpretation Library* – JIL) i zawierają obowiązkowy zbiór wymagań, których należy przestrzegać podczas każdej oceny produktu należącego do dziedziny technicznej objętej umową SOG-IS i wytycznych, które są opcjonalne w odniesieniu do ich wykorzystania.

Warto wskazać, że szereg działań SOG-IS i CCRA wykonują wspólnie. Dotyczy to wzajemnego powoływania się na dokumenty a także przeprowadzania wzajemnych ocen schematów funkcjonujących w ramach umów międzynarodowych (części z nich, jeśli dotyczą identycznego zakresu przedmiotu obu porozumień).

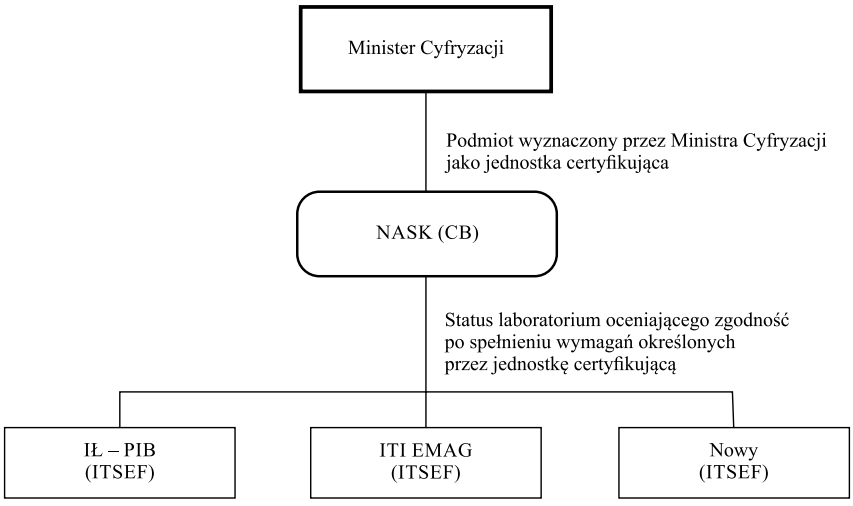
Wreszcie należy wskazać, że wymagania, wytyczne, techniki i praktyki oceny i certyfikacji są w dużej mierze efektem prac grup technicznych złożonych z ekspertów pochodzących z jednostek certyfikujących, laboratoriów oraz producentów z danej dziedziny technicznej. Są też grupy użytkowników Common Criteria i fora wymiany informacji. Za certyfikacją produktów zgodnych z Common Criteria stoi cały ekosystem zapewniający powiązania między produktem, jego zastosowaniem oraz procesami oceny i certyfikacji.

Projekt KSO3C

Projekt KSO3C jest wspólnym przedsięwzięciem konsorcjum naukowego złożonego z trzech jednostek naukowo-badawczych tzn. Instytutu Łączności – Państwowego Instytutu Badawczego (IŁ-PIB, lider konsorcjum), Naukowej i Akademickiej Sieci Komputerowej (NASK) oraz Instytutu Technik Innowacyjnych EMAG (ITI EMAG).

Celem Projektu jest opracowanie i wdrożenie w Polsce schematu oceny i certyfikacji bezpieczeństwa produktów informatycznych umożliwiającego przeprowadzenie oceny i wydanie certyfikatów zgodności z normą oceny (ewaluacji) bezpieczeństwa teleinformatycznego PN-ISO/IEC 15408 (Common Criteria). Certyfikaty wydawane w ramach polskiego schematu – po spełnieniu szeregu warunków formalnych i merytorycznych – będą uznawane przez najbardziej zaawansowane gospodarczo kraje świata oraz w ramach Unii Europejskiej.

Na rys. 1 przedstawiono proponowaną strukturę schematu oceny i certyfikacji w Polsce.



Rys. 1. *Krajowy schemat oceny i certyfikacji w Polsce*

Zakłada się, że schemat oceny i certyfikacji będzie strukturą otwartą, w której mogą pojawiać się nowe laboratoria oceniające zgodność z Common Criteria. Warunkiem uczestnictwa w schemacie będzie spełnienie wymagań, jednakowych dla wszystkich laboratoriów, określonych przez jednostkę certyfikującą z poszanowaniem zasady transparentności i bezstronności.

