CBKE
e-BIULETYN

Podstawowe zastosowania podpisu elektronicznego opartego na kryptografii dynamicznej

Mariusz Drożdż

Inspektor i biegły zakresie w komunikacji elektronicznej

Wprowadzenie

Pomimo, że wiele aktów prawnych, obok tradycyjnej formy podpisu, pozwala praktycznie wykorzystywać bezpieczny podpis elektroniczny[1] weryfikowany przy pomocy kwalifikowanych certyfikatów[2], to istnieje wiele obszarów w życiu gospodarczym i prawnym, w których podpis elektroniczny w klasycznej formie do tej pory nie znalazł swojego zastosowania, bądź jego zastosowanie obejmuje tylko niewielką cześć usług. Możliwości zastosowania tej technologii do dokumentów elektronicznych jak by się wydawać mogło są praktycznie nieograniczone a moc prawna "bezpiecznego podpisu elektronicznego" zrównująca go z podpisem własnoręcznym pozwala stosować go w coraz to nowych obszarach. Czy jednak takie stwierdzenie jest prawdziwe ? Jak się okazuje podstawowe bariery wdrażania klasycznego podpisu elektronicznego w życiu gospodarczym i prawnym naszego kraju związane są nie tylko niektórymi restrykcyjnymi w stosunku do niej wymogami ustawowymi ale również z właściwościami podpisu elektronicznego

1 (art.. 3 ust 2 ustawy) Bezpieczny podpis elektroniczny to podpis elektroniczny, który jest przyporządkowany do osoby składającej podpis, jest sporządzony za pomocą bezpiecznych urządzeń służących do składania podpisu elektronicznego w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna

2 (art. 20 ust. 1 ustawy) Kwalifikowany certyfikat to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis i służą do jej identyfikacji

Opublikowane: 4 marca 2009

opartego na metodzie kryptografii asymetrycznej[3]. Spróbujmy zweryfikować te obszary, w których do tej pory nie było możliwe zastosowanie podpisu elektronicznego.

Obszary stosowania podpisu elektronicznego

W chwili obecnej użytkownik może stosować bezpieczne podpisy elektroniczne oparte na kwalifikowanych certyfikatach, które funkcjonują w praktyce w następujących dziedzinach życia gospodarczego:

- e-zdrowie, e-deklaracje, e-faktura, e-KRS, e-GIODO, Certyfikat dla ZUS,
- przesyłanie danych do Generalnego Inspektora Informacji Finansowej (GIIF),
- przetargi i aukcje elektroniczne, kontakty z urzędami administracji publicznej.

Jak widać podpis elektroniczny obejmuje podstawowe usługi, które użytkownik może wykonać w kontakcie z administracją czy tez innymi podmiotami mającymi istotne znaczenie w jego działalności zawodowej czy prawnej. Natomiast podmioty wdrażające swoje usługi w oparciu o podpis elektroniczny już teraz trafiają na wiele barier nie tylko systemowych związanych z przedmiotem usługi, którą świadczą, ale również na bariery prawne związane z wymogami ustawowymi dotyczącymi w głównej mierze sposobu przechowywania i archiwizacji dokumentów podpisanych elektronicznie. Oto niektóre przykłady takich usług, z którymi do tej pory nie poradził sobie podpis elektroniczny.

Usługi, których nie obejmuje podpis elektroniczny

Wymiar sprawiedliwości

Zgodnie z ustawą z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz. U. z 2001 r. Nr 17, poz.209) każdy ma prawo do składania wniosków i dokumentów do sądów rejestrowych i Centralnej Informacji oraz uzyskiwania informacji drogą elektroniczną, a także orzeczeń, odpisów, wyciągów, zaświadczeń, informacji i kopii dokumentów doręczanych wnioskodawcom drogą elektroniczną (art. 6 pkt 3). Istnieje jednak wiele obszarów, w których obecnie nie można uruchomić usług w formie elektronicznej. Są to na przykład:

