mgr inż. PRZEMYSŁAW NOWAK
mgr inż. DARIUSZ ROGOWSKI
mgr IRENA STYCZEŃ
Instytut Technik Innowacyjnych EMAG

Certyfikacja lokalnego środowiska rozwojowego (*Site Certification*) jako innowacyjne podejście do oceny produktów według standardu Common Criteria

Artykuł jest wynikiem analiz związanych z realizacją projektu „Środowisko rozwojowe produktów i systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa – CCMODE". W artykule zawarto krótkie wprowadzenie do rodziny standardów Common Criteria przeznaczonych do oceny i projektowania zabezpieczeń teleinformatycznych, następnie omówiono wyniki pierwszych dwóch zadań projektu CCMODE uwzględniających zagadnienia certyfikacji lokalnego środowiska rozwojowego. Dalej przedstawiono najważniejsze korzyści wynikające ze stosowania certyfikacji lokalnego środowiska rozwojowego w praktyce; scharakteryzowano aktualny stan i główne kierunki prac badawczych prowadzonych na świecie przez kluczowe ośrodki zajmujące się tą tematyką. Na zakończenie artykułu przedstawiono podstawowe definicje, wymagania, procedury oraz noty aplikacyjne niezbędne do poprawnego prowadzenia procesu certyfikacji lokalnego środowiska rozwojowego bezpiecznych produktów lub systemów IT.

1. WPROWADZENIE

Celem artykułu jest omówienie, na podstawie dostępnej literatury i materiałów konferencyjnych, zagadnień dotyczących certyfikacji środowisk rozwojowych bezpiecznych produktów IT, obecnego stanu badań w tej dziedzinie oraz pokazanie, w jaki sposób wykorzystano przedstawione zagadnienia w ramach prac prowadzonych w projekcie CCMODE.

Obecny rozwój społeczeństwa informacyjnego, wraz z towarzyszącymi mu technikami i narzędziami, nie byłby możliwy bez równoczesnego rozwoju technologii poufności i zaufania. Ważne zadania polegające na wytwarzaniu, przetwarzaniu, przesyłaniu i przechowywaniu danych realizowane są za pomocą różnego typu rozwiązań sprzętowo-programowych, których oczywistym zadaniem jest także zapewnienie odpowiednio skutecznej i wiarygodnej ochrony dla powierzanych zasobów. Jednakże wielu odbiorców produktów IT nie ma odpowiednich kwalifikacji, wiedzy i doświadczenia, aby móc osądzić, czy ich zaufanie do zastosowanej w produkcie ochrony jest uzasadnione i czy wystarczające jest opieranie się w tej kwestii tylko na deklaracjach konstruktora lub sprzedawcy. Źródłem takiego zaufania może być rygorystyczny proces konstruowania oraz niezależna ocena, a następnie certyfikacja produktów, w których zastosowano zabezpieczenia.

Metodyka Common Criteria (CC) opisana w standardzie ISO/IEC 15408 [1], [2], [3] jest podstawową metodyką kreowania uzasadnionego zaufania dla produktów informatycznych, które w terminologii standardu określane są jako przedmiot oceny (ang. *TOE – Target of Evaluation*) i posiadają zabezpieczenia swoich funkcji użytkowych. Inaczej mówiąc, produkty mają zaimplementowane funkcje zabezpieczające, które powinny cechować się uzasadnionym zaufaniem (ang. *assurance*), czyli być źródłem przekonania użytkownika o tym, że produkt spełnia wy-

specyfikowane dla niego cele zabezpieczeń. Uzasadnione zaufanie jest mierzone w skali EAL (ang. *Evaluation Assurance Level*) od minimalnego poziomu EAL1 do maksymalnego poziomu EAL7 [4].

Stosowanie metodyki Common Criteria do oceny zabezpieczeń teleinformatycznych przyczynia się do uzyskania powtarzalności i obiektywności wyników oceny, ale nie jest samo w sobie wystarczające. Wiele z kryteriów oceny wymaga zastosowania dogłębnej wiedzy i intuicji ekspertów, a w celu wzmocnienia spójności wyników oceny, muszą one podlegać dodatkowo procesowi certyfikacji. Jedno z kluczowych pojęć metodyki CC to ocena produktu prowadzona przez niezależną instytucję według uzgodnionych procedur i kryteriów w zakresie spełnienia zakładanych wymagań dotyczących poufności, integralności i dostępności informacji. Pozytywna ocena oznacza, że przedmiot oceny realizuje prawidłowo określone funkcje bezpieczeństwa – występują w nim pożądane zachowania oraz że produkt posiada mierzalny poziom zaufania (EAL) – brak w nim niepożądanych zachowań. Zanim zostanie wystawiony certyfikat, przeprowadza się pracochłonne oceny i testy produktów w akredytowanych i nadzorowanych laboratoriach badawczych [5].

Procesy oceny i certyfikacji mogą obejmować takie typy produktów informatycznych jak: środki sprzętowe, oprogramowanie (w tym układowe), środki sprzętowo-programowe, aplikacje, narzędzia do rozwoju produktów oraz całe systemy. Wyróżnia się trzy rodzaje ocen w zależności od etapu rozwoju produktu: ocena towarzysząca powstawaniu produktu (na etapie planowania, koncepcji, projektu, implementacji lub prototypu) – to podejście jest najbardziej efektywne, gdyż ewentualne braki w zakresie bezpieczeństwa są korygowane już we wczesnym stadium rozwoju produktu; ocena gotowego produktu – obarczona jest dość dużym ryzykiem, gdyż ewentualne błędy projektowe powodujące obniżenie bezpieczeństwa produktu mogą być bardzo trudne do usunięcia, a przez to kosztowne lub wręcz niemożliwe; powtórna ocena nowej wersji produktu – recertyfikacja.

Poddanie produktu procesowi oceny i certyfikacji przynosi wiele korzyści, głównie technicznych i marketingowych, ponieważ wymusza to staranne opracowanie produktu i jego dokumentacji, znacząco podnosi zaufanie – zwłaszcza po ocenie towarzyszącej tworzeniu produktu, ocenione produkty częściej wykorzystywane są do budowy bezpiecznych systemów IT, ułatwia użytkownikom wybór produktów IT o właściwie dobranym poziomie bezpieczeństwa, ułatwia producentom ocenionych produktów wprowadzenie ich na rynki międzynarodowe.

Postępowanie według metodyki CC wymuszające stosowanie rygorystycznych zasad tworzenia produktów IT i pracochłonna ich ocena wpływają na wzrost końcowej ceny tych produktów. Stosowanie komputerowych narzędzi wspomagających, przygotowanie stosownych materiałów dowodowych oraz rozwiązań umożliwiających ich wielokrotne użycie mogą znacząco obniżyć koszty rozwoju, wytwarzania, oceny i certyfikacji bezpiecznych produktów. Więcej szczegółowych informacji na temat procesów projektowania zabezpieczeń według metodyki CC czytelnik może uzyskać m.in. z pracy [4]. W artykule skoncentrowano się na metodzie oceny i certyfikacji wymagań środowiska rozwojowego produktów IT według, coraz bardziej ostatnio popularyzowanego w społeczności Common Criteria, podejścia certyfikacji lokalnego środowiska rozwojowego (ang. *Site Certifiaction*), które w dalszej części artykułu w skrócie będziemy określać pojęciem certyfikacji środowiska lokalnego. Proces certyfikacji środowiska lokalnego pozwala na uzyskanie oszczędności czasu i kosztów oceny wytwarzanego produktu poprzez efektywne, wielokrotne użycie materiału dowodowego związanego z klasą wymagań metodyki CC, która wspiera cykl życia produktu.

2. PROJEKT CCMODE W KONTEKŚCIE CERTYFIKACJI ŚRODOWISKA LOKALNEGO

Celem projektu „Środowisko rozwojowe produktów i systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa – CCMODE" jest opracowanie metodyki i narzędzi do budowy i zarządzania środowiskami rozwojowymi produktów i systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa z zamiarem ich certyfikacji. Projekt jest realizowany w ramach Programu Operacyjnego „Innowacyjna Gospodarka" (POIG 1.3.1)[1], współfinansowanego ze środków Unii Europejskiej (więcej szczegółowych informacji można znaleźć na witrynie internetowej projektu)[2]. Założenia i wstępne wyniki projektu opisano w referacie [4]. Poszczególne zadania projektu ukierunkowane są na zgromadzenie odpowiedniej wiedzy, opracowanie wzorców materiałów dowodowych, opracowanie metodyk postępowania oraz narzędzi, które będą służyły do budowy środowisk rozwojowych przez różnych przedsiębiorców. W środowiskach tych będą oni mogli konstruować, produkować i utrzymywać produkty IT z mierzalnym poziomem uzasadnionego

[1] http://www.poig.gov.pl
[2] http://www.ccmode.emag.pl

zaufania do wbudowanych w nie zabezpieczeń. Artykuł stanowi m.in. podsumowanie prac wykonanych w zakończonych już dwóch zadaniach projektu.