Schemat oceny i certyfikacji jest przedsięwzięciem komercyjnym, które umożliwi:

- przedsiębiorcom i dostawcom – zwiększenie konkurencyjności produktów teleinformatycznych zapewniając uzasadnione zaufanie do wydanych certyfikatów zgodności z powszechnie stosowaną normą międzynarodową, na rynku polskim oraz regionalnym (europejskim) i światowym,
- polskim i zagranicznym przedsiębiorcom – przejście procesu oceny ich produktów na zgodność z wymaganiami bezpieczeństwa w polskich laboratoriach,
- jednostkom administracji państwowej – spełnienie wymagań wynikających z przyjętych zobowiązań przez Państwo Polskie wobec Unii Europejskiej, które pozwolą na aktywne promowanie polskich produktów teleinformatycznych w UE,
- polskim użytkownikom – możliwość korzystania z produktów posiadających poświadczenie spełniania wysokich wymagań bezpieczeństwa, bez konieczności aplikowania o takie oceny w laboratoriach innych krajów,
- ogólnie, polskiej gospodarce – zwiększenie konkurencyjności oraz potencjału technicznego w różnych sektorach, dzięki ochronie całego procesu wytwórczego i interesów polskich przedsiębiorców.

Najważniejsze informacje dotyczące Projektu KSO3C

Poniżej przedstawiono najistotniejsze informacje dotyczące Projektu:

- oficjalne rozpoczęcie realizacji projektu – **1 marca 2018 r.**

- czas trwania projektu – **36 miesięcy**
- koszt całkowity projektu – **24 164 009,28 zł (brutto).**

Kryterium jakościowe – opracowany i wdrożony schemat oceny i certyfikacji spełniający wymagania podmiotowe i przedmiotowe, wystarczające do przyjęcia Polski do porozumień międzynarodowych, jako Strony porozumień SOGIS i CCRA, wydającej certyfikaty (*Certificate Authorized Member*).

Zakres Projektu – opracowanie i wdrożenie schematu oceny i certyfikacji obejmującego:

- przygotowanie organizacyjne, proceduralne i techniczne NASK-PIB do realizacji funkcji jednostki certyfikującej (CB) oraz osiągnięcie przez CB zdolności operacyjnej,
- przygotowanie organizacyjne, proceduralne i techniczne IŁ-PIB oraz ITI EMAG jako laboratoriów dokonujących oceny bezpieczeństwa produktów teleinformatycznych (ITSEF), oraz osiągnięcie przez te podmioty zdolności operacyjnej,
- przygotowanie i przeprowadzenie dwóch pełnych certyfikacji wybranych produktów teleinformatycznych (pilotaż),
- przygotowanie wniosków o przyjęcie do Porozumień CCRA oraz SOG-IS MRA jako uczestnik autoryzowany, wydający uznawane globalnie certyfikaty bezpieczeństwa,
- przejście procedury weryfikacji wniosku o przyjęcie, w tym przeprowadzenie certyfikacji w trybie nadzorowanym (tzw. *Shadow Certification*) dla dwóch (dodatkowych) wybranych produktów ICT, zakończonych wynikiem pozytywnym.

W dalszej części artykułu zostanie przedstawiona koncepcja utworzenia laboratorium oceny bezpieczeństwa w IŁ-PIB, na podstawie przeglądu najlepszych praktyk istniejących na rynku.

Wymagania dla laboratorium oceny bezpieczeństwa w IŁ-PIB na bazie najlepszych praktyk

W poszczególnych kategoriach istotnych dla organizacji laboratorium tzn.:

- model biznesowy,
- zakres przedmiotowy oceny bezpieczeństwa,
- struktura organizacyjna i role w procesie ewaluacji,
- personel,
- zapewnienie i utrzymanie jakości oceny bezpieczeństwa,

zostanie przedstawiona ogólna charakterystyka praktyk stosowanych w podobnych jednostkach, ze szczególnym uwzględnieniem podmiotów funkcjonujących w Europie oraz wskazany wariant optymalny dla laboratorium w IŁ-PIB.

Model biznesowy

Istnieją cztery podstawowe formy prawne, w ramach których funkcjonują laboratoria oceny bezpieczeństwa zgodnej z Common Criteria:

- przedsiębiorstwo prywatne, tzn. niezależny podmiot prawny, najczęściej w formie zbliżonej do spółki z ograniczoną odpowiedzialnością,
- spółka akcyjna bądź podobna – niezależny podmiot prawny, notowany na giełdzie,
- instytut badawczy – podmiot non-profit, założony przez przedsiębiorstwa lub placówki naukowo-badawcze,
- agencja rządowa – laboratoria należące do rządu danego kraju.

Oddzielną kategorię stanowią laboratoria nieposiadające osobowości prawnej, czyli części firm międzynarodowych, oferujących szerokie portfolio produktów i usług ICT, określanych w kontekście badania jako „zależne".

