Podsumowanie Narodowego Testu Interoperacyjności Podpisu Elektronicznego

mgr inż. ROBERT POZNAŃSKI, mgr inż. KAROL SZACKI, inż. ŁUKASZ STROIŃSKI

Instytut Maszyn Matematycznych, Warszawa

Podpis elektroniczny został wprowadzony do prawa europejskiego przez dyrektywę 99/93/EC, która została uchwalona w roku 1999. W Polsce podpis elektroniczny został zaimplementowany w roku 2001 poprzez uchwalenie „Ustawy o podpisie elektronicznym". Przepisy prawa nadają szczególne znaczenie podpisowi kwalifikowanemu, który jest zrównany z podpisem odręcznym.

Format podpisu, który może być stosowany przy składaniu podpisów kwalifikowanych został zdefiniowany przez ETSI (*European Telecommunications Standards Institute*) w trzech odrębnych specyfikacjach, opisujących formaty podpisu XAdES, CAdES i PAdES. Ze względu na fakt, iż wymienione specyfikacje są bardzo obszerne, podpisy utworzone na ich podstawie mogą znacznie różnić się między sobą.

Narodowy Test Interoperacyjności Podpisu Elektronicznego (NTIPE) miał na celu zbadanie o opisanie stanu rynku aplikacji służących do składania i weryfikacji bezpiecznego podpisu elektronicznego. Istotnymi elementami było zweryfikowanie problemów związanych ze współpracą różnych aplikacji, uznawalnością certyfikatów wydanych przez różne centra certyfikacji oraz ocena zgodności składanych podpisów z wymaganiami prawa.

W teście wzięło udział w sumie dziesięć aplikacji przygotowanych zarówno przez krajowe jak i zagraniczne podmioty.

Na potrzeby NTIPE zbudowano autorskie środowisko zapewniające możliwość udostępniania plików z testami, możliwość wprowadzania rezultatów testu. Utworzono także centrum certyfikacji, które służyło do wydawania i obsługi certyfikatów testowych oraz wydawania testowych znaczników czasu.

Do wygenerowania przypadków testowych wymagających złożenia podpisu elektronicznego wykorzystano aplikację SD-DSS udostępnioną przez Komisję Europejską (aplikacja udostępniona pod adresem: http://www.osor.eu/projects/sd-dss). Wszystkie wyniki wymagające weryfikacji podpisu były sprawdzane przy użyciu wymienionej aplikacji.

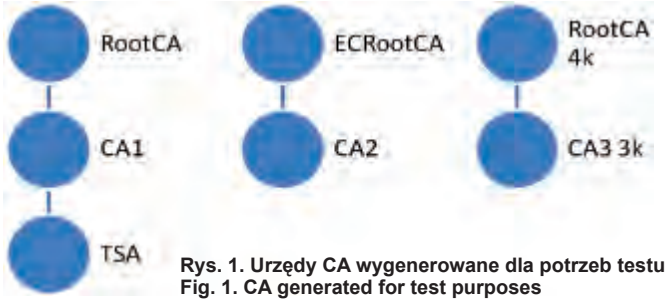
Do weryfikacji zgodności złożonego podpisu z decyzją 2011/130/UE wykorzystano aplikację własnej produkcji, która kontrolowała automatycznie obecność wymaganych elementów podpisu, ale nie weryfikowała ważności podpisu.

Testowane aplikacje były instalowane na stanowiskach przygotowywanych przez ich producentów. Część testów była wykonywana przy wykorzystaniu certyfikatów kwalifikowanych. Certyfikaty testowe były wykorzystywane w przypadkach, gdy uzyskanie certyfikatu kwalifikowanego sprawiałoby trudność. Przykładem użycia certyfikatu testowego może być test CK04, w którym certyfikat zawiera błędne rozszerzenie krytyczne.

W celu odzwierciedlenia różnych ścieżek certyfikacji, na potrzeby NTIPE wygenerowano trzy odrębne urzędy certyfikacji:

Pierwsza ścieżka odzwierciedla infrastrukturę aktualnie działającą w Polsce. Kolejne dwie odzwierciedlają warianty infrastruktury docelowej, która mogłaby być zainstalowana po zmianie algorytmów kryptograficznych.