Wynikiem zadania 1 projektu CCMODE jest model odniesienia środowiska rozwojowego, który uwzględnia wszystkie fazy cyklu życia dla różnych typów produktów sprzętowych i programowych. Model odniesienia uwzględnia także struktury organizacyjne środowisk budowanych zgodnie z podejściem certyfikacji środowiska lokalnego, które pozwala na dekompozycję pełnego środowiska rozwojowego na moduły zwane środowiskami lokalnymi (ang. *sites*), które mogą znajdować się w różnych fizycznych lokalizacjach, i w których realizowane są poszczególne fazy cyklu życia produktu. Certyfikaty środowisk lokalnych stanowią następnie istotny wkład podczas oceny produktów w nich wytwarzanych, gdyż pozwalają na wielokrotne użycie raz ocenionego materiału dowodowego, z czym wiążą się znaczne oszczędności czasu i kosztów.

Wynikiem zadania 2 projektu CCMODE jest szczegółowy model otwartego, modułowego środowiska rozwojowego, który powstał na podstawie opracowanego w zadaniu 1 modelu odniesienia. Opracowano wzorce projektowe, które będą wymagały odpowiedniego dokończenia, skonfigurowania i przystosowania do potrzeb i uwarunkowań konkretnego środowiska, w którym będą wdrażane. W ramach zadania opracowano szczegółowy wzorzec zadania zabezpieczeń dla środowiska lokalnego (ang. *SST – Site Security Target*) oraz wykonano analizę wymagań klasy AST przeznaczonej do oceny tego zadania zabezpieczeń. Opracowano także wzorce materiału dowodowego do oceny środowiska, oparte na wymaganiach klasy ALC, wspierającej cykl życia produktu w ujęciu tradycyjnym (wymagania z trzeciej części normy CC [3]) oraz w ujęciu zgodnym z certyfikacją środowiska lokalnego (do wymagań klasy ALC dodaje się noty aplikacyjne uwzględniające wymogi certyfikacji środowiska lokalnego). W celu prawidłowego stosowania procesu certyfikacji środowiska lokalnego podczas oceny środowiska i powstających w nim produktów należy kierować się szeregiem wymagań, zasad i procedur, które w niniejszym artykule zostały opisane w najważniejszych punktach.

Obecnie trwające prace w ramach zadania 3 projektu CCMODE zmierzają do opracowania metodyki wyboru właściwych modułów wzorcowych, ich skonfigurowania, dostosowania i zintegrowania w spójny system zarządzania środowiskiem rozwojowym. W ramach niej powstaną m.in.: metoda transformacji modułu wzorcowego zadania zabezpieczeń środowiska lokalnego w zadanie zabezpieczeń danego środowiska oraz metoda transformacji modułów wzorcowych materiału dowodowego w materiał dowodowy przygotowywany do oceny danego środowiska lokalnego.

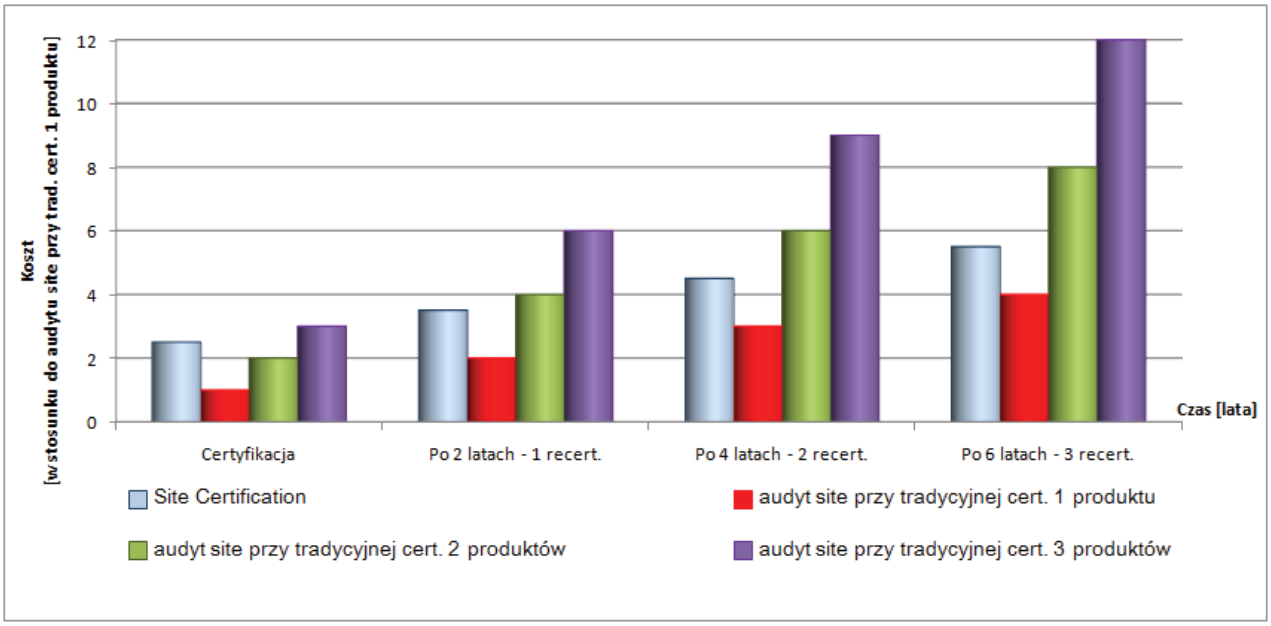
Opisane wyżej pierwsze trzy zadania projektu wskazują, że jest on zgodny z koncepcją certyfikacji środowiska lokalnego, co jest jednym z elementów, które decydują o jego innowacyjnym charakterze w skali międzynarodowej.

3. MOTYWACJA TOWARZYSZĄCA CERTYFIKACJI ŚRODOWISK LOKALNYCH

Rosnąca potrzeba certyfikacji środowisk lokalnych wynika z możliwości zaoszczędzenia czasu i redukcji kosztów prowadzenia procesu oceny powstających w tych środowiskach produktów. Duże możliwości w tym zakresie daje ponowne użycie (ang. *reusability*) materiału dowodowego ocenionego według wymagań klasy ALC, konstruowanego przy zastosowaniu tych samych podprocesów i czynności, występujących w ramach danej fazy cyklu życia realizowanej w lokalnym środowisku rozwojowym.

Wiele środowisk rozwojowych składa się z wielu lokalnych środowisk zlokalizowanych w różnych miejscach świata. Sensowne jest takie podzielnie środowiska rozwojowego, aby jego poszczególne części reprezentowały poszczególne fazy cyklu życia produktu. Części te mogą być poddane ocenie i certyfikacji zgodnie z opisanymi w dalszej części artykułu odpowiednimi wymaganiami klasy ALC. Certyfikat środowiska rozwojowego może być później wielokrotnie używany w ramach ocenionych wymagań klasy ALC i jednocześnie zadeklarowanych w zadaniu zabezpieczeń (ang. *ST – Security Target*) dla produktu, bez konieczności ponownej oceny tych samych wymagań. W przypadku wprowadzenia zmian w danym środowisku lokalnym, nie ma potrzeby ponownej certyfikacji całego środowiska rozwojowego, ale tylko jego zmienionej części, co daje możliwości bardziej efektywnego i optymalnego użycia certyfikowanych części środowiska rozwojowego, czyli certyfikowanych środowisk lokalnych.

Standardowy proces certyfikacji, polegający na przygotowaniu produktu do oceny zgodnie z wymaganiami standardu CC, wymaga opracowania wielu dokumentów stanowiących materiał dowodowy na spełnienie wymagań na uzasadnione zaufanie do zabezpieczeń (ang. *SAR – Security Assurance Requirements*). Zakres i rygoryzm dostarczanych dokumentów rośnie wraz z poziomem EAL uzasadnionego zaufania do zabezpieczeń produktu.