W całej grupie laboratoriów oceny bezpieczeństwa ponad 50% funkcjonuje w formie spółki akcyjnej bądź z ograniczoną odpowiedzialnością. W kontekście tego badania nazywa się je „niezależnymi". Prawnie niezależne laboratoria stanowią większość licencjonowanych laboratoriów w Norwegii (100%), Niemczech (87%) i Francji (60%).

Druga grupa podmiotów świadczących usługi oceny bezpieczeństwa składa się z laboratoriów zależnych. Stanowią one większość licencjonowanych laboratoriów w Australii (100%), Wielkiej Brytanii (100%) i Kanadzie (75%).

Trzecia grupa obejmuje instytuty badawcze oraz agencje rządowe. Istnieje na świecie kilka schematów, w których znaczenie podmiotów niekomercyjnych jest szczególne. Agencja rządowa jest jedynym licencjonowanym laboratorium w ramach indyjskiego systemu. Instytuty badawcze stanowią znaczącą część licencjonowanych laboratoriów w Japonii i Korei.

Model biznesowy różni się również udziałem usług oceny bezpieczeństwa w przychodach. Można zidentyfikować następujące modele:

- podstawowy: oceny bezpieczeństwa zgodne z Common Criteria są podstawową działalnością danego podmiotu,
- zorientowany na bezpieczeństwo IT: podmiot koncentruje się na usługach bezpieczeństwa ICT, jednak oceny bezpieczeństwa zgodne z Common Criteria są istotną częścią zakresu świadczonych usług,
- zorientowany na certyfikację: podmiot oferuje portfolio usług oceny lub certyfikacji w wielu dziedzinach, w tym również zgodne z Common Criteria,
- minimalny: oceny zgodne z Common Criteria to tylko niewielka część szerokiego portfolio produktów i usług, w tym sprzedaży zintegrowanych rozwiązań bezpieczeństwa lub IT.

46% badanych laboratoriów należy uznać za należące do modelu podstawowego. Znacznie mniejsza liczba (13%) laboratoriów skupia się na bezpieczeństwie IT, którego certyfikacja jest tylko częścią. Najmniejsza grupa (6%) składa się z laboratoriów świadczących usługi certyfikacyjne w wielu dziedzinach. Istotny odsetek laboratoriów (35%) stanowią podmioty zależne od dużych firm, często międzynarodowych, dla których certyfikacja CC ma minimalne znaczenie biznesowe. Wyniki klasyfikacji ograniczone do SOG-IS MRA są zgodne z podobnymi wzorami, z wyjątkiem relatywnie większego znaczenia modelu biznesowego zorientowanego na bezpieczeństwo IT.

Analiza formy prawnej i modelu biznesowego laboratoriów prowadzi do wniosku, że większość licencjonowanych laboratoriów działających w ramach systemu SOG-IS to niezależne prywatne firmy

skupione na samych usługach oceny, a liczba ta jest znacznie wyższa niż w przypadku laboratoriów objętych CCRA.

Oznacza to, że rynek oceny bezpieczeństwa zgodnej z Common Criteria nie charakteryzuje się wielką koncentracją kapitału, a jednostki podobne do IŁ-PIB (czyli świadczące usługi oceny bezpieczeństwa jako istotną część całego portfolio usług IT) stanowią duży odsetek w branży. Zwiększa to szanse laboratorium IŁ-PIB na zaistnienie na rynku usług oceny bezpieczeństwa, także w kontekście międzynarodowym (np. współpracy z innymi laboratoriami przy większych projektach).

Zakres przedmiotowy oceny bezpieczeństwa

Baza danych publikowanej przez CCRA zawiera informacje o certyfikowanych produktach ICT [6]. W europejskich laboratoriach przeprowadzono większość ocen bezpieczeństwa. Z uwagi na zwykle 3-letni okres ważności certyfikatów, istotne są dane dotyczące liczby przeprowadzonych ocen i wydanych certyfikatów w układzie rocznym.

W tablicy 1 przedstawiono rozkład liczby certyfikatów w poszczególnych krajach będących stronami porozumienia SOG-IS MRA w latach 2014–2016.

Tabl. 1. *Liczba certyfikatów wydanych w latach 2014–2016 w ramach porozumienia SOG-IS MRA*

Kraj	Lata			Całkowita liczba wydanych certyfikatów (od 1999 r.)
	2014	2015	2016	
Niemcy	62	46	11	878
Hiszpania	7	7	8	80
Francja	75	57	57	777
Włochy	1	8	3	21
Holandia	2	12		45
Szwecja	6	7	3	21
Wielka Brytania	7	10	1	41

W układzie rodzajowym, przedmiotem certyfikacji są w ogromnej większości produkty z kategorii dedykowanych układów scalonych i kart inteligentnych (rys. 2).

