§ 1

KIERUNKI REGULACJI PRAWNYCH NA ŚWIECIE

Kwestie związane z jakością usług podpisów elektronicznych, a co za tym idzie, bezpieczeństwa obrotu za pośrednictwem Internetu, są na tyle ważkie, iż stały się przedmiotem prac legislacyjnych. Mają one na celu zrównanie prawne podpisu elektronicznego z podpisem własnoręcznym oraz wytyczają normy regulujące działalność urzędów certyfikacji. Prawne regulacje podpisu elektronicznego istnieją już w wielu krajach, m. in. USA, Czechach, Wielkiej Brytanii, Niemczech, Hiszpanii, Irlandii... Lista jest długa ponieważ kraje Unii Europejskiej były zobligowane unormować swoje prawo odnośnie podpisu elektronicznego już do połowy lipca 2001 roku. W światowych regulacjach główny nacisk kładzie się na otwarty katalog technologii podpisów, w wiarygodne procedury autoryzacji i weryfikacji składania oświadczeń woli w drodze elektronicznej, ochronę konsumenta, ochronę danych, bezpieczeństwo prawne obrotu, regulacje rynku poświadczania autentyczności podpisów elektronicznych oraz możliwie najwyższy poziom tych usług.

Również Polska jako kandydat do Unii Europejskiej musi dostosować odpowiednio swoje normy prawne w tym zakresie. Prace nad polską ustawą o podpisie elektronicznym rozpoczęto już w 2001 roku. Początkowo istniały dwa projekty, różniące się zasadniczo w wielu punktach, z których powstała finalna wersja ustawy przyjęta przez Sejm 31 sierpnia 2001 roku. Wskutek wniesienia poprawek senackich ustawa wróciła pod obrady Sejmu, gdzie 18 września 2001 roku na ostatnim posiedzeniu w kadencji ostatecznie uchwalono obowiązujący tekst ustawy. Po podpisaniu przez Prezydenta RP, została ogłoszona 15 listopada 2001r. w Dzienniku Ustaw. Vacatio legis dla ustawy wynosi dziewięć miesięcy. Wprowadzenie rozwiązań dotyczących tej kwestii wymaga pośpiechu, gdyż tylko te kraje, które szybko dostosują się do wyzwań społeczeństwa informacyjnego mogą liczyć na największe korzyści. Uchwalona przez Sejm ustawa jest zgodna z Dyrektywą Unii Europejskiej w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego.

Najważniejszym zadaniem ustawy jest usankcjonowanie prawne ważności podpisu elektronicznego oraz uznanie go za wiążący dowód zawarcia umowy. Od chwili, gdy podpis elektroniczny wejdzie do polskiego systemu prawnego, będzie możliwe przeprowadzanie transakcji od początku do końca w Internecie. Wyobraźmy sobie sprzedaż polisy

ubezpieczeniowej on-line. Oto jak może ona wyglądać w nieodległej przyszłości. Klient wypełnia na stronie WWW formularz i otrzymuje ofertę z wysokościami składek. Następnie wybiera polisę, składa podpis elektroniczny i otrzymuje podpisaną umowę, oczywiście również w postaci elektronicznej. Wówczas płaci pierwszą składkę, używając ponownie podpisu elektronicznego. Dziś w Internecie można jedynie uzyskać informację o ofercie towarzystw ubezpieczeniowych i wypełnić formularz, dzięki któremu agent ma szansę wcześniej przygotować umowę. Papierowe dokumenty wciąż dublują techniki komputerowe.

Obecnie niezadowolenie właścicieli firm sprzedających produkty lub usługi za pośrednictwem Sieci jest w pełni uzasadnione. Internetowi dowcipnisie nie próżnują, często podają fałszywe dane i znaczna część transakcji nie jest finalizowana. W przyszłości nie będzie miejsca na takie żarty. Kupującemu, który złoży zamówienie potwierdzone elektronicznym podpisem, trudno będzie wyprzeć się zawarcia umowy. Zagrożone będzie to sankcją karną.

