Narodowy test interoperacyjności podpisu elektronicznego

dr inż. MAREK HOŁYŃSKI, Instytut Maszyn Matematycznych, Warszawa

Duży zbiór rodzajów dokumentów elektronicznych oraz różnorodne ich przeznaczenie wymusza wielość formatów i rodzajów e-podpisu. Na rynku pojawiają się rozmaite, nie zawsze zgodne z sobą produkty oraz aplikacje. Istnieje zatem pilna potrzeba uporządkowania tej sytuacji i praktycznej weryfikacji oferowanych przez producentów rozwiązań na otwartym publicznym forum.

Dla oceny rzeczywistej sytuacji w dniach 26–27 października 2011 r. został zorganizowany w Warszawie Narodowy Test Interoperacyjności Podpisu Elektronicznego. Koordynacji tego wydarzenia podjął się Instytut Maszyn Matematycznych, w którym od dwóch lat działa Laboratorium Podpisu Elektronicznego. Impreza organizowana była przy współpracy Ministerstwa Gospodarki i pod osobistym patronatem wicepremiera Waldemara Pawlaka. Narodowy Test Interoperacyjności Podpisu Elektronicznego został również wpisany w program polskiej prezydencji w Unii Europejskiej.

W tych samych dniach równolegle z testami odbyła się konferencja poświęcona wymianie wiedzy i doświadczeń dostawców rozwiązań z kraju i zagranicy, w której uczestniczyli przedstawiciele administracji publicznej, będącej głównym beneficjentem rozwiązań podpisu elektronicznego. Wspólna organizacja tych przedsięwzięć pozwoliła skonfrontować planowanie na poziomie organizacyjnym i legislacyjnym z praktyką, wymienić informacje pomiędzy dostawcami usług i osobami kreującymi kształt rozwiązań. Oba dni konferencji kończyły bardzo owocne dyskusje na temat rozwiązań oraz przyszłości rozwoju technik i interoperacyjności podpisu elektronicznego.

Ze względu na duże zainteresowanie ze strony biznesu i administracji publicznej dostępnością aplikacji właściwie ze sobą współpracujących, organizatorzy szczególną uwagę zwrócili na przetestowanie podpisywania oraz weryfikacji podstawowych formatów podpisu elektronicznego. Dodatkowo podczas testów sprawdzona została kooperacja aplikacji z rozwiązaniami proponowanymi przez administrację publiczną, np. Elektroniczną Platformą Usług Administracji Publicznej (PUAP).

Ze względu na przewidywaną liczbę testów nierealne było wykonanie ich w ciągu jedynie dwóch dni. Dlatego też w terminie 26 września – 17 października 2011 r. odbyły się pretesty, podczas których pliki testowe były udostępniane użytkownikom online za pomocą portalu testowego. Testy przeprowadzano w trzech funkcjonalnych etapach polegających na złożeniu podpisu, jego kontrasygnacie i weryfikacji. W 39 pretestach sprawdzano formaty CAdES, PAdES i XAdES. Każdy z uczestników miał do wykonania 145 zadań testowych. W ramach sesji warsztatowych odbytych 26–27 października zrealizowano 262 testy, przeprowadzając weryfikację wyników pretestów, ocenę zgodności z decyzją 2011/130/EC w zakresie podpisu elektronicznego, weryfikację podpisów złożonych przez poszczególne aplikacje oraz testy złożenia podpisu przy wykorzystaniu certyfikatów kwalifikowanych wydanych przez polskie centra certyfikacji.

W testach, do których mogli przystąpić wszyscy chętni, wzięło udział sześć wiodących aplikacji krajowych i cztery zagraniczne (z Węgier, Niemiec, Włoch i Japonii). Odsetek poprawnych rezultatów w teście zgodności z decyzją 2011/130/EC wyniósł 100% dla formatów CAdES i PAdES oraz 71,4% dla XAdES. Aplikacje biorące udział w teście dokonywały bezbłędnej weryfikacji złożonych podpisów przeciętnie w 70…80% przypadków. Na poziomie 77,7% kształtuje się poprawność rozpoznania ścieżki certyfikacji zawierającej urzędy CA z algorytmami SHA256, SHA512 oraz długością kluczy RSA 3072 bit i 4096 bit. Rozpoznawanie certyfikatów kwalifikowanych wydanych za granicą z wykorzystaniem listy TSL wynosi 62,5% dla CAdES i PAdES oraz 44% dla XAdES. Stosunkowo niska, bo jedynie 50%, jest poprawność reakcji aplikacji na rozpoznanie błędnego rozszerzenia krytycznego zdefiniowanego w certyfikacie.

Na podstawie wstępnych wyników z wykorzystaniem materiału testowego z różnych państw można stwierdzić, że obecnie zdarzają się trudności związane z budową ścieżki certyfikacji i dostępem do informacji dotyczącej jej ważności oraz z zagadnieniami wsparcia dla obsługi listy TSL. Pozostałe problemy wynikały zazwyczaj z drobnych błędów implementacyjnych popełnionych przez producentów aplikacji do składania lub weryfikacji podpisu.

Przykładowy wynik jednego z testów. **Example result of one of the tests**

Szczegółowe dane i wnioski zostaną przedstawione w raporcie, który będzie opublikowany po dokładnym przeanalizowaniu rezultatów. W dyskusji podsumowującej konferencję uczestnicy podkreślali, iż Narodowy Test Interoperacyjności Podpisu Elektronicznego w empiryczny sposób przyczynił się do uzyskania obiektywnej oceny stanu rynku w tej dziedzinie i ulepszenia istniejących rozwiązań. Organizacja testu w przyszłych latach nie tylko przyczyni się do obiektywnej oceny rynku rozwiązań dla podpisu elektronicznego, ale będzie także motywacją dla dostawców aplikacji do dostarczenia produktów spełniających wymagania norm i oczekiwania klientów.