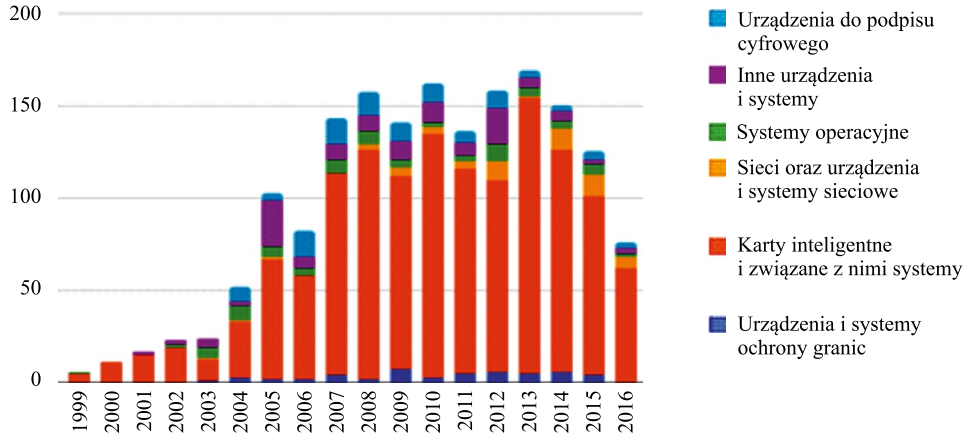
Jeśli pominąć certyfikaty związane z kartami inteligentnymi i ponownie przeprowadzić analizę, to następnymi najpopularniejszymi kategoriami produktowymi certyfikacji są bazy danych, urządzenia do podpisów cyfrowych i urządzenia sieciowe (rys. 3).

Doświadczenia innych krajów, zwłaszcza Francji③, a także nowe regulacje UE, stanowią istotne czynniki spodziewanego w najbliższym czasie wzrost rynku certyfikacji oprogramowania. Jeśli uwzględnić dodatkowo proces tworzenia następnej edycji norm ISO/IEC 15408④, w której unormowane zostaną

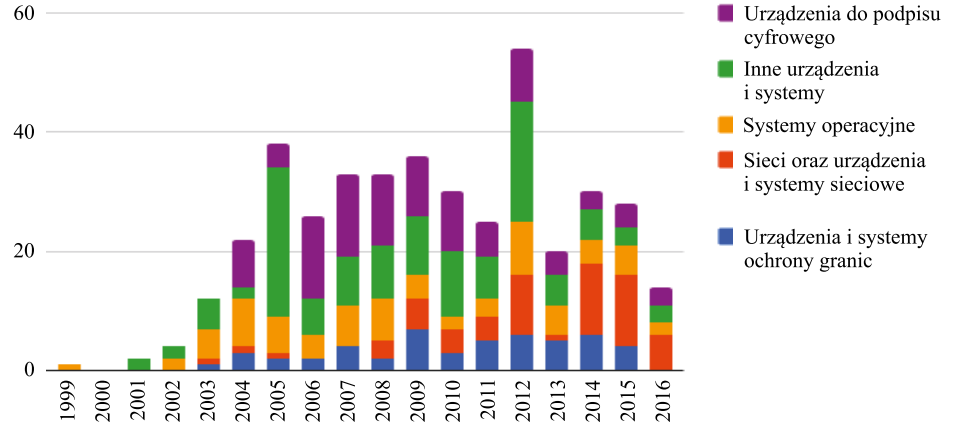
③ Informacje pochodzące z niepublikowanych materiałów Agence nationale de la sécurité des systèmes d'information (ANSSI), krajowej agencji cyberbezpieczeństwa we Francji.
④ Publikacja nowej edycji norm ISO/IEC 15408 jest spodziewana w połowie 2020 roku (na podstawie materiałów wewnętrznych ISO).

znacznie prostsze niż dotychczasowe modele bezpieczeństwa oraz techniki ewaluacji, to oczywistym zdaje się istotna zmiana struktury rodzajowej produktów podlegających certyfikacji, w stronę komponentów sprzętowo-programowych oraz oprogramowania (w tym aplikacji mobilnych).

Z uwagi na fakt, że osiągnięcie zdolności operacyjnej laboratorium w IŁ-PIB jest planowane pod koniec 2019 roku, laboratorium musi być przygotowane na przyjęcie do oceny produktów w tych kategoriach rodzajowych.



