Ćwiczenia laboratoryjne z przedmiotu Kryptografia i Bezpieczeństwo Danych

Temat: Podpis Elektroniczny

Autor: Sławomir Samolej

Wprowadzenie

1. Podpis elektroniczny ma zapewnić integralność podpisywanych danych i umożliwić weryfikację osoby, która go składa. Stosuje się to tego kryptografię klucza publicznego. Na wysokim poziomie ogólności zasadę składania podpisu elektronicznego można przedstawić w następujący sposób. Osoba podpisująca ciąg danych wykonuje na tym ciągu funkcję hash (mieszającą). Otrzymany skrót danych szyfruje za pomocą swojego klucza prywatnego. Osoba, która chce zweryfikować podpis bierze dokument, liczy z niego funkcję hash i porównuje tę funkcję z odszyfrowaną za pomocą klucza publicznego osoby podpisującej. Jeśli obie funkcje hash są identyczne, to wiadomość jest integralna. Klucz publiczny wskazuje, kto był osobą podpisującą.

2. Potwierdzeniem, że dana para kluczy jest przypisana konkretnej osobie zajmuje się urząd certyfikacji. Jeśli dysponujemy dostępem do urzędu certyfikacji, który może np. być komponentem serwera, który może zarządzać kluczami na poziomie biura, instytucji, kraju, czy świata, możemy w ramach sprawdzania podpisu zwrócić się do niego o weryfikację posiadacza danej pary klucz sekretny - klucz publiczny. Poprawne wygenerowanie kluczy dla możliwości do weryfikacji podpisu obejmuje, po wygenerowaniu kluczy zwrócenie się do urzędu certyfikacji o wystawienie certyfikatu dla klucza publicznego. Osoba, chcąca podpisywać dokumenty powinna posiadać taki certyfikat dla swojego klucza. Certyfikat, w zasadzie też jest podpisem elektronicznym. Zawiera on oprócz klucza publicznego osoby podpisującej, również dane ją identyfikujące, oraz uprawnienia danego klucza co do podpisywania. Można mieć wystawiony certyfikat tylko do podpisu email, tylko do podpisu oprogramowania, czy ogólnie do podpisywania dokumentów. Jeśli chcemy uzyskać certyfikat umożliwiający podpisywanie dokumentów równoważny z podpisem odręcznym, to należy „wyrobić" sobie tzw. podpis kwalifikowany. Wystawienie certyfikatu kwalifikowanego wiąże się z wystąpieniem do odpowiedniej instytucji, która takie certyfikaty udziela. Na określonym etapie następuje osobista weryfikacja danych osobowych potwierdzona notarialnie lub przez wyznaczoną osobę.

3. Z technicznego punktu widzenia podpisy cyfrowe są ustalonymi na etapie prawnym strukturami danych. Przykładowo, format pdf zakłada możliwość włączenia w strukturę dokumentu pdf podpisu elektronicznego. Może on być zaznaczony wizualnie w dokumencie, ale zawiera również w wewnętrznych strukturach danych wszystkie informacje pozwalające na cyfrową jego weryfikację. Podobne „miejsce" na podpis elektroniczny zawiera standard wiadomości pocztowych MIME. Stąd możliwe jest łatwe podpisywanie wiadomości email. Niektóre dokumenty elektroniczne wprost mają postać elektronicznego podpisu. Dobrym przykładem jest elektroniczna legitymacja studencka przechowywana w karcie chipowej studenckiej legitymacji.

Uwagi:

Ćwiczenie będzie wymagało zainstalowania oprogramowania Acrobat ReaderDC, Mozilla Thunderbird i Visual Studio

Przebieg ćwiczenia

1. Proszę prześledzić wprowadzenie prowadzącego dotyczące uzyskiwania i posługiwania się kwalifikowanym podpisem elektronicznym [1].

2. Proszę prześledzić wprowadzenie prowadzącego dotyczące podpisywania dokumentów PDF z zastosowaniem samodzielnie wygenerowanych certyfikatów i innych certyfikatów zgromadzonych w magazynie osobistym. [2]
3. Proszę prześledzić wprowadzenie prowadzącego dotyczące posługiwania się narzędziem New-SelfSignedCertificate (PowerShell) do generowania własnych certyfikatów [3].
4. Proszę prześledzić wprowadzenie prowadzącego dotyczące posługiwania się narzędziem signtool dostarczanym wraz z Visual Studio do tworzenia i weryfikacji podpisów elektronicznych [4] plików wykonywalnych (exe, dll, i inne).
5. Proszę wygenerować własny certyfikat w programie Acrobat Reader DC i za jego pomocą podpisać wybrany dokument PDF.
6. Proszę wygenerować własny certyfikat do podpisu w programie New-SelfSignedCertificate i podpisać nim wybrany dokument pdf.
7. Proszę podpisać wybrany plik wykonywalny na dysku z zastosowaniem własnego certyfikatu i narzędzia signtool.
8. Proszę skonfigurować program Thunderbird do podpisywania wiadomości pocztowych, porady można znaleźć w [5]. Można to tego zastosować klucze PGP oraz darmowe certyfikaty możliwe do uzyskania ze stron opublikowanych w [7].

Literatura

[1] (Strona Certum – jednego dostawców podpisów kwalifikowanych) https://www.certum.pl/pl/

[2] (Instrukcja podpisywania dokumentów PDF w programie Acrobar Reader DC) https://helpx.adobe.com/pl/reader/using/sign-pdfs.html#sign_a_document

[3] (Strona modułu PowerShell „PKI client" do zarządzania certyfikatami) https://docs.microsoft.com/en-us/powershell/module/pki/

[4] (Strona narzędzia wiersza poleceia Visual Studio – SignTool) https://docs.microsoft.com/pl-pl/windows/win32/seccrypto/signtool

[5] (Instrukcja instalacji certyfikatu w Thunderbird) https://support.globalsign.com/digital-certificates/digital-certificate-installation/install-certificate-mozilla-thunderbird

[6] (Przykładowa strona z testowymi certyfikatami do podpisu elektronicznego) https://www.certum.pl/pl/certum_pz_certyfikaty_testowe/

[7] (Przykładowa strona z odnośnikami do instytucji wystawiające darmowe certyfikaty SMIME) http://kb.mozillazine.org/Getting_an_SMIME_certificate