Bardzo istotny jest fakt, że ustawy o podpisie elektronicznym są całkowicie "wolne" technologicznie i nie ograniczają w żaden sposób rozwiązań, które będą wspierać zastosowanie podpisu elektronicznego. W wyniku zastosowania takich rozwiązań nie trzeba będzie zmieniać norm prawnych w razie dalszego rozwoju technologicznego.

---

§ 2
ZAUFANIE ZWYKŁE I KWALIFIKOWANE

Wiarygodność prawna obrotu na stronach WWW zakłada wiele jego poziomów, takich jak konstrukcja instytucji prawa materialnego, dostosowanie procedur odpowiednio do przyjmowanej wartości oświadczeń woli składanych drogą elektroniczną, ochrona prawna komunikowania się w cyberprzestrzeni oraz wyznaczenie poziomu zaufania do osób świadczących usługi dla kontrahentów w Internecie.

Uważa się, że między kontrahentami w sieci najważniejsza rola przypadnie tzw. zaufanej trzeciej stronie (ang. trusted third party), czyli osobom, firmom lub urzędom dostawcom usług poświadczania autentyczności podpisu (ang. certification service providers). Przy podpisie odręcznym taką rolę pełnią notariusze, a w pewnych sytuacjach

adwokaci i radcy prawni oraz urzędnicy. Poziom zaufania publicznego, podobnie jak w stosunku do wyżej wymienionych, zakłada instytucjonalna forma akredytacji przy specjalnym urzędzie nadzorującym podmioty świadczące usługi certyfikacyjne. Przy tym nie neguje się istnienia innej kategorii takich podmiotów, gdyż zgodnie z kierunkiem wytycznych Unii Europejskiej nie ma obowiązku akredytacji. Zaufanie trzeciej strony działa w obrocie niejako na dwóch poziomach zaufania: "bez akredytacji" oraz "z akredytacją". Obie kategorie można określić jako:

- zaufanie zwykłe ("bez akredytacji") czyli nie wykraczające poza ogólne ramy gwarancji i rękojmi powszechnego obrotu cywilno-prawnego;
- zaufanie kwalifikowane ("z akredytacją") odnoszące się do szczególnego poziomu weryfikacji oferowanych usług i związane z tym odpowiednio najwyższe zaufanie do jakości usług poświadczania i certyfikacji. Przypada więc ono podmiotom akredytowanym przy kompetentnym urzędzie nadzorującym i monitorującym usługi wydawania certyfikatów.

Warto zauważyć, że znany i używany na całym świecie system oprogramowania zapewniający "całkiem niezłą prywatność" PGP (ang. pretty good privacy) wymaga tylko znalezienia i zaakceptowania przez strony nawiązujące kontakt dwóch osób, firm lub instytucji, które już mają poświadczenia swoich podpisów. Te dwa podmioty swoim podpisem i autorytetem certyfikują podpisy i klucze innych. Wynika z tego wniosek, iż system poświadczania autentyczności może się obejść bez kontroli urzędów i centralnego monitorowania.

---

§ 3
STRUKTURA KLUCZA PUBLICZNEGO

Światowe rozwiązania prawne wprowadzają pojęcia dwóch rodzajów certyfikatów: zwykłego i kwalifikowanego. Certyfikat kwalifikowany wydawany jest przez podmiot posiadający akredytację Krajowego Centrum Certyfikacji. Wprowadzenie zasady akredytacji, ma na celu zapewnienie użytkowników, że organizacje ubiegające się o pełnienie funkcji zaufanej trzeciej strony są do tego odpowiednio przygotowane i spełniają założenia właściwej im ustawy. Jednakże akredytacja jest całkowicie dobrowolna a organy, które nie będą jej podlegały mogą

wystawiać tzw. certyfikaty zwykłe. W ten sposób powstaje hierarchia centrów certyfikacji oparta o strukturę klucza publicznego (PKI). Infrastruktura Klucza Publicznego (PKI) służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów. Większość najważniejszych standardów w dziedzinie bezpieczeństwa teleinformatycznego jest zaprojektowana tak, aby umożliwić współpracę z PKI. Do podstawowych usług PKI należą:

- uwierzytelnianie podmiotów partnerskich, które oznacza pełną identyfikację uczestników transakcji
- uwierzytelnianie danych pozwalające stwierdzić, że informacja była podpisana przez użytkownika
- zapewnienie integralności danych czyli pewności, że informacja podpisana cyfrowo nie została zmieniona
- poręczenie niezaprzeczalności, uniemożliwiające uczestnikom transakcji późniejsze zaprzeczenie podpisu
- zapewnienie odpowiedniego stopnia poufności, umożliwiającej użytkownikom właściwą ochronę danych przed nieuprawnionym ujawnieniem
- zapewnienie prywatności, pozwalającej użytkownikom na nakazanie specjalnej obsługi informacji podczas transmisji.

Idea PKI oparta jest na cyfrowych certyfikatach potwierdzających związek między konkretnymi uczestnikami transakcji a kluczami kryptograficznymi, stosowanymi podczas realizowania bezpiecznych transakcji.

Certyfikat cyfrowy jest wydawany przez Urząd Certyfikacji (Certification Authority - CA), który w momencie wydania dokumentu potwierdza podpisem cyfrowym związek pomiędzy użytkownikiem a kluczem, którego używa. Ponieważ tak wystawiony certyfikat ma zawsze pewien okres ważności (np. jeden rok), należy przewidzieć następujące sytuacje związane z zarządzaniem certyfikatami: rejestracja użytkowników, generowanie certyfikatów, dystrybucja, aktualizacja i unieważnianie.

Struktura PKI składa się z trzech głównych elementów :

- Urzędów Rejestracji (ang. Registration Authority - RA), dokonujących weryfikacji danych użytkownika a następnie jego rejestracji.
- Urzędów Certyfikacji (ang. Certification Authority - CA), wydających certyfikaty cyfrowe. Jest to poprzedzone procesem identyfikacji

zgłaszającego się o wydanie certyfikatu. Pozytywne rozpatrzenie zgłoszenia kończy się wydaniem certyfikatu wraz z datą jego rozpatrywania.

- Repozytoriów kluczy, certyfikatów i list unieważnionych certyfikatów (ang. Certificate Revocation Lists - CRLs). Dostęp do CRLs jest możliwy dzięki protokołom HTTP, FTP, X.500, LDAP i poczcie elektronicznej. Certyfikat może stać się nieważny przed datą jego wygaśnięcia. Przyczyną tego może być np. zmiana nazwiska lub adresu poczty elektronicznej użytkownika czy ujawnienie klucza prywatnego. W takich przypadkach CA odwołuje certyfikat i umieszcza jego numer seryjny na ogólnodostępnej liście CRL.

Struktura PKI jest tworzona w oparciu o Główny Urząd Certyfikacji, przy czym dla każdego z obszarów zastosowań (np. handel elektroniczny, sektor bankowo-finansowy, administracja publiczna), które będą korzystać z PKI, można tworzyć odrębne CA podległe Głównemu Urzędowi. Główny CA określa ogólną politykę certyfikacji, natomiast CA obsługujące dany obszar zastosowań odpowiadając za politykę w tym obszarze. W strukturze podległej danemu CA dla konkretnych zastosowań może istnieć dowolna liczba podległych CA oraz użytkowników. Taka struktura tworzy hierarchię uwierzytelniania, która z kolei określa łańcuch certyfikatów, wiodący od użytkowników aż do cieszącego się ich zaufaniem Głównego CA. Krajowa struktura PKI musi współdziałać ze strukturami PKI innych krajów, aby zapewnić usługi o podobnym do opisanych charakterze w kontaktach międzypaństwowych.