Rys. 2. *Liczba wydanych certyfikatów w układzie rodzajowym*



Rys. 3. *Liczba wydanych certyfikatów w układzie rodzajowym z pominięciem kategorii kart inteligentnych i podobnych urządzeń*

Struktura organizacyjna i role w procesie oceny bezpieczeństwa

Praca oceniającego (ewaluatora) obejmuje przegląd dokumentacji dostarczonej przez sponsora lub dewelopera (producenta), a także testy i ocenę podatności na zagrożenia samego produktu. W dużych laboratoriach najczęściej występują specjalizacje (np. w obszarze testów oprogramowania czy sprzętu).

W pracy ewaluatora obowiązuje zasada „czterech oczu", która wynika z wymagań Common Criteria. Każdy etap pracy wykonywanej przez ewaluatora jest zazwyczaj weryfikowany przez co najmniej jednego kompetentnego współpracownika. Duża liczba przeglądów i kontroli gwarantuje wysoką jakość procedur oceny zgodnie z Common Criteria.

Każda ocena jest prowadzona przez starszego/wiodącego ewaluatora. Praca w takiej roli zazwyczaj obejmuje ścisły i aktywny nadzór ewaluatora. Starszy ewaluator powinien być doświadczonym profesjonalistą i dlatego jest zwykle pierwszym punktem kontaktowym dla wszystkich ewaluatorów w projekcie, jeśli pojawią się pytania lub wątpliwości. Istotne decyzje i wyniki testów, które potencjalnie mają wpływ na całą ewaluację, są zatwierdzane przez starszego ewaluatora.

Starszy ewaluator odpowiada za cały projekt, a zatem podejmuje również decyzje techniczne dotyczące ogólnego harmonogramu i budżetu projektu. Ponadto, starszy ewaluator zazwyczaj odpowiada za kontaktowanie się z klientami, ustalanie trybów współpracy, spotkania w kluczowych momentach projektu i podobne działania.

Kierownik laboratorium nadzoruje wszystkie procesy oceny, które są prowadzone w danym laboratorium. W odniesieniu do samych procesów oceny, kierownik laboratorium przejawia zwykle niższy poziom zaangażowania. Jeśli pojawi się spór techniczny pomiędzy osobami oceniającymi (lub między osobami dokonującymi oceny a twórcą lub sponsorem), można zaangażować kierownika laboratorium. Jednak w dużej liczbie laboratoriów pozycja kierownika laboratorium jest postrzegana jako pozycja zarządcza, a nie techniczna. Oznacza to, że kierownik laboratorium niekoniecznie musi mieć umiejętności techniczne i wiedzę, aby omawiać wszystkie problemy techniczne. Główne zadaniem kierownika laboratorium to:

- nadzór nad przestrzeganiem przepisów i procedur,
- zapewnienie rozpowszechniania nowych interpretacji i not aplikacyjnych dotyczących wymagań koniecznych do zastosowania podczas przeprowadzanych ocen,
- komunikowanie się z jednostką certyfikującą i organem akredytującym we wszystkich istotnych kwestiach związanych z akredytacją licencjonowango laboratorium.

Z uwagi na ewidentny podział zespołu laboratorium IŁ-PIB na część specjalizującą się w zagadnieniach sprzętowo-programowych oraz część zorientowaną programowo, od początku zakłada się specjalizację podzespołów w odniesieniu do charakteru badanych produktów (sprzętowych, sprzętowo-programowych oraz programowych). Na starszych ewaluatorów będą typowane osoby, które przejdą długookresowe staże w zagranicznych laboratoriach. Zakłada się też, że kierownik laboratorium może również występować w roli prowadzącego oceny bezpieczeństwa.

Personel

Jednym z podstawowych warunków, jaki musi spełnić krajowy schemat oceny i certyfikacji, aby zostać przyjęty do porozumień międzynarodowych, to zapewnienie zespołu specjalistów mających wiedzę, umiejętności i doświadczenie umożliwiające samodzielne przeprowadzenie ocen bezpieczeństwa. Należy w tym miejscu nadmienić, że ten czynnik jest zwykle przedmiotem wymagań ze strony jednostki certyfikującej w odniesieniu do laboratorium, co powoduje, że można wskazać wiele różnic między poszczególnymi krajowymi schematami. W tablicy 2 przedstawiono wymagania odnośnie do ewaluatorów w niektórych krajowych schematach porozumienia SOG-IS MRA.