Wydziały ksiąg wieczystych

3 Kryptografia asymetryczna - Kryptografia asymetryczna to rodzaj kryptografii, w którym używa się zestawów dwu lub więcej powiązanych ze sobą kluczy, umożliwiających wykonywanie różnych czynności kryptograficznych

W wydziale ksiąg wieczystych nie można zastosować przepisów tej ustawy przede wszystkim ze względu na wymóg przechowywania dokumentów przez okres 50 lat. Ustawa o podpisie elektronicznym (Dz.U. Z 2001 r. Nr 130, poz. 1450, z 2002 r. Nr 153, poz. 1271, z 2003 r. Nr 124, poz. 1152.) wprost definiuje wymagany od dostawców okres przechowywania certyfikatów klucza publicznego w repozytorium[4] na 20 lat (art. 13 pkt 2). Po tym okresie nie będzie możliwa weryfikacja dokumentów podpisanych elektronicznie. W przypadku kwalifikowanych podmiotów świadczących usługi certyfikacyjne obowiązek przechowania dokumentów i danych, o których mowa w ust. 1, trwa przez okres 20 lat od chwili powstania danego dokumentu. Taki zapis nie pozwala na zastosowanie podpisu elektronicznego np. przy składaniu wniosków do księgi wieczystej.

Notariaty państwowe

Tutaj również rozporządzenia[5] nakładają obowiązek przechowywania dokumentów notarialnych tj. testament, dokumenty i akty związane z nieruchomościami, potwierdzenia notarialne związane posiadanym majątkiem i inne przez okres dłuższy niż 20 lat (na podstawie art. 90 § 8 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (Dz. U. z 2002 r. Nr 42, poz.369, z późn. zm.) . Ustala się następujące okresy przechowywania akt i ksiąg notarialnych, dokumentujących dokonanie czynności notarialnych w archiwum dokumentacji notarialnej prowadzonej przy właściwej izbie notarialnej: 20 lat - dokumenty wymienione w § 6 ust. 1. Podobnie jak w przypadku ksiąg wieczystych obszar ten również nie może zostać objęty elektroniczną formą dokumentu ze względu na ograniczony czas przechowywania certyfikatów klucza publicznego, który obejmuje jedynie okres przechowywania dokumentów w izbie notarialnej. Dokumenty elektroniczne kategorii A nie mogły być być przekazane do archiwum państwowego.

Ośrodki badawcze i akademickie

W środowiskach naukowych oraz urzędach gromadzących i rejestrujących wynalazki również nie można składać wniosków w formie elektronicznej. Wiąże się to nie tylko z koniecznością długiego okresu ochrony i przechowywania tych dokumentów, które nakłada ustawa

4 Repozytorium - to centralna baza danych certyfikatów oraz dokumentów związanych z funkcjonowaniem Centrum Certyfikacji

5 § 3. Dokumenty kategorii A i kategorii B po upływie okresu przechowywania u notariusza przekazuje on do archiwum dokumentacji notarialnej prowadzonej przy właściwej izbie notarialnej natomiast dokumenty kategorii A po upływie okresu przechowywania w archiwum dokumentacji notarialnej prowadzonej przy właściwej izbie notarialnej, przekazuje się do właściwego archiwum państwowego.

z dnia 30 czerwca 2000r. (Dz.U. z 2003r. Nr 119, poz. 1117 z późniejszymi zmianami). Na przykład prawo własności przemysłowej mówi, że rejestracja wzoru przemysłowego obejmuje okres 25 lat. Jest to okres znacznie przekraczający czas przechowywania kluczy publicznych. Problemy związane są także ze strukturą samych dokumentów, które w dużej części składają się z planów, schematów, czy też innych form graficznych. Trudno jest szyfrować czy podpisywać formy graficzne klasycznymi algorytmami. Są to podstawowe bariery w rejestracji wynalazków, wzorów przemysłowych, oznaczeń geograficznych czy topografii układów scalonych drogą elektroniczną.

Sektor bankowy i finansowy

Wdrożenie podpisu elektronicznego w tym obszarze napotkało na problemy infrastrukturalne. Sektor bankowy od dawna wykorzystuje certyfikaty klucza publicznego w oferowanych przez siebie internetowych i elektronicznych formach usług. Zwykłym podpisem cyfrowym posługiwały się banki już 8 lat temu przy dokonywaniu przelewów w systemie ELIXIR[6] (bez użycia papieru). Podobnie dokonywany jest obrót papierami wartościowymi, które w postaci zdematerializowanej zapisywane są na rachunkach w Krajowym Depozycie Papierów Wartościowych S. A. Ustawa z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. Nr 19, poz. 177) wprowadziła możliwość przeprowadzania przetargów i aukcji drogą elektroniczną. Zgodnie z art. 78 niniejszej Ustawy oferty składane podczas elektronicznych przetargów i aukcji powinny być opatrywane, pod rygorem nieważności, bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

Elektroniczna faktura

Z dniem 3 sierpnia 2005 roku weszło w życie Rozporządzenie w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, a także przechowywania oraz udostępniania organowi podatkowemu lub organowi kontroli skarbowej tych faktur (Dz. U. 133 z dnia 20 lipca 2005 r. poz. 1119). Rozporządzenie miało otworzyć drogę do zaistnienia elektronicznej faktury w życiu gospodarczym naszego kraju. Niestety i tutaj rozporządzenie trafiło na szereg barier, które zahamowały rozwój tej formy składania dokumentów. Wprowadzenie e-faktury miało stać się znaczącym czynnikiem usprawniającym procesy i obniżającym koszty funkcjonowania firm i instytucji. Jednak w praktyce tak się nie stało. Problemem stało się na przykład wielokrotne podpisywanie masowej liczby faktur w jednej sesji. Ze względów bezpieczeństwa każdorazowe złożenie podpisu elektronicznego wymaga ukazania się odpowiedniego komunikatu i reakcji

6 ELIXIR - (Elektroniczna Izba Rozliczeniowa) - funkcjonujący w ramach Krajowej Izby Rozliczeniowej międzybankowy system pośredniczący w elektronicznej wymianie komunikatów o zleceniach płatniczych oraz wierzytelnościach

podpisującego realizującej prawną funkcję finalizacyjną. Dla złożenia wielu podpisów decydujące w aspekcie praktycznym znaczenie ma tutaj brzmienie art. 18, ust. 1 Ustawy o podpisie elektronicznym: „ Bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej: gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ze złożeniem podpisu elektronicznego.” W praktyce oznacza to, że podpisujący będzie musiał dokonać pewnej czynności akceptującej dla każdego podpisu z osobna. Taki zapis ustawy uniemożliwia stosowanie podpisu elektronicznego w sposób masowy. Kolejnym problemem jest to, że automat stanowy karty kryptograficznej może nie dopuszczać do składania wielu podpisów a ingerencja w system operacyjny karty może być nawet technicznie niemożliwa lub naruszać prawa producenta karty. Karta również nie posiada własnego zegara co uniemożliwia ograniczenie czasu składania podpisu. Ponadto przy masowym wykorzystywaniu karty kryptograficznej do podpisywania istnieje niebezpieczeństwo szybkiego zużycia karty. Pamięć tego typu ma bowiem ograniczoną liczbę zapisów a proces zużywania się pamięci ma charakter nieuchronny. Są to istotne ograniczenia w masowym stosowaniu e-podpisu przy wystawianiu dużej liczby faktur.