Rys. 1. Porównanie kosztów certyfikacji tradycyjnej i certyfikacji środowiska lokalnego (opracowanie własne na podstawie [6])

Jedną z grup wymagań SAR jest wspomniana wcześniej klasa ALC. Jeżeli dany produkt jest konstruowany, produkowany i testowany odpowiednio w kilku różnych lokalizacjach (środowiskach lokalnych), do oceny produktu należy przedstawić materiał dowodowy spełnienia wymagań klasy ALC dla każdej z tych lokalizacji. Dodatkowo w każdej z tych lokalizacji musi być przeprowadzony audyt przez oceniających. Często zdarza się tak, że wielu producentów korzysta z tych samych linii produkcyjnych lub laboratoriów testujących podzespoły tego samego typu. W takich sytuacjach każdy z tych producentów potrzebuje podobnego lub nawet identycznego materiału dowodowego niezbędnego do oceny swoich produktów, a oceniający muszą wielokrotnie przeprowadzać audyt środowisk lokalnych.

W celu uniknięcia niepotrzebnego, wielokrotnego wykonywania ocen według tych samych wymagań dla różnych produktów IT, niemiecki urząd ds. bezpieczeństwa informacji BSI, będący również jednostką certyfikującą CC, wypracował procedury certyfikacji środowisk lokalnych. Certyfikat środowiska lokalnego zwalnia konstruktorów produktów IT od przedstawiania dodatkowego materiału dowodowego zgodnego z wymaganiami klasy ALC. Korzyści płynące z procedur certyfikacji środowiska lokalnego wynikają przede wszystkim z obniżonych kosztów certyfikacji wielu produktów, które są konstruowane, wytwarzane i testowane w tych samych środowiskach lokalnych. Niemieccy specjaliści [6], którzy brali udział w pierwszej certyfikacji [7] wykazali, że już przy trzech produktach korzystających z tych samych certyfikowanych środowisk lokalnych, jest ona bardziej opłacalna, mimo że początkowy koszt oceny tych środowisk jest około 2,5 razy większy niż koszt oceny tych samych środowisk według tradycyjnej certyfikacji produktu (co pokazano na rys. 1). Zysk jest jeszcze większy przy kolejnych recertyfikacjach, ponieważ koszt recertyfikacji środowiska lokalnego, wymagany raz na 2 lata, jest taki sam jak koszt ponownego audytu środowiska lokalnego przy tradycyjnej recertyfikacji.

Certyfikacja środowisk lokalnych jest zatem tym korzystniejsza, im więcej produktów jest w nich wytwarzanych oraz im dłużej są te środowiska wykorzystywane do wytwarzania produktów IT z myślą o ich późniejszej certyfikacji według wymagań standardu Common Criteria.

4. CERTYFIKACJA ŚRODOWISKA LOKALNEGO – AKTUALNY STAN BADAŃ NA ŚWIECIE

Prace nad doskonaleniem metodyki CC dotyczą między innymi badań nad tworzeniem i certyfikacją złożonych środowisk rozwojowych. Dekompozycja faz cyklu życia produktu na poszczególne lokalne środowiska rozwojowe wymusza konieczność oceny poprawności ich zastosowania tak, aby cykl życia produktu pozostawał spójny, oraz zwraca uwagę na problemy dotyczące oceny produktów powstających w środowiskach składających się z kilku środowisk lokalnych. Wiodące prace w tym obszarze koordynuje niemiecki BSI, współpracując z firmami ATSEC, TNO, Philips, IBM oraz

T-system. Prace nad certyfikacją środowisk lokalnych zostały rozpoczęte w 2006 r. i trwają do dzisiaj, obejmując twórcze przystosowanie metodyki Common Criteria do opracowania optymalnego środowiska rozwojowego dla określonej grupy produktów i poddania go następnie procesowi certyfikacji.

W dalszej części artykułu zostanie przedstawiony krótki przegląd prac badawczych wykonywanych na świecie w tym zakresie na podstawie materiałów dostępnych na portalu standardu CC[3], dokumentacji wydawanej przez BSI oraz komitet ds. rozwoju CC (ang. *CCDB – Common Criteria Development Board*), oraz przewodników lub dokumentacji obowiązkowej (ang. *mandatory documents*) do standardu CC wydawanej przez innych realizatorów badań. Opis prac możliwy był także na podstawie dostępnych materiałów z odbywających się rokrocznie Międzynarodowych Konferencji CC (*ICCC – International Common Criteria Conference*). Dotychczasowy postęp prac można było także ocenić na podstawie udostępnionych dokumentów stanowiących szablony raportów technicznych z oceny środowiska (ang. *ETR – Evaluation Technical Report*), szablonu zadania zabezpieczeń środowiska lokalnego SST oraz pierwszych ocenionych zadań zabezpieczeń SST dla wybranych środowisk rozwojowych dla produktów takiego typu jak karty inteligentne (ang. *smart cards*) i układy scalone.

4.1. Geneza i rozwój idei certyfikacji środowiska lokalnego

Pierwsze spostrzeżenia i wyniki prac nad rozwojem procesu certyfikacji środowiska lokalnego przedstawione zostały przez BSI na VII Międzynarodowej Konferencji CC (7th ICCC), która odbyła się w 2006 r., w Hiszpanii [8].

BSI zaprezentowało poszczególne procedury procesu certyfikacji środowiska rozwojowego oraz pierwsze wyniki próbnego zastosowania tego procesu w praktyce, a także omówiło strukturę oraz podstawowe wytyczne konstruowania zadania zabezpieczeń SST. Na konferencji zwrócono uwagę na wzrastające zapotrzebowanie konstruktorów różnego rodzaju produktów IT na certyfikaty środowisk rozwojowych oraz na korzyści wynikające ze stosowania certyfikacji w jednym lub kilku lokalnych środowiskach rozwojowych danego produktu. Wśród korzyści wymieniano redukcję czasu i kosztów dla ocen prowadzonych w krótkim przedziale czasu dla produktów wytwarzanych w tych samych warunkach, możliwość rozszerzenia CC o aspekty dotyczące zarządzania bezpieczeństwem informacji oraz możliwości wejścia produktów certyfikowanych według CC na nowe rynki.

W prezentowanych materiałach podano także definicję lokalnego środowiska rozwojowego i jego zakresu, omówiono podstawowe procedury certyfikacji, integracji i łączenia, przedstawiono korzyści procesu certyfikacji środowisk lokalnych, omówiono także zestaw minimalnych i opcjonalnych wymagań uzasadniających zaufanie (SAR) niezbędnych do rozpoczęcia certyfikacji środowiska lokalnego (zagadnienia te zostaną bardziej szczegółowo omówione w dalszej części artykułu). Prezentowane podejście spotkało się z pozytywnymi reakcjami zainteresowanych stron, które wyrażały postulaty, aby ustanowić proces certyfikacji środowiska lokalnego jako część standardu CC, jednocześnie kilkunastu konstruktorów zgłosiło chęć uczestnictwa w kolejnych, próbnych certyfikacjach swoich środowisk rozwojowych.

Należy zaznaczyć, że na tej samej konferencji przedstawiono już wyniki pierwszego próbnego zastosowania procesu certyfikacji środowiska lokalnego na przykładach dwóch środowisk rozwojowych, z których jedno przeznaczone było do wytwarzania produktów sprzętowych, a drugie dla produktów programowych [9]. Jako podstawa do prowadzenia testów wykorzystana została dokumentacja opisu procesu w wersji 0.93 dostępna od kwietnia 2006 r., wymagania klasy AST dla oceny zadania zabezpieczeń SST środowiska lokalnego dostępne od lutego 2006 r., wnioski z dyskusji na temat procesu certyfikacji przeprowadzonych w styczniu i kwietniu 2006 r. i zorganizowanych przez komitety zarządzający (ang. *CCMB – Common Criteria Management Board*) i rozwojowy (CCDB) do spraw standardu CC, natomiast próbne zastosowanie procesu rozpoczęło się w maju 2006 r.

Głównymi celami badań było potwierdzenie spodziewanych korzyści ze stosowania certyfikacji środowisk lokalnych. W trakcie badań zdefiniowano odpowiednie środowiska lokalne oraz utworzono ich zadania zabezpieczeń SST. Prace koordynowane przez BSI były wspierane przez firmy IBM i AT-SEC w zakresie testów środowiska dla produktów programowych oraz przez firmy Philips i T-Systems w zakresie testów środowiska dla produktów sprzętowych.