Tabl. 2. *Wymagania dotyczące personelu w wybranych krajowych schematach oceny i certyfikacji*

Kraj	Wymagania dla ewaluatorów (oceniających)
Wielka Brytania	3 poziomy kwalifikacji: • Oceniający Stażysta (szkolenie, które jest prowadzone przez Wykwalifikowanego Oceniającego i zatwierdzone przez jednostkę certyfikującą), • Wykwalifikowany Oceniający (Oceniający Stażysta, wobec którego jednostka certyfikująca uznała, że może wykonywać pracę ewaluacyjną bez nadzoru), • Specjalista Oceniający (uznany za spełniającego warunki kwalifikacji dla niektórych klas uzasadnienia pewności zgodnie z Common Criteria; dla innych może spełniać jedynie warunki Oceniającego Stażysty). Ocena dla poziomu Wykwalifikowany i Specjalista Oceniający jest dokonywana na podstawie pozytywnej rekomendacji kierownictwa laboratorium oraz pisemnych raportów opracowanych przez Oceniającego Stażystę.
Szwecja	Dwa poziomy kwalifikacji: • Oceniający (działa pod nadzorem Wykwalifikowanego Oceniającego), • Wykwalifikowany Oceniający. Aby uzyskać status Oceniającego, kandydat musi ukończyć szkolenie CC organizowane przez jednostkę certyfikująca i zdać egzamin. Aby uzyskać status Wykwalifikowanego Oceniającego, Oceniający musi wykazać się doświadczeniem w planowaniu i przeprowadzaniu działań ewaluacyjnych i co najmniej raz samodzielnie sporządzić raport dla wszystkich działań ewaluacyjnych na poziomie EAL4 lub wyższym.
Niemcy	Każdy z Oceniających jest uznawany przez jednostkę certyfikującą po ocenie jego kompetencji i ukończeniu szkolenia przeprowadzonego przez jednostkę certyfikującą; szkolenie obejmuje udział w ewaluacji próbnej (skonstruowany fikcyjny przypadek).
Holandia	Szkolenie organizowane lub zatwierdzone przez jednostkę certyfikującą, zakończone egzaminem. Ukończenie szkolenia z wynikiem pozytywnym skutkuje uzyskaniem statusu Oceniającego.
Francja	Jednostka certyfikująca jest odpowiedzialna za ogólną ocenę zdolności laboratorium, w tym ocenę umiejętności personelu.

Przy konstruowaniu zespołu specjalistów w laboratorium IŁ-PIB zakłada się przyjęcie prostej dwupoziomowej struktury pracy ewaluatorów, jak to już wskazano powyżej. W pierwszej fazie operacyjnego funkcjonowania polskiego schematu nie zakłada się aktywnej roli jednostki certyfikującej przy ocenie kwalifikacji ewaluatorów. W polskim schemacie odniesieniem referencyjnym będzie opublikowana właśnie 3-częściowa norma międzynarodowa ISO/IEC 19896 *Competence requirements for information security testers and evaluators*.

Zapewnienie i utrzymanie jakości oceny bezpieczeństwa

Mechanizm licencjonowania

Istotnym instrumentem zapewnienia jakości oraz spójności ocen bezpieczeństwa jest mechanizm licencjonowania laboratoriów oceny bezpieczeństwa przez jednostki certyfikujące uczestniczące w porozumieniach CCRA i SOGIS. Licencjonowanie odbywa się w ramach krajowego schematu, co oznacza, że uzyskanie statusu laboratorium oceny bezpieczeństwa w innym krajowym schemacie wymaga wystąpienia o odrębną licencję. Dopiero ostatnio członkowie porozumień SOG-IS MRA i CCRA rozpoczęli prace nad warunkami wzajemnego uznawania licencji dla laboratorium (*cross-licencing*).

Do najważniejszych cech zróżnicowania mechanizmów licencjonowania należy zaliczyć:

- procedura jednoetapowa – ocena techniczna zdolności wnioskodawcy jest wystarczająca do otrzymania licencji,
- procedura dwuetapowa – postępowanie o udzielenie licencji może być podzielone na dwie fazy tzn. oceny gotowości technicznej oraz oceny testowej). Dodatkowo, w niektórych schematach dopuszcza się wstępną licencję po przejściu badania technicznego gotowości laboratorium, a następnie stałą licencję po pomyślnym zaliczeniu oceny testowej,
- uzyskanie akredytacji jako warunku wstępnego: posiadanie akredytacji potwierdzającej zgodność z normą ISO/IEC 17025 jest obowiązkowe we wszystkich analizowanych schematach, jednak w niektórych systemach dopuszcza się rozpoczęcie oceny przez jednostkę certyfikującą przed spełnieniem przez wnioskodawcę wymogu akredytacji,
- w części schematów jednostka certyfikująca pobiera opłaty licencyjne, w części licencja jest bezpłatna.

Należy zauważyć, że w schematach krajów europejskich jednostki certyfikacyjne udzielają licencji laboratoriom w ramach CCRA i – równolegle – w ramach SOG-IS MRA.

Typowe procesy i procedury

Ocena bezpieczeństwa zgodna z Common Criteria zwykle odbywa się w interakcji między deweloperem a laboratorium. Deweloper przedstawia laboratorium dowody, że produkt spełnia wymagania, które są określone w dokumentacji bezpieczeństwa. Laboratorium analizuje i testuje dowody oraz przekazuje informacje zwrotne do dewelopera. Jeśli test kończy się negatywnie to odpowiednia dokumentacja i sam przedmiot oceny (*Target of Evaluation* – TOE) są poprawiane, a proces zaczyna się od początku.

Oceny są zwykle organizowane w postaci oddzielnego badania kilku klas uzasadnienia pewności. Oznacza to, że następujące obszary oceny bezpieczeństwa są adresowane jeden po drugim:

- specyfikacja wymagań bezpieczeństwa (klasa AST),
- dokumentacja projektowa (klasa ADV),
- dokumentacja produktu (klasa AGD),
- dokumentacja cyklu życia produktu (klasa ALC),
- testowanie i analiza podatności (klasy ATE i AVA).

Ogólny czas, który należy przewidzieć na przeprowadzenie oceny bezpieczeństwa, zależy od następujących czynników (w tej kolejności):

- wybrany poziom uzasadnienia pewności (EAL). Podstawą do oszacowania jest lista jednostek pracy opisana w normie ISO/IEC 18045, które odnoszą się do wybranego EAL,
- złożoność przedmiotu oceny,
- doświadczenie dewelopera,
- doświadczenie laboratorium,
- dojrzałość kryteriów.

Z powyższego zestawienia wynika, że czynniki wpływające na czas i – co za tym idzie – koszt oceny bezpieczeństwa są wielorakie i mają różne źródła, zatem ten parametr jest wyjątkowo trudny do ogólnego szacowania. Warto wspomnieć, że w niektórych schematach ramy czasowe (np. w USA) są ograniczone do maks. 9 miesięcy, co wymaga zapewnienia ścisłej współpracy między deweloperem a laboratorium.

Zakłada się, że ramy czasowe w zależności od EAL są następujące:

- EAL 1, 2, 3 – oceny zwykle mogą trwać krócej niż 6 miesięcy,
- EAL 4 – oceny są zazwyczaj planowane na 1 rok,
- EAL 5 i powyżej: 1,5 roku i więcej.

Złożoność produktu może wpłynąć na czas ewaluacji w następujący sposób:

- proste produkty – nie wpływa na wydłużenie czasu ewaluacji,
- produkty o średniej złożoności – zwykle do czasu oceny należy dodać 10-20%,
- złożone produkty – zwykle do czasu oceny należy dodać 50% lub więcej.

Doświadczenie dewelopera jest bardzo ważnym czynnikiem długości procesu ewaluacji. Odpowiednie przygotowanie produktu może łatwo skrócić ramy czasowe, o których wspomniano wcześniej, nawet o połowę, szczególnie jeśli wcześniejsza wersja produktu była już certyfikowana.

Doświadczenie laboratorium oceniającego i dojrzałość kryteriów oceny są dwoma czynnikami, które są rzadziej omawiane. Mimo że nie istnieją wiarygodne dane na ten temat, empiryczne obserwacje prowadzą do wniosku, że doświadczenie laboratorium ma znaczący wpływ na ramy czasowe oceny. To nie odnosi się tylko do doświadczeń laboratorium w ogóle (czyli ile ocen laboratorium przeprowadziło), ale szczególnie do doświadczeń laboratoryjnych w odniesieniu do podobnych produktów. Jako przykład: laboratorium, które ma już przeprowadzone oceny zapór ogniowych według określonego profilu ochrony będą miały znaczną przewagę w tej dziedzinie (nawet w porównaniu z innymi laboratoriami, które są bardziej doświadczone, ale nie miały do czynienia z podobnym produktem).

Wreszcie, ważnym aspektem jest dojrzałość kryteriów oceny. Nie dotyczy to dojrzałości samych Wspólnych Kryteriów (*Common Criteria*), ale odnosi się bardziej do dojrzałości dedykowanych profili ochrony, interpretacji i wytycznych. W szczególności, gdy takie kryteria są stosowane po raz pierwszy, oceny zwykle trwają znacznie dłużej.