Podstawowe funkcje, które musi realizować każde PKI, aby zapewnić właściwy poziom usług to :

- rejestracja (ang. registration)

Użytkownik końcowy składa wniosek do Organu Rejestracji o wydanie certyfikatu. Jest to związane z dostarczeniem szeregu informacji, wymaganych przez Kodeks Postępowania Certyfikacyjnego (Certification Practices Statement - CPS) wybranego CA. Dane te to np. nazwa własna, nazwa domenowa czy adres IP. Zanim CA wystawi certyfikat sprawdza (korzystając z wytycznych zapisanych w CPS), czy podane przez użytkownika dane są zgodne z prawdą. Jeżeli o certyfikat ubiega się osoba fizyczna, CA weryfikuje także autentyczność własnoręcznego podpisu na wniosku o wydanie certyfikatu.

- certyfikacja (ang. certification)

Jeżeli dane podane przez ubiegającego się o certyfikat we wniosku zostaną potwierdzone, CA wystawia nowy certyfikat (zawierający m.in. klucz publiczny posiadacza) i dostarcza go użytkownikowi. Jednocześnie certyfikat zostaje udostępniony wszystkim zainteresowanym poprzez złożenie go we właściwym repozytorium publicznym.

- generacja kluczy (ang. key generation)

Para kluczy (prywatny i publiczny) może zostać wygenerowana samodzielnie przez użytkownika końcowego lub może on tę operację powierzyć CA. W pierwszym przypadku użytkownik przesyła do CA jedynie swój klucz publiczny w celu poddania go procesowi certyfikacji. Klucz prywatny pozostaje przez cały czas w rękach właściciela, dlatego też metodę tę uważa się za najbardziej bezpieczną. Jeżeli natomiast klucze generuje CA, to są one dostarczane do użytkownika końcowego w sposób gwarantujący ich poufność. Najchętniej wykorzystuje się do tego celu karty mikroprocesorowe (ang. smartcard) czy karty PCMCIA, obie zabezpieczone dodatkowym kodem PIN.

- odnawianie kluczy (ang. key update)

Wszystkie pary kluczy oraz skojarzone z nimi certyfikaty wymagają okresowego odnawiania. Jest to kolejne zabezpieczenie na wypadek ujawnienia klucza prywatnego skojarzonego z kluczem publicznym umieszczonym na certyfikacie. Istnieją dwa przypadki, kiedy wymiana kluczy jest konieczna :

a) upłynął okres ważności certyfikatu

Jest to sytuacja normalna, występująca regularnie co pewien czas (np. raz do roku). Wymiana kluczy odbywa się wtedy w możliwie krótkim czasie, bez dodatkowych formalności.

b) klucz prywatny skojarzony z kluczem publicznym umieszczonym na certyfikacie został skompromitowany

Jest to sytuacja wyjątkowa, a więc wymiana kluczy nie będzie już tak płynna jak poprzednio. W takich przypadkach CA odwołuje certyfikat poprzez umieszczenie jego numeru seryjnego na ogólnodostępnej liście CRL. Od tego momentu stary certyfikat traci ważność i rozpoczyna się procedura wystawiania nowego certyfikatu. Najgorszy przypadek dla każdego CA to kompromitacja klucza prywatnego jego Głównego CA (Root CA). W takim przypadku cała infrastruktura PKI podległa temu

pechowemu CA zostaje uznana za skompromitowaną i musi być tworzona od nowa.

- certyfikacja wzajemna (ang. cross-cerification)

Ponieważ społeczność międzynarodowa nie stworzyła dotąd Globalnego Organu Certyfikacji (Global Root CA), powstało wiele Głównych Organów Certyfikacji (Root CA), początkowo nie powiązanych wzajemnie relacjami zaufania. Certyfikacja wzajemna rozwiązuje ten problem i pozwala użytkownikom z jednej struktury PKI ufać certyfikatom wystawianym przez CA z innej struktury. Główne CA z różnych struktur certyfikują się wzajemnie - może być to certyfikacja jednokierunkowa albo dwukierunkowa.