Wykonane prace badawcze potwierdziły, że certyfikacja środowiska lokalnego umożliwia:

- uniknięcie dublowania prac związanych z oceną wymagań klasy ALC pomiędzy różnymi procesami oceny;
- zmniejszenie kosztów oceny i certyfikacji;
- uniezależnienie certyfikatu środowiska lokalnego od certyfikatu produktu;

[3] http://www.commoncriteriaportal.org

- wielokrotne używanie certyfikatów środowisk lokalnych przez różne laboratoria oceniające i narodowe organy certyfikujące.

Wypracowano także następujące wnioski z testowego zastosowania procesu certyfikacji środowiska lokalnego:

- proces daje się łatwo zastosować i sprawdził się w obydwu testowych środowiskach;
- proces jest na tyle elastyczny, aby mógł być stosowany we wszystkich rodzajach środowisk rozwojowych;
- spodziewane korzyści w redukcji czasu i kosztów oceny rosną podczas wielokrotnego wykorzystywania danego środowiska lokalnego;
- wyzwaniem dla procesu certyfikacji jest poprawne ustalanie zakresu (fizycznych i logicznych granic) środowisk lokalnych, które mają być certyfikowane.

Po kilku podobnie wykonanych testach w ramach grupy roboczej ISCI (ang. *Information Security Certificate Initiative*) idea procesu certyfikacji środowiska lokalnego została przekształcona w konkretny dokument pomocniczy dla standardu CC w postaci poradnika [10], który został opracowany przez BSI. Dokument ten definiuje proces, kryteria, metodykę oraz interpretacje dla oceny i certyfikacji środowisk lokalnych zgodnych ze standardem CC.

4.2. Pierwszy certyfikat, aktualizacja poradników i szablonów

Po wydaniu poradnika dla prowadzenia procesu oceny środowiska lokalnego [10], grupa robocza organizacji Eurosmart zdecydowała się przeprowadzić próbną ocenę wybranych środowisk rozwojowych. Należy tutaj wspomnieć, że Eurosmart[4] jest międzynarodową organizacją non-profit, mającą swą siedzibę w Brukseli i reprezentującą przemysł inteligentnych zabezpieczeń dla wielosektorowych zastosowań. W testowym zastosowaniu procesu certyfikacji środowiska lokalnego brały udział również Infineon oraz NXP wspierane przez BSI. Pierwszym krokiem w procesie oceny środowiska lokalnego było utworzenie jego zadania zabezpieczeń SST. Eurosmart było sponsorem utworzenia odpowiedniego szablonu dokumentu SST, który został ostatecznie napisany przez T-Systems we współpracy z wcześniej wymienionymi firmami oraz BSI. Przeprowadzony test pokazał, że potrzebnych jest jeszcze wiele aktualizacji i dodatkowych wskazówek w celu dokładniejszego wyjaśnienia procesu, co doprowadziło do wydania nowych uaktualnionych poradników i szablonów dokumentów. Ostatecznie pierwszy certyfikat dla środowiska lokalnego został wydany 31 lipca 2009 r. Po tym sukcesie, w innych środowiskach lokalnych rozpoczęto kolejne procesy certyfikacji, a certyfikaty wraz z zadaniami zabezpieczeń SST opublikowano na portalu BSI[5].

W latach 2008 i 2009 na Międzynarodowych Konferencjach CC (ICCC), organizacja Eurosmart wraz ze swoimi partnerami przedstawiła wyniki kolejnych etapów prac związanych z praktycznym sprawdzeniem procesu certyfikacji środowiska lokalnego i przyznaniem pierwszego certyfikatu.

Na IX konferencji ICCC w 2008 r. [11] podkreślano, że głównym powodem, dla którego wypracowano proces certyfikacji środowiska lokalnego jest duża złożoność produktów, których części składowe mogą być projektowane i wytwarzane w wielu środowiskach rozwojowych i produkcyjnych, tak jak obecnie ma to miejsce w przypadku wielu układów scalonych lub kart inteligentnych. Zauważono także, że wiele operacji rozwojowych i produkcyjnych w procesach przemysłowych jest niezależnych od samego produktu, dlatego zadania oceny związane z tymi operacjami (dotyczącymi aspektów środowiska zgodnie z wymaganiami klasy ALC) można oddzielić od procesu oceny samego produktu. To pozwoli na wielokrotne użycie wyników oceny środowiska lokalnego podczas oceny samego produktu według kryteriów CC, niezależnie dla jednego lub kilku produktów, konstruowanych przez tego samego lub różnych producentów. Na konferencji przedstawiono również harmonogram pierwszego testowego zastosowania procesu oceny i certyfikacji środowiska lokalnego na przykładzie niemieckiego producenta zabezpieczeń dla paszportów elektronicznych, firmy HID. Cele prac zostały wyznaczone na:

- wykonanie oceny i certyfikacji środowiska lokalnego przy wykorzystaniu wytycznych zawartych w poradniku [10];
- wypracowanie szablonu zadania zabezpieczeń SST – ogólnego dokumentu w rodzaju poradnika zawierającego noty aplikacyjne, który będzie służył jako podstawa tworzenia innych dokumentów SST dla różnych środowisk lokalnych i różnych procesów w nich stosowanych;
- utorowanie drogi dla następnych certyfikacji – zdefiniowanie i wyjaśnienie jak poszczególne zagadnienia mają być uwzględniane w zadaniu zabezpieczeń SST; zdefiniowanie i wyjaśnienie w jaki sposób mają być spełnione pozytywnie poszczególne jednostki oceny dotyczące SST; zapewnienie przewodników dla konstruktorów i oceniających; zapewnienie szablonów dla oceniających.

[4] http://www.eurosmart.com

[5] https://www.bsi.bund.de

Na X konferencji ICCC w 2009 r. podsumowano osiągnięte wyniki pierwszej oceny i certyfikacji środowiska lokalnego [6], [12], i tak:

- utworzono zadanie zabezpieczeń SST środowiska lokalnego firmy HID – luty 2009 r.;
- sporządzono raport z oceny wymagań klasy AST – luty 2009 r.;
- sporządzono raport z audytu środowiska lokalnego – luty 2009 r.;
- sporządzono raport z oceny wymagań klasy ALC – marzec 2009 r.;
- sporządzono raport techniczny z oceny (ETR) środowiska lokalnego – marzec 2009 r.;
- utworzono szablony dokumentacji i poradniki – marzec 2009 r.;
- wydano pierwszy certyfikat dla środowiska lokalnego – lipiec 2009 r.

Powyższe wyniki pozwoliły ponownie potwierdzić, że jakkolwiek początkowy koszt certyfikacji środowiska lokalnego jest wyższy niż początkowy koszt certyfikacji samego produktu, to jednak recertyfikacja środowiska wykonywana jest tylko raz na 2 lata i nie zależy od liczby klientów wykorzystujących dane środowisko rozwojowe, co w dłuższej perspektywie czasu przynosi oszczędności w kosztach oceny środowiska rzędu do 40% względem standardowego procesu oceny. W wyniku przeprowadzonej weryfikacji procesu certyfikacji środowiska lokalnego zaktualizowano i wydano następujące materiały pomocnicze w postaci szablonów dokumentów oraz podręczników:

- suplement [13] dla podręcznika certyfikacji środowiska lokalnego [10] – zawiera wskazówki ułatwiające poprawne sporządzenie dokumentacji; zawiera jednostki oceny dla oceniających nieuwzględnione w podręczniku [10]; zawiera wskazówki jak usuwać braki w dokumentacji (interpretacje, korekty);
- dokument szczegółowo opisujący strukturę i zawartość raportu technicznego oceny ETR [14];
- szablon raportu z oceny spełnienia wymagań klasy AST w zadaniu zabezpieczeń SST [15];
- szablon raportu z oceny spełnienia wymagań klasy ALC w materiale dowodowym [16];
- szablon zadania zabezpieczeń SST [17].