Z dyskusji powyższych czynników wynika, że sukces laboratorium jest w znacznej mierze uwarunkowany dobrą organizacją pracy (która umożliwia skuteczne prowadzenie kilku ewaluacji jednocześnie) oraz szybkim zdobyciem doświadczenia przez zespół. Oba te warunki niezwykle trudno spełnić bez pomocy ekspertów dysponujących odpowiednią wiedzą popartą wieloletnią praktyką.

Oczywiście, nie bez znaczenia jest nawiązanie wczesnej współpracy z partnerami – deweloperami produktów będących potencjalnymi przedmiotami oceny, co znacznie ułatwia późniejsze przeprowadzenie samej ewaluacji. To wskazuje na potrzebę odpowiedniej promocji projektu KSO3C oraz wsparcia ze strony administracji państwowej, stowarzyszeń i federacji przedsiębiorców z branży oraz grup użytkowników.

Podsumowanie

Projekt KSO3C jest wielką szansą na wprowadzenie Polski do elitarnej grupy państw dysponujących potencjałem umożliwiającym przeprowadzenie najbardziej rygorystycznych ocen bezpieczeństwa w odniesieniu do najbardziej złożonych produktów teleinformatycznych i w najbardziej wymagających zastosowaniach.

KSO3C odpowiada na aktualne wyzwania w obszarach cyberbezpieczeństwa i prywatności, wynikających z regulacji unijnych, które powodują konieczność uwzględnienia wymagań Jednolitego Rynku Cyfrowego, ale też z rozwoju technologii i biznesu, które zmieniają zastosowania produktów i sposoby ich użytkowania.

Osiągnięcie gotowości operacyjnej laboratorium IŁ-PIB w czasie krótszym niż dwa lata będzie jednym z najszybszych wdrożeń w historii stosowania Common Criteria, a sam projekt KSO3C jest uważnie obserwowany przez wszystkich członków społeczności związanej z oceną i certyfikacją cyberbezpieczeństwa.

Artykuł powstał z wykorzystaniem części materiałów zgromadzonych na potrzeby opracowania ENISA „Overview of the practices of ICT Certification Laboratories in Europe”, https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories--in-europe

Bibliografia

[1] *The European Union and the African Union – A statistical portrait*, http://ec.europa.eu/eurostat/web/products-statistical-books/-/KS-FQ-17-001?msg=mailSent

[2] ISO/IEC 15408 Information Technology – Security Techniques – Evaluation criteria for IT security (wydanie 3.1), przyjęta do systemu Polskich Norm w 2016 roku.

[3] *About The Common Criteria*, https://www.commoncriteriaportal.org/ccra/

[4] SOG-IS Recognition Agreement, https://www.sogis.org/uk/mra_en.html

[5] SOG-IS Technical Domains, https://www.sogis.org/uk/tech_domain_en.html

[6] Informacje dotyczące certyfikatów wydanych w ramach porozumienia SOGIS, www.commoncriteriaportal.org

Elżbieta Andrukiewicz

Dr inż. Elżbieta Andrukiewicz jest uznanym ekspertem w obszarze zarządzania bezpieczeństwem informacji. Zajmuje się opracowywaniem metodyk w obszarze bezpieczeństwa informacji, opracowywaniem i wdrażaniem systemów zarządzania bezpieczeństwem informacji. Ma na swoim koncie ponad 100 audytów bezpieczeństwa jako audytor wiodący. Jest ekspertem normalizacyjnym w podkomitecie technicznym ISO/IEC JTC1 Subcommittee SC27 „Information techniques - IT Security Techniques" oraz redaktorem wielu norm międzynarodowych z obszaru bezpieczeństwa teleinformatycznego. Obecnie jest kierownikiem projektu Krajowy schemat oceny i certyfikacji bezpieczeństwa produktów ICT zgodnie z Common Criteria (KSO3C).

email: e.andrukiewicz@itl.waw.pl

Nils Tekampe

Mgr inż. Nils Tekampe jest informatykiem i przez wiele lat był kierownikiem laboratorium oceny bezpieczeństwa funkcjonującym w niemieckim schemacie oceny i certyfikacji bezpieczeństwa zgodnym z Common Criteria. Przy ocenach bezpieczeństwa współpracował z dwoma największymi światowymi producentami oprogramowania. Obecnie Nils Tekampe prowadzi firmę Konfidas i jest konsultantem w zakresie bezpieczeństwa informacji i oceny bezpieczeństwa. Ma ogromne doświadczenie w prowadzeniu ocen bezpieczeństwa zgodnie z Common Criteria, ale także FIPS oraz FIDO. Obszary zainteresowania Nilsa to biometria, inteligentne systemy elektroenergetyczne oraz złożone systemy oprogramowania.

email: nt@konfidas.de