Część testów była wykonywana przy wykorzystaniu certyfikatów kwalifikowanych. Certyfikaty testowe były wykorzystywane w przypadkach, gdy uzyskanie certyfikatu kwalifikowanego sprawiałoby trudność.



Rys. 1. Urzędy CA wygenerowane dla potrzeb testu
Fig. 1. CA generated for test purposes

Tab. 1. Testowane aplikacje. Tabl. 1. Tested applications

Nazwa Firmy	Aplikacja	Podpis			Weryfikacja		
		CADES	PADES	XADES	CADES	PADES	XADES
ENIGMA Systemy Ochrony Informacji Sp. z o.o.	PEM-HEART SIGNATURE	x	x	x	x	x	x
Krajowa Izba Rozliczeniowa SA	SZAFIR	x	x	x	x	x	x
Unizeto Technologies SA	SmartSign	x	x	x	x	x	x
Unizeto Technologies SA	WebNotarius				x	x	x
PWPW SA	Sigillum Sign	x	x	x	x	x	x
Microsec Ltd.	e-Szignó	x	x	x	x	x	x
EC2 Sp. z o.o.	Protektor			x			x
BIT4ID	FIRMA4NG	x	x	x	x	x	x
Hitachi	CVS						x
OpenLimit SignCubes AG	OpenLimit Middleware Version 3 Client	x	x		x	x	

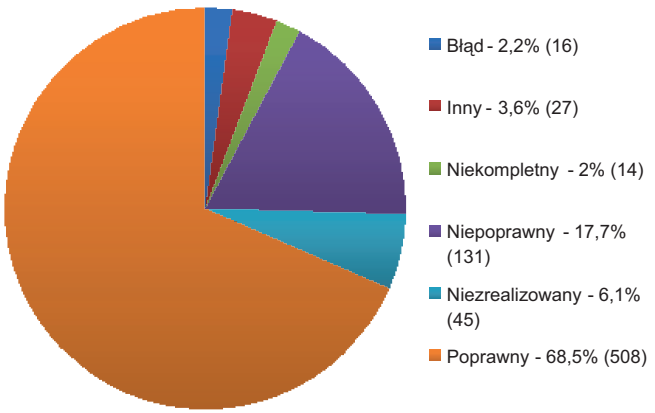
Pierwszym etapem testów były tak zwane pretesty trwające od 26 września do 17 października 2011 r. Pliki z testami oraz wyniki przekazywane były poprzez dedykowany i przygotowany specjalnie na potrzeby testu portal WWW. W sumie przygotowanych zostało 39 przypadków testowych, które podzielić można na trzy części:

Tab. 2. Testy składania podpisu elektronicznego
Tabl. 2. Digital signature creation tests

ID	Nazwa testu
CK06	Możliwość składania przez aplikacje podpisu RSA1024 + SHA1
CK07	Możliwość składania przez aplikacje podpisu RSA 2048 + SHA 256
CK08	Możliwość składania przez aplikacje podpisu ECDSA256 +SHA256
CK09	Możliwość składania przez aplikacje podpisu weryfikowanego nieważnym certyfikatem
DC01	Składanie podpisu zgodnego z Decyzją 2011/130/EC dla XAdES
DC02	Składanie podpisu zgodnego z Decyzją 2011/130/EC dla CAdES
DC03	Składanie podpisu zgodnego z Decyzją 2011/130/EC dla PAdES
DC04	Dołączenie do podpisu identyfikatora polityki podpisu
DC05	Rozpoznawanie polityki podpisu podczas składania podpisu
DC06	Możliwość włączenia rozszerzenia CommitmentType do podpisu
DC07	Możliwość dołączenia znacznika czasu do podpisu
DC08	Możliwość dołączenia dowolnego znacznika czasu do podpisu
DC09	Możliwość tworzenia wersji archiwalnej podpisu
DC10	Obsługa wersji archiwalnej podpisu z dołączonym CRL
DC11	Obsługa wersji archiwalnej podpisu z dołączonym OCSP

Tab. 3. Testy składania kontrasygnaty
Tabl. 3. Countersignature tests

ID	Nazwa testu
IK01	Interoperacyjność aplikacji w zakresie kontrasygnaty
IK02	Interoperacyjność z ePUAP w zakresie kontrasygnaty



Rys. 2. Wyniki Pretestów. Fig. 2. Pretests results

Tab. 4. Testy weryfikacji podpisu elektronicznego
Tabl. 4. Digital signature verification tests

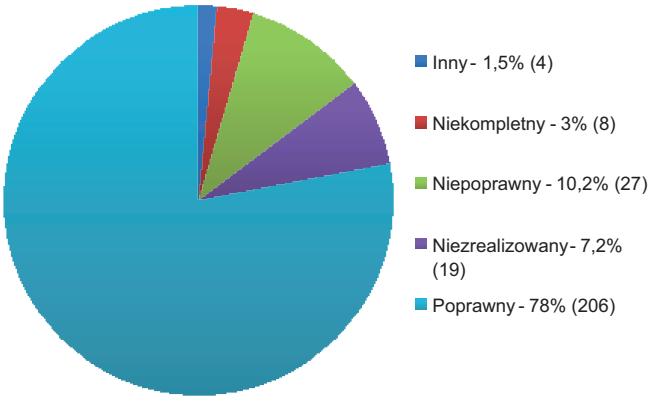
ID	Nazwa testu
CK01	Budowanie ścieżki certyfikacji dla certyfikatów wydawanych w kraju
CK02	Rozpoznanie certyfikatu kwalifikowanego po określonej polityce certyfikacji
CK03	Rozpoznanie certyfikatu kwalifikowanego na podstawie rozszerzenia QCStatement
CK04	Rozpoznanie, że certyfikat kwalifikowany jest nieprawidłowy
CK05	Budowanie ścieżki certyfikacji dla certyfikatów wydawanych za granicą
DC12	Rozpoznawanie dołączenia polityki podpisu
DC13	Rozpoznawanie ograniczeń zdefiniowanych w politykach podpisu
DC14	Weryfikacja podpisów ze znacznikiem czasu
DC15	Weryfikacja podpisu w wersji archiwalnej dla certyfikatu ważnego
DC16	Weryfikacja podpisu w wersji archiwalnej dla certyfikatu zawieszonego
DC17	Weryfikacja podpisu w formacie BES dla certyfikatu zawieszonego
DC18	Weryfikacja podpisu z unieważnionym znacznikiem czasu
DC19	Weryfikacja podpisu z nieprawidłowym skrótem
DC20	Weryfikacja zmodyfikowanego pliku
DC21	Weryfikacja podpisów detached
DC22	Weryfikacja podpisów enveloped
DC23	Weryfikacja podpisów enveloping
DC24	Weryfikacja podpisu zawierającego w hierarchii certyfikaty RSA 4k+SHA512 i RSA3k + SHA256
DC25	Weryfikacja podpisu zawierającego w hierarchii certyfikaty ECDSA 256 +SHA256 i RSA2k + SHA256
IK03	Interoperacyjność aplikacji w zakresie weryfikacji
IK04	Interoperacyjność z ePUAP w zakresie weryfikacji
IK05	Weryfikacja podpisu zgodnego z Decyzją 2011/130/EC złożonego przez aplikacje biorące udział w teście

Tab. 5. Weryfikacja wyników pretestów
Tabl. 5. Verification of pretests results

ID	Nazwa testu
CK04	Rozpoznanie faktu, że certyfikat podpisującego zawiera nieprawidłowe rozszerzenie krytyczne
CK05	Weryfikacja wykorzystania przez aplikację listy TSL do ustalenia zaufania dla certyfikatów kwalifikowanych wydanych za granicami kraju
DC24	Weryfikacja przygotowania na wprowadzenie nowych ścieżek certyfikacji zawierających algorytmy SHA2 i RSA o długości powyżej 2048 bit

Tab. 6. Testy dla uczestników warsztatów
Tabl. 6. Tests for workshop participants

ID	Nazwa testu
DC1	Weryfikacja czy aplikacja umożliwia złożenie podpisu zgodnego z formatem referencyjnym dla XAdES
DC02	Weryfikacja czy aplikacja umożliwia złożenie podpisu zgodnego z formatem referencyjnym dla CAdES
DC03	Weryfikacja czy aplikacja umożliwia złożenie podpisu zgodnego z formatem referencyjnym dla XAdES
IK5	Weryfikacja podpisu zgodnego z Decyzją 2011/130/UE złożonego przez aplikacje biorące udział w teście
IK6	Złożenie podpisu kwalifikowanego przy użyciu dowolnego certyfikatu kwalifikowanego wydanego w Polsce



Rys. 3. Wyniki warsztatów. Fig. 3. Workshop results

W sumie w ramach pretestów zrealizowano 742 testy. Na poniższym wykresie pokazany jest procentowy rozkład wyników oraz, w nawiasie, ilość testów z danym wynikiem.

Ponieważ warsztaty realizowane były równolegle z konferencją w terminie 26–27 października, niemożliwe było przeprowadzenie takiej samej liczby testów jak w pretestach. Z tego względu organizatorzy zdecydowali się przeprowadzić trzy testy w ramach weryfikacji wyników pretestów oraz pięć testów dedykowanych uczestnikom warsztatów:

W ramach warsztatów zostały przeprowadzone 264 testy. Poniższy wykres pokazuje procentowy rozkład wyników oraz, w nawiasie, ilość testów z danym wynikiem.

Mając na uwadze otrzymane wyniki można obalić mit o problemach we współpracy pomiędzy aplikacjami do składania i weryfikacji podpisu elektronicznego. Dodatkowo, dzięki uczestnictwu podmiotów z innych krajów widać, że również współpraca z zagranicznymi aplikacjami nie sprawia dużych problemów. Pomimo dosyć wysokiego poziomu interoperacyjności aplikacji, należy zauważyć, że przy narzędziu takim jak podpis elektroniczny oczekiwania użytkowników są znacznie wyższe. Przeciętna osoba będzie oczekiwać poprawności działania na poziomie zbliżonym do 100%. Porównując sytuację na rynku podpisu elektronicznego do rynku telefonów komórkowych, użytkownik oczekuje, że będzie mógł dzwonić na dowolny model telefonu, a nie tylko na wybrane. Wynika z tego, że na rynku podpisu elektronicznego jest jeszcze sporo do zrobienia.

Więcej informacji o wynikach testów wraz z ich omówieniem znaleźć można w „Raporcie Końcowym" NTIPE, który można zamówić na stronie WWW pod adresem http://www.commonsign.eu/.

Ochrona urządzeń mobilnych

25 kwietnia w Warszawie odbyła się konferencja **Symantec.Future.** W trakcie spotkania organizatorzy (firma Symantec) przedstawili praktyczne zastosowania swoich rozwiązań a zaproszeni goście opowiedzieli o problemach, przed którymi stanęli oraz sposobach ich rozwiązania.

Jednym z głównych poruszanych zagadnień było zapewnienie bezpieczeństwa urządzeniom mobilnym, które wchodzą do naszych domów oraz przedsiębiorstw, a także ochrona informacje przed wyciekiem jak i przed utratą w coraz bardziej otwartych i mobilnych środowiskach pracy.

W roku 2011 na świecie sprzedano 472 mln smartphonów co stanowiło wzrost o +58% w stosunku do roku ppoprzedniego. Przewiduje się, że do 2015 roku urządzenia mobilne stanowić będą 50% sprzedaży laptopów.

Dziś, wg światowych badań 21% ruchu w sieci pochodzi własnie z urządzeń mobilnych, niektóre firmy kalkulują, że jest to nawet więcej niż 50%. Prognozy na rok 2013 przewidują że liczba # połączeń z Internetem realizowana za pomocą komputera wyniesie ok. 1,78 mld, a liczba połączeń z Internetem realizowana za pomocą urządzeń mobilnych przekroczy 1,82 mld.

Rynek rozwiązań mobilnych w Polsce rozwija się dynamicznie. Wg IDC w roku 2011 sprzedano w Polsce 10,8 mln telefonów komórkowych, a w tym 3,3 mln smartphonów, zanotowano wzrost o 8% (rok/rok). Wg Ministerstwa Cyfryzacji w roku 2011 było 3,5 miliona użytkowników Internetu mobilnego. (cr)