Podsumowując, pierwsze zastosowanie procesu certyfikacji środowiska lokalnego zakończyło się sukcesem. Powstało kilka dokumentów uzupełniających, które wspomagają oceniających i konstruktorów w stosowaniu procesu. Uzyskano oszczędności czasu i kosztów po obydwu stronach – oceniającego i konstruktora. Certyfikat został wydany przez BSI, a członkowie porozumienia CCRA (ang. *Common Criteria Recognition Arrangement*) zaakceptowali proces certyfikacji środowiska lokalnego jako część procesu oceny produktu. Próby certyfikacji swoich środowisk lokalnych rozpoczęły inne firmy, np. SMARTRAC i irlandzki oddział firmy HID, których zadania zabezpieczeń w wersjach skróconych (ang. *lite*) [18], [19] umieszczono na stronach internetowych BSI. Obecnie trwają prace nad standaryzacją wymagań na środki zabezpieczeń wykorzystywane w procesie certyfikacji środowiska lokalnego, a do prac dołączyła grupa robocza JIL (ang. *Joint Interpretation Library*), która ma opracować dokument dotyczący prowadzenia audytów środowisk lokalnych (ang. *Site Visits*).

5. WYMAGANIA PROCESU CERTYFIKACJI

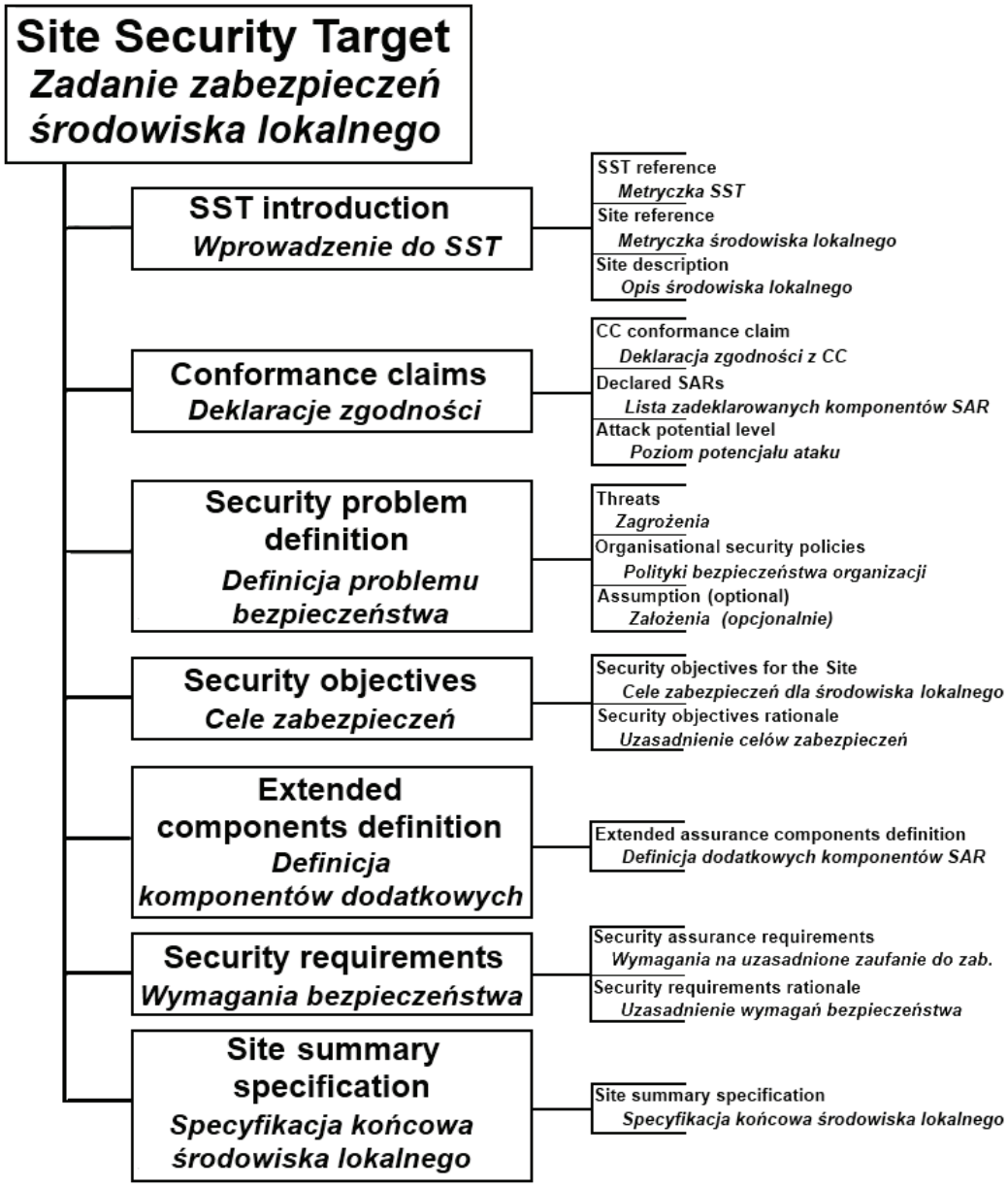
Jak już wyżej wspomniano, wiele środowisk rozwojowych jest bardzo złożonych i może składać się z wielu środowisk lokalnych w różnych lokalizacjach. Podzielenie środowiska rozwojowego na części, reprezentujące poszczególne fazy cyklu życia produktu, przynosi wiele korzyści, ponieważ części te mogą być poddane ocenie i certyfikacji zgodnie z opisanymi szczegółowo w dalszej części artykułu, odpowiednimi wymaganiami klasy ALC. Raz wydany certyfikat środowiska lokalnego może być później wielokrotnie wykorzystywany podczas oceny produktu. Proces certyfikacji środowiska lokalnego wymaga przedstawienia materiału dowodowego w postaci zadania zabezpieczeń SST, w którym należy wykazać, że środowisko lokalne związane z daną fazą cyklu życia produktu spełnia minimalne wymagania klasy ALC. Wymagania te zostaną krótko opisane w dalszej części tego rozdziału.

5.1. Definicja środowiska lokalnego

Konstruktorzy mogą swobodnie definiować części lub całość środowiska rozwojowego istniejącego lub przewidywanego dla rozwoju produktu jako środowiska lokalne, przy czym środowisko lokalne:

- może być pełnym środowiskiem rozwojowym;
- może stanowić jedną fizyczną lokalizację, może być częścią lokalizacji lub może obejmować wiele różnych lokalizacji;
- może składać się z jednej jednostki organizacyjnej, może być częścią jednostki organizacyjnej lub obejmować wiele jednostek organizacyjnych.

Zakres środowiska lokalnego jest określany za pomocą jego logicznych i fizycznych granic. Granicę logiczną opisuje faza cyklu życia produktu, jaką realizuje dane środowisko lokalne. Granica fizyczna jest definiowana przez jedną lub więcej fizycznych lokalizacji środowiska lokalnego.



Rys. 2. Struktura zadania zabezpieczeń środowiska lokalnego (opracowanie własne na podstawie [10])

5.2. Zadanie zabezpieczeń SST

Pierwszym krokiem do oceny środowiska lokalnego jest przygotowanie jego zadania zabezpieczeń, które definiuje zakres środowiska lokalnego i opisuje, jak środowisko spełnia wymagania uzasadniające zaufanie do zabezpieczeń SAR. Kryteria i metodyka oceny zadania zabezpieczeń SST są wyrażone poprzez wymagania klasy AST.

Jak pokazano na rys. 2 zadanie zabezpieczeń SST posiada następującą strukturę:

- wprowadzenie do SST (ang. *SST Introduction*) – zawiera metryki dokumentu i środowiska oraz opis środowiska lokalnego;
- deklaracje zgodności (ang. *CCL – Conformance claims*) – deklaracja wskazuje m.in. z jaką wersją standardu CC oraz z jakimi komponentami klasy ALC zgodny jest dokument SST;
- definicja problemu bezpieczeństwa (ang. *SPD – Security problem definition*) – opisuje zagrożenia, którym środowisko lokalne musi się przeciwstawić, polityki bezpieczeństwa organizacji (ang. *OSP – Organisational Security Polices*) oraz założenia dotyczące otoczenia środowiska lokalnego;
- cele zabezpieczeń dla środowiska rozwojowego (ang. *Security objectives for the site*) – wskazują jak środowisko lokalne przeciwstawia się zagrożeniom i jak wymusza polityki bezpieczeństwa organizacji;
- definicja komponentów dodatkowych (ang. *ECD – Extended components definition*) – definicje nowych komponentów SAR, niewystępujących w trzeciej części normy CC;

- wymagania bezpieczeństwa (ang. *Security requirements*) – wyrażenie celów zabezpieczeń za pomocą wymagań SAR zapisanych w postaci komponentów uzasadniających zaufanie z trzeciej części normy CC;
- specyfikacja końcowa środowiska lokalnego (ang. *SSS – Site summary specification*) – podsumowanie tego, w jaki sposób w środowisku lokalnym wdraża się wymagania na uzasadnione zaufanie SAR.

5.3. Minimalne i opcjonalne wymagania dla certyfikacji środowiska lokalnego

Każde środowisko lokalne poddawane ocenie musi spełniać minimalny zbiór wymagań. Podstawowym wymaganiem jest stosowanie w każdym z nich systemu zarządzania konfiguracją (ang. *CM – Configuration Management*), który unikalnie identyfikuje wszystkie elementy konfiguracji danego środowiska. Drugim, obligatoryjnym wymaganiem jest zapewnienie bezpieczeństwa środowiska lokalnego, gwarantujące poufność i integralność procesów oraz wyników tych procesów objętych ocenianym środowiskiem lokalnym dla produktów lub ich części. Minimalny zbiór wymagań dla środowisk lokalnych jest następujący:

- ALC_CMC.3 lub wyższy – kontrola uprawnień – system CM powinien dostarczyć środki dopuszczające tylko autoryzowane zmiany w liście konfiguracji;
- ALC_CMS.3 lub wyższy – zastosowanie systemu zarządzania konfiguracją dla reprezentacji implementacji[6] – lista konfiguracji powinna zawierać: produkt, wszystkie dowody oceny wymagane przez komponenty SAR, części składające się na produkt oraz reprezentację implementacji;
- ALC_DVS.1 lub wyższy – identyfikacja środków bezpieczeństwa – dokumentacja bezpieczeństwa środowiska rozwojowego powinna zawierać wszystkie fizyczne, proceduralne, osobowe i inne środki bezpieczeństwa, konieczne dla ochrony poufności i integralności fazy projektowania i implementacji produktu w jego środowisku rozwojowym.

Procedura łączenia, która będzie omówiona w dalszej części artykułu, umożliwia połączenie wielu różnych środowisk lokalnych w większe lub nawet pełne środowisko rozwojowe. Ostateczne stwierdzenie, czy środowiska lokalne do siebie pasują w sposób dokładny, może być dostarczone przez definicję pełnego cyklu życia TOE zgodnie z wymaganiami komponentu ALC_LCD.1 lub hierarchicznie wyższego ALC_LCD.2.

Należy również pamiętać, że wszystkie wymagania zależne dla komponentów klasy ALC muszą być także spełnione. Jednak certyfikacja środowisk lokalnych oraz procedura łączenia nie mają powiązania z rzeczywistym produktem, więc zależności, które są wymaganiami spoza klasy ALC nie muszą być spełnione. Zależności te staną się istotne podczas procedury integracji, w której produkt jest głównym elementem analiz.

Opcjonalne wymagania dla środowisk lokalnych stanowią pozostałe wymagania z klasy ALC, które deklarowane są dodatkowo (lub dla wyższych poziomów EAL) względem wymagań minimalnych. Wymagania opcjonalne obejmują:

- wymagania wszystkich pozostałych komponentów klasy ALC nie wymienione jako obowiązkowe;
- wymagania rodziny ALC_FLR – usuwanie usterek (ang. *Flaw remediation*), związane ze specyficznymi fazami cyklu życia, których spełnienie weryfikuje procedura łączenia.

Wymagania minimalne muszą być spełnione przez wszystkie środowiska lokalne posiadające certyfikaty, w przeciwieństwie do wymagań opcjonalnych. Przykładem jest sytuacja, gdy dane wymaganie opcjonalne jest obowiązkowe dopiero na wyższym poziomie EAL przy ocenie produktu (np. ALC_TAT jest wymagane dopiero od EAL4 i mimo że narzędzia do wykonania procesów projektowania i programowania są tutaj niezbędne, to dla niższych EAL nie ma potrzeby ich ewidencjonowania).

5.4. Ogólne noty aplikacyjne dla wymagań klasy ALC

Poniżej opisano podstawowe noty aplikacyjne dla wymagań klasy ALC w kontekście procesu certyfikacji środowiska lokalnego.

Interpretacja produktu IT w kontekście certyfikacji środowiska lokalnego

Zgodnie z częścią 1 standardu CC, ocena produktu IT może przebiegać równolegle do jego rozwoju. Oznacza to, że badanie środowiska lokalnego, zgodnie z wymaganiami ALC, może odbywać się w obecności jeszcze nieukończonego produktu. Sensowna wydaje się implementacja środków bezpieczeństwa w środowisku lokalnym przed rozpoczęciem wytwarzania rzeczywistego produktu. Zatem większość wymagań klasy ALC może zostać zaimplementowana w środowisku lokalnym bez udziału produktu. Tylko niektóre wymagania są ściśle połączone z produktem i traktują go jako przedmiot oceny w procesie certyfikacji. W przypadku tych wymagań należy przenieść punkt zainteresowania raczej na badanie istnienia samych procesów niż aktualnych wyników, które dają te procesy. Przykładem może być wymaganie ALC_CMC.x.1C dotyczące sprawdzenia unikalnego oznaczenia produktu. W tym przypadku ważniejsze jest sprawdzenie, czy istnieje

[6] https://www.bsi.bund.de

odpowiedni proces zapewniający poprawne etykietowanie produktu, a nie sprawdzenie samych etykiet.

Elementy konfiguracji w procesie certyfikacji środowiska lokalnego

W procesie certyfikacji środowiska lokalnego należy dokonać następującego rozróżnienia elementów konfiguracji:

- elementy konfiguracji niezwiązane z produktem lub jego częścią (np. narzędzia programistyczne, dokumentacja ALC), które nie wymagają żadnych dodatkowych interpretacji, a kryteria ALC mogą być stosowane zgodnie z metodyką CC,
- elementy konfiguracji ściśle związane z produktem lub jego częścią (np. dokumentacja projektowa, reprezentacja implementacji), które wymuszają, podczas oceny środowiska, skupienie się na procesach zarządzających tymi elementami konfiguracji.

Zależności i dokumenty wejściowe

Jak już opisano, wszystkie wymagania zależne dla wymagań komponentów ALC muszą być spełnione. Jednak certyfikacja środowiska lokalnego oraz procedura łączenia nie mają powiązania z rzeczywistym produktem, więc te zależności, które są wymaganiami spoza klasy ALC, nie muszą być spełnione. Zależności te staną się istotne podczas procedury integracji w procesie certyfikacji środowiska lokalnego, gdzie produkt staje się właściwym przedmiotem analizy.

Dokumenty wejściowe wymagane przez klasę ALC do oceny środowisk lokalnych są istotne, jeśli nie są związane z konkretnym produktem. Dokumenty specyficzne dla produktu (np. ST, reprezentacja implementacji) będą przedmiotem rozważań dopiero w procedurze integracji.

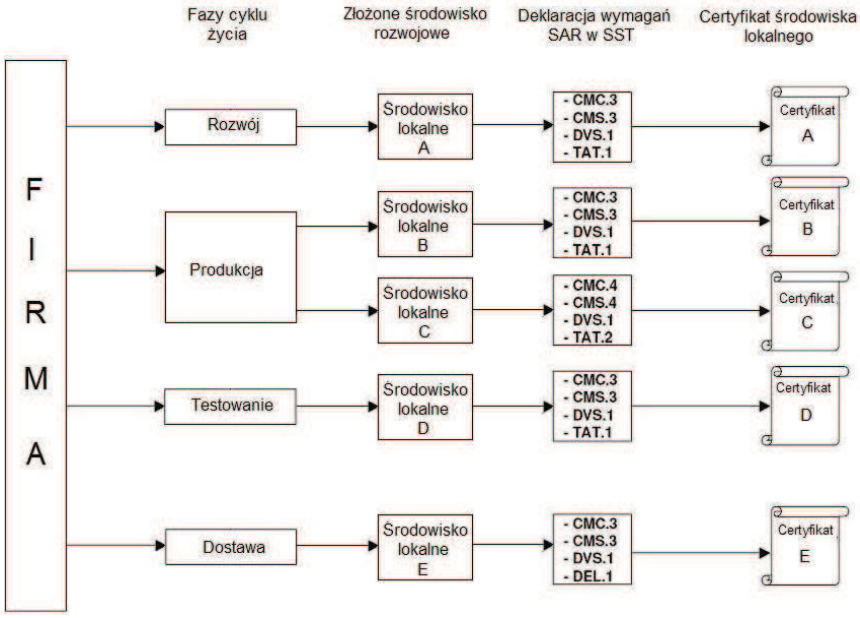
6. PROCEDURY PROCESU CERTYFIKACJI ŚRODOWISKA LOKALNEGO

Proces certyfikacji środowiska lokalnego można podzielić na trzy niezależne procedury: certyfikacji środowiska lokalnego; integracji certyfikatów środowisk lokalnych (ang. *Site Certificate Integration*) oraz łączenia (ang. *Splicing*).

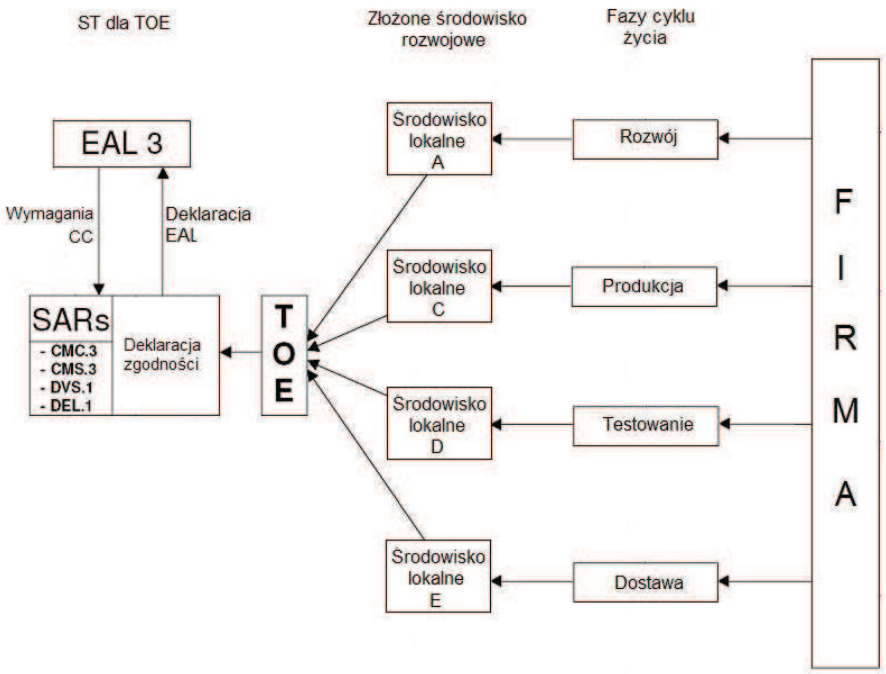
Procedury te są szczegółowo opisane w przewodniku [10], a w niniejszym artykule zostaną przybliżone jedynie ich główne założenia i cele, dotyczące cyklu życia produktu opracowywanego i tworzonego w środowiskach lokalnych.

6.1. Certyfikacja środowiska lokalnego

Procedura certyfikacji środowiska lokalnego opisuje wszystkie niezbędne kroki, które muszą zostać wykonane w celu otrzymania certyfikatu dla środowiska lokalnego lub złożonego środowiska tworzącego pełne środowisko rozwojowe. Punktem wyjścia dla procedury jest zdefiniowanie zakresu każdego środowiska lokalnego, realizującego co najmniej jedną fazę cyklu życia produktu. Definicja i opis zakresu środowiska lokalnego zawarta jest w jego indywidualnym zadaniu zabezpieczeń (SST), tak jak to pokazuje rys. 3, w którym opisano także wymagania uzasadniające zaufanie klasy ALC uwzględniane podczas oceny danego środowiska lokalnego. Po pozytywnej ocenie i certyfikacji zadań zabezpieczeń wydawany jest certyfikat dla danego środowiska lokalnego.



Rys. 3. Certyfikacja środowisk lokalnych (opracowanie własne na podstawie [10])



Rys. 4. Integracja certyfikatów środowisk lokalnych w procesie oceny produktu (opracowanie własne na podstawie [10])

6.2. Integracja certyfikatów środowisk lokalnych

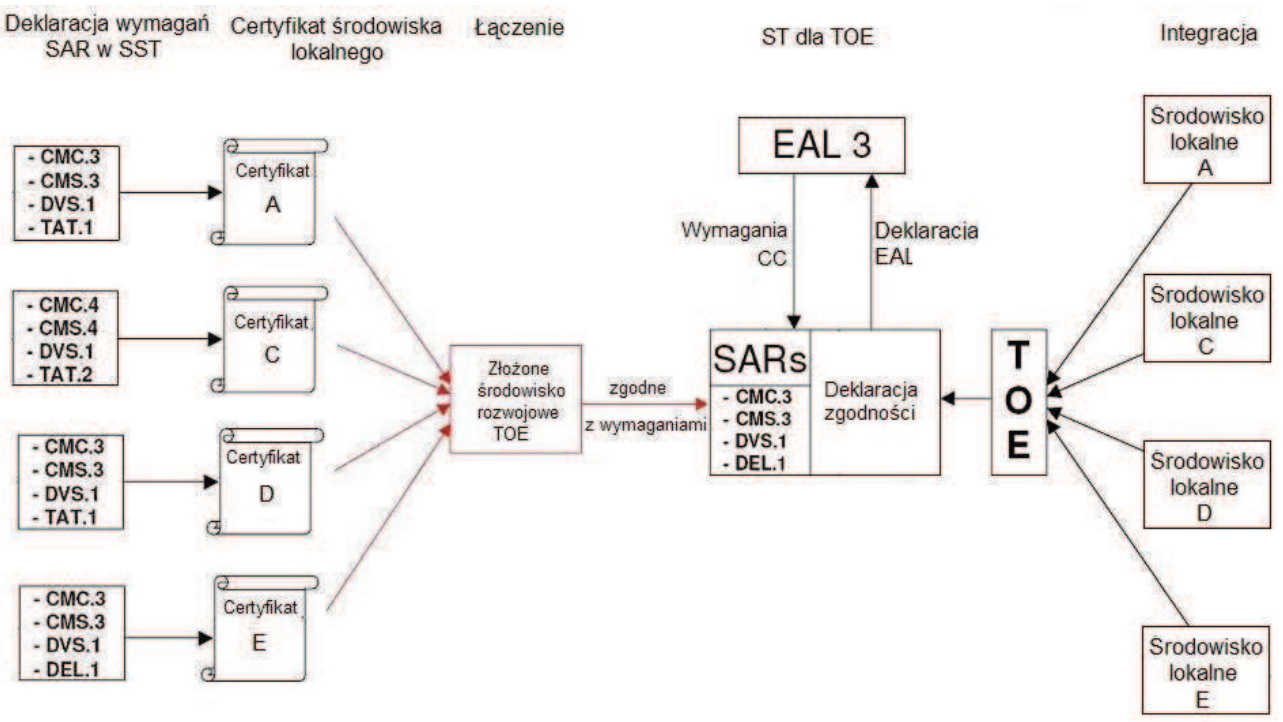
Procedura opisuje sposób użycia (integracji) ocenionego już względem klasy ALC materiału dowodowego podczas oceny produktu. W trakcie tworzenia zadania zabezpieczeń dla produktu, projektant zobowiązany jest do określenia zakresu środowiska rozwojowego za pomocą wymagań klasy ALC oraz musi uwzględnić wszystkie pozostałe komponenty klasy ALC, wynikające z zadeklarowanego dla produktu poziomu EAL (tak jak to pokazuje rys. 4, w którym ustalono ocenę produktu według poziomu EAL3). Zakładając, że nie zaszły żadne zmiany w certyfikowanych środowiskach lokalnych, wydane certyfikaty mogą zostać użyte podczas oceny produktu. Co więcej, jeśli certyfikaty środowisk lokalnych spełniają wszystkie wymagania klasy ALC zawarte w zadaniu zabezpieczeń dla produktu, to nie zachodzi konieczność ponownej oceny tych wymagań podczas oceny samego produktu.

6.3. Łączenie środowisk lokalnych

Procedura przedstawia sposób łączenia certyfikowanych i niecertyfikowanych części cyklu życia produktu w większą jednostkę, która może reprezentować całe środowisko rozwojowe, i która może być użyta później podczas oceny tego produktu. W artykule przedstawiono przykład łączenia certyfikowanych środowisk lokalnych, które tworzą złożone środowisko rozwojowe dla danego przedmiotu oceny (rys. 5). Dla prawidłowej oceny tak utworzonego, złożonego środowiska rozwojowego, oceniający powinien dobrze zrozumieć model cyklu życia zastosowany przez projektanta. Oznacza to, że podczas oceny produktu oceniający powinien zwrócić szczególną uwagę na to, czy projektant zadeklarował prawidłowe środowiska lokalne powstawania produktu, które wraz ze swoimi fazami cyklu życia powinny poprawnie ze sobą współdziałać. Oceniający powinien także potwierdzić, że deklarowany w certyfikatach środowisk lokalnych poziom podatności na zagrożenia jest proporcjonalny do tego deklarowanego dla produktu za pomocą rodziny AVA_VAN. Rodzina ta służy do analizy podatności (ang. *Vulnerability analysis*) produktu na zagrożenia w trakcie jego rozwoju oraz przyszłego użytkowania, które mogą prowadzić do naruszenia jego zabezpieczeń funkcjonalnych. Procedura łączenia weryfikowana jest za pomocą sprawdzenia zgodności cyklu życia produktu z wymaganiami rodziny ALC_LCD, odpowiadającej za poprawne definiowanie tego cyklu (ang. *Life-cycle definition*).

7. PODSUMOWANIE

W artykule opisano prace badawcze dotyczące procesu certyfikacji lokalnych środowisk rozwojowych bezpiecznych produktów IT zgodnych z wymagania-



Rys. 5. Łączenie środowisk lokalnych (opracowanie własne na podstawie [10])

mi normy CC. Rosnąca potrzeba oceny środowisk lokalnych wynika ze złożoności rozwijanych i wytwarzanych w nich produktów oraz konieczności zmniejszenia pracochłonności i kosztów późniejszej oceny tych produktów. Prace nad procesem certyfikacji środowiska lokalnego rozpoczęło BSI w 2006 r., kiedy to miało miejsce pierwsze, próbne zastosowanie certyfikacji dla dwóch środowisk lokalnych przeznaczonych do tworzenia oprogramowania i elementów sprzętowych. Wynikiem przeprowadzonych testów było m.in. opracowanie pierwszego poradnika dla certyfikacji środowisk lokalnych [10] oraz potwierdzenie, że metoda pozwala na wielokrotne użycie ocenionych środowisk lokalnych, co przynosi oszczędności czasu i kosztów oceny samego produktu.

W kolejnych latach organizacje Eurosmart i BSI wraz z firmami partnerskimi zrealizowały pierwszy projekt certyfikacji rzeczywistego środowiska lokalnego dla bezpiecznych paszportów elektronicznych. Prace te doprowadziły do wydania w lipcu 2009 r. pierwszego certyfikatu środowiska lokalnego oraz przyczyniły się do aktualizacji i uszczegółowienia poradników i wydania wzorców raportów, ułatwiających pracę konstruktorom oraz oceniającym.

W artykule opisano krótko zakres zastosowania procesu certyfikacji środowiska lokalnego w ramach projektu CCMODE. Opracowany w projekcie model środowiska rozwojowego z wkomponowanym cyklem życia produktu uwzględnia moduły wzorcowe przeznaczone do budowy złożonych środowisk rozwojowych zgodnie z podejściem certyfikacji środowisk lokalnych. Na moduły wzorcowe składają się zadanie zabezpieczeń SST środowiska lokalnego, materiał dowodowy klasy ALC oraz odpowiadające im metody transformacji wzorców do postaci docelowej dla konkretnego środowiska.

W dalszej części artykułu przybliżono czytelnikowi podstawowe pojęcia związane z procesem certyfikacji środowiska lokalnego, omówiono minimalne wymagania konieczne do poprawnego prowadzenia certyfikacji, opisano noty aplikacyjne dla wymagań klasy ALC, ogólnie scharakteryzowano podstawowe procedury certyfikacji, integracji i łączenia.

Złożone środowiska rozwojowe dekomponują cykl życia produktu na różne lokalizacje w obrębie różnych jednostek organizacyjnych, co tym samym wymaga dokładnego sprawdzenia spójności zastosowanego cyklu życia. Mimo że proces rozwoju produktu w takich środowiskach jest bardziej złożony, to certyfikacja środowisk lokalnych, będących częścią pełnego środowiska rozwojowego i ponowne wykorzystanie rezultatów oceny są uzasadnione, gdyż umożliwiają redukcję kosztów i czasu oceny samego produktu. Celem prac nad dalszym rozwijaniem procesu certyfikacji środowisk lokalnych jest uzyskanie jak najefektywniejszych metod wielokrotnego użycia ocenionego materiału dowodowego.

Literatura

1. ISO/IEC 15408-1, v3.1, Information technology – Security techniques – Introduction and general model (Common Criteria Part 1), 2009.
2. ISO/IEC 15408-2, v3.1, Information technology – Security techniques – Security functional requirements (Common Criteria Part 2), 2009.
3. ISO/IEC 15408-3, v3.1, Information technology – Security techniques – Security assurance requirements (Common Criteria Part 3), 2009.
4. *Białas A.*: Informatyczne produkty sprzętowe, oprogramowanie oraz systemy o zadanym poziomie uzasadnionego zaufania. Mechanizcja i Automatyzacja Górnictwa, Katowice, grudzień 2009.
5. *Białas A.*: Wspólne Kryteria do projektowania i oceny zabezpieczeń teleinformatycznych (Common Criteria, ISO/IEC 15408) – autorskie szkolenie wprowadzające dla odbiorców certyfikowanych produktów informatycznych, ITI EMAG, Katowice 2009.
6. Site Certification – Good News & Guidelines, 10th ICCC, Tromso, Norway, September 22-24 2009.
7. Site Security Target Lite for the Inlay Production of HID Global GmbH in Erfurt, Certification ID: BSI-DSZ-CC-S-0001, version 1.1, 24.07.2009.
8. Site Certification Process. Frank Sonnenberg (BSI), Lanzarote, Spain, 7th ICCC/19.09.2006.
9. First Trial-Use-Results of the Site Certification Process. Thomas Borch (BSI), Lanzarote, Spain, 7th ICCC/19.09.2006.
10. Supporting Document Guidance, Site Certification, Version 1.0 Revision 1, CCDB-2007-11-001, October 2007.
11. Site Certification – Another step to improve the CC process and to reduce costs. Hans-Gerd Albertsen, NXP Semiconductors Germany GmbH; Jürgen Noller, Infineon Technologies AG. Jeju, Korea, 9th ICCC, September 23-25 2008.
12. Experiences gained from the first Site Certification Projects. Christian Krause (BSI), Thomas Schröder (T-Systems), 10ICCC / 22 September 2009.
13. Guidance for Site Certification, Version 1.0, BSI 2010.
14. Details for the structure and content of the ETR for Site Certification, version 1.0. BSI, 2010.
15. Single Evaluation Report of the Assurance Class AST (Site Security Target evaluation), Version 1.0, 16th, BSI – Template_ETR-Part_AST_v1_0.doc, September 2010.
16. Single Evaluation Report of the Assurance Class ALC (Life-Cycle Support), Version 1.0, 16th, BSI – Template_ETR-Part_ALC_v1_0.doc, September 2010.
17. Site Security Target Template, version 1.0, Eurosmart, 21.06.2009.
18. Site Security Target for SMT1 Smartrack Technology Ltd., Certification ID: BSI-DSZ-CC-S-0002, version 1.51 lite, 30.09.2009.
19. Site Security Target Lite of HID Global Ireland Teoranta in Galway, Ireland, Certification ID: BSI-DSZ-CC-S-0004, 13.07.2010.

Recenzent: dr inż. Andrzej Michalski

KOMUNIKAT

Centrum Badań i Certyfikacji Instytutu Technik Innowacyjnych EMAG

– Jednostki Certyfikującej Wyroby:

(Certyfikat akredytacji nr AC 053)

o wydanych i cofniętych certyfikatach

Wydano:

1. Certyfikat zgodności nr 1/11 uzyskany w certyfikacji dobrowolnej, system 1b ISO (marzec 2011 r.)
   Dostawca: **Dąbrowska Fabryka Maszyn Elektrycznych DAMEL Spółka Akcyjna**, **Aleja Józefa Piłsudskiego 2, 41-300 Dąbrowa Górnicza**
   Wyrób: **Silnik indukcyjny trójfazowy**
   Typ (odmiany): **SG3 450Y 12/4**

2. Certyfikat zgodności nr 2/11 uzyskany w certyfikacji dobrowolnej, system 1b ISO (marzec 2011 r.)
   Dostawca: **OPA-ROW Sp. z o.o., ul. Rymera 40c, 44-270 Rybnik**
   Wyrób: **Prostownik**
   Typ (odmiany): **PT 130F**