Administracja publiczna

Od sierpnia 2006 roku ustawa o podpisie elektronicznym nakłada na organy władzy publicznej obowiązek umożliwienia odbiorcom usług certyfikacyjnych wnoszenia podań i wniosków oraz innych czynności w postaci elektronicznej. Pierwsze projekty administracji publicznej wypełniające wymogi ustawy zostały już wdrożone. Przykładem jest projekt "Wrota Małopolski", w ramach którego wiele gmin i powiatów z tego regionu zapewniło swoim mieszkańcom możliwość elektronicznego załatwiania spraw w urzędzie. Kolejnym wdrażanym projektem są „Wrota Podlasia” czy też „Wrota Wielkopolski”. Podstawą prawną działania przedmiotowego portalu był Plan Informatyzacji Państwa[7] na rok 2006 przyjęty rozporządzeniem Rady Ministrów z dnia 1 sierpnia 2006 r. w sprawie Planu Informatyzacji Państwa na rok 2006 (Dz. U. Nr 147, poz. 1064). Plan ten został przedłużony na lata 2007-2010 i w najbliższym czasie informatyzację rozwijać będzie w trzech dziedzinach: e-zdrowie, e-edukacja i centrum certyfikacji – czyli wydającego certyfikaty kwalifikowane i niekwalifikowane, dzięki którym będzie możliwy elektroniczny obieg dokumentów. Platformy te jednak nie mogą obsługiwać wniosków w tak kluczowych obszarach jakimi jest na przykład planowanie i zagospodarowanie przestrzenne. Plany

7 Plan Informatyzacji Państwa – jest instrumentem planowania i koordynowania informatyzacji działalności podmiotów publicznych w zakresie realizowanych przez te podmioty zadań publicznych. Zasady ustanawiania Planu określa Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

urbanistyczne i koncepcje zagospodarowania w dalszym ciągu są przyjmowane w postaci tradycyjnej. Projekty takie mają kluczowe znaczenie dla rozwoju przestrzennego oraz mają wpływ na środowisko. Ustawa „ Prawo zagospodarowania przestrzennego" (Dz.U.99.15.139 z dnia 25 mają 1999 zm. Dz.U.99.41.412) reguluje ograniczenie niekontrolowanego rozpraszania zabudowy czy racjonalizację modelu osadnictwa (np. rozwój policentryczny), politykę wobec miast, politykę metropolizacji, zadania ośrodków regionalnych oraz określa zasady tworzenia i składania wniosków budowlanych.

Urzędy stanu cywilnego

Taki stan rzeczy jest spowodowany w głównej mierze barierami technologicznymi jak również wysokimi kosztami budowy infrastruktury związanej z przechowywaniem certyfikatów klucza publicznego. Przedłużenie okresu przechowywania elektronicznych potwierdzeń na dłuższy czas niż określa to ustawa o podpisie elektronicznym wymaga wdrażania nowych technologii przechowywania danych w postaci elektronicznej oraz dużych nakładów na budowę bezpiecznych centrów gromadzenia danych. Wszystkie te aspekty w chwili obecnej stanowią duży problem natury cywilizacyjnej i nie są możliwe do podźwignięcia dla podmiotu świadczącego usługi jako Centrum Certyfikacji.

Podpis elektroniczny stosowany w obecnej formie długo jeszcze nie będzie mógł sprostać wszystkim wymaganiom, jakie niesie ze sobą ustawodawca oraz dostarczać wszystkich usług, którymi są zainteresowani potencjalni użytkownicy. W takiej sytuacji przynieść mogą pomoc jedynie nowe rozwiązania oparte na kryptografii dynamicznej[8]. Przełamią one obecne bariery we wdrażaniu nowych usług związanych z podpisem i dokumentem elektronicznym.

Podpisy cyfrowe oparte na kryptografii dynamicznej

Całkowicie inne podejście do podpisów elektronicznych mają algorytmy kryptografii dynamicznej, które nie używają klucza publicznego w jawnej postaci. Przykładem algorytmu szyfrowania dynamicznego jest metoda ZT-UNITAKOD[9]. Istotnym elementem systemu kryptograficznego opartego na tej metodzie są tablice kodów kryptograficznych tworzone dynamicznie podczas szyfrowania wiadomości. Taki system kryptograficzny charakteryzują następujące cechy.

8 Kryptografia dynamiczna – model szyfrowania oparty na generowaniu dynamicznych tablic kryptograficznych

9 ZT-UNITAKOD – protokół szyfrowania zapewniający ochronę informacji, identyfikację nadawcy i odbiorcy oraz szyfrowanie nagłówku. Posiada w patent Stanach Zjednoczonych nr 08/775, zrealizowany jako system TMW-ULTRA.

– jawność metody ochrony informacji, zamiast obowiązującej tajności ochrony klucza prywatnego,
– możliwość szyfrowania dowolnej informacji, w dowolnym języku, jak również planów i zdjęć,
– usunięcie czynnika ludzkiego, który był najsłabszym elementem systemu kryptograficznego.

Nie ma tutaj możliwość zgubienia lub kradzieży karty kryptograficznej oraz ujawnienia PIN-u.

Podpisana i zaszyfrowana wiadomość nie wymaga przechowywania certyfikatów klucza publicznego w repozytorium. Wygenerowany szyfrogram można odczytać oraz zidentyfikować jego nadawcę po dowolnie długim okresie czasu bez konieczności wyszukiwania w bazie certyfikatów klucza publicznego. Taka forma kryptografii nie wymaga użycia kluczy do składania podpisu elektronicznego. Kluczem w tej kryptografii jest podpisywana informacja, czyli dokument. Nie ma więc konieczności budowania centrum, które musiało by przechowywać klucze wszystkich podmiotów używających podpisu. W ten sposób wymogi związane z koniecznością budowy i utrzymania infrastruktury klucza publicznego zostają wyeliminowane. Implikuje to ze sobą daleko idące uproszczenia w stosowaniu e-podpisu w obszarach o szczególnych wymaganiach takich jak. np. wydziały ksiąg wieczystych, urzędy patentowe czy urzędy rejestrujące znaki przemysłowe itd. W algorytmie szyfrowania bierze udział sam ciąg szyfrowy jako cześć składowa algorytmu. Na podstawie treści nadawanej wiadomości są generowane tablice kryptograficzne. Tak więc rolę klucza w rozumieniu klasycznej kryptografii pełni sama wiadomość. Taka sytuacja stwarza wprost brak konieczności stosowania jakichkolwiek kluczy kryptograficznych zaszytych w formę certyfikatu klucza publicznego bądź prywatne go. Certyfikaty te są w każdej sesji być wymieniane pomiędzy nadawcą a odbiorcą, a najważniejszym elementem bezpieczeństwa i generowania tablic kryptograficznych jest czas. Ma to swoje daleko idące konsekwencje w rozwiązaniach systemowych obsługujących podpisywanie i szyfrowanie wiadomości tą metodą.

Lista usług i obszarów zastosowań, których może objąć podpis elektroniczny oparty na kryptografii dynamicznej jest długa: wpisy do księgi wieczystej, plany urbanistyczne, potwierdzenia notarialne, wnioski patentowe itd.

Zastosowania, które może objąć kryptografia dynamiczna

Szansę na zmianę sytuacji, w której podpis elektroniczny nie jest w stanie sprostać wszystkim wymaganiom ustawowym daje opracowana w 2004 r. metoda ZT-UNITAKOD. Metoda

ta może być stosowana przy konstruowaniu systemów podpisu elektronicznego opartych na kryptografii dynamicznej. Pierwsze wdrożenia tej metody umożliwią potencjalnym użytkownikom na dostęp do usług, które do tej pory nie były dostępne w formie elektronicznej. Kryptografia ta rozszerza możliwości, które daje obecnie podpis elektroniczny o nowe obszary zastosowań zarezerwowane tylko do formy papierowej.