- odwołanie certyfikatu (ang. revocation)

Istnieją sytuacje, w których zachodzi potrzeba wcześniejszego odwołania certyfikatu. Powodem może być kompromitacja klucza prywatnego, zmiana nazwy przez użytkownika końcowego czy też odejście pracownika z firmy, która wystawiła mu certyfikat. Zdefiniowana w standardzie X.509 metoda odwoływania certyfikatów wykorzystuje wspomniane już Listy Unieważnionych Certyfikatów (Certificate Revocation Lists - CRLs), okresowo publikowane przez CA w tym samym repozytorium, w którym są przechowywane certyfikaty. Każdy certyfikat posiada swój unikalny numer seryjny przypisany przez CA w momencie jego wystawiania. Lista CRL zawiera spis identyfikatorów odwołanych certyfikatów i jest opatrzona znacznikiem czasu wystawionym przez CA.

- odzyskiwanie klucza (ang. key recovery)

Jest to dodatkowe zabezpieczenie na wypadek sytuacji, gdy użytkownik utraci swoje klucze. Jeżeli wszystkie klucze do szyfrowania albo negocjacji kluczy były przechowywane w bezpiecznym archiwum, to będzie można je odzyskać i umożliwić dostęp do zaszyfrowanych danych. Najważniejszym zagadnieniem przy realizacji tej funkcji jest zagwarantowanie, że klucze będzie mógł odzyskać tylko ich właściciel a nie osoba trzecia.

---

§ 4
ROZWIĄZANIA PRAWNE W STANACH ZJEDNOCZONYCH

Pierwszym krajem, który przyjął ustawę o podpisie elektronicznym były Stany Zjednoczone. Prezydent Bill Clinton podpisał 30 czerwca 2000 roku ustawę o podpisach elektronicznych w obrocie krajowym i globalnym (Electronic Signatures in Global and National Commerce Act), która weszła w życie trzy miesiące później. Ustawa amerykańska przyznaje podpisowi elektronicznemu identyczną moc prawną jaką ma podpis złożony na papierze, jednak nie nakłada obowiązku posługiwania się nim. Przewiduje, że w każdej okoliczności należy zagwarantować obywatelom możliwość posługiwania się wyłącznie podpisem odręcznym. Zgodnie z ustawą, podpis elektroniczny jest ciągiem zakodowanych znaków, które jednoznacznie identyfikują użytkownika. Aby uniknąć oszustw w USA każdy podpis będzie weryfikowany dodatkowo poprzez np. wpisanie numeru ubezpieczenia społecznego. Ustawa nie przesądza jaka technologia podpisu elektronicznego może być stosowana, nie ogranicza też rynku usług certyfikacyjnych.

Federalna ustawa amerykańska (tzw. e-sign) weszła w życie 1 października 2000 roku. Przyjętą praktyką w USA jest, iż ustawy federalne mają charakter ramowy, pozostawiając szczegółowe rozwiązania regulacjom stanowym. Ustawa federalna nie jest więc prawem zupełnym, jakie można odnieść do materii podpisu elektronicznego, problematyka ta bowiem jest objęta jeszcze ustawami stanowymi. Dwadzieścia dwa stany wprowadziły, po poprawkach, tzw. Uniform Electronics Transaction Act. Kilka stanów np. Utah, Kalifornia i Washington wprowadziło dodatkowo przepisy dotyczące rejestracji oraz licencjonowania organów certyfikacyjnych.

Amerykańscy analitycy podkreślają, że choć przyjęcie tego aktu prawnego jest niezmiernie istotne dla tworzenia podstaw funkcjonowania elektronicznego obrotu gospodarczego, upłynie jednak sporo czasu zanim elektroniczne podpisy i certyfikaty zyskają powszechną aprobatę i zaufanie. Chociaż Amerykanie mogą już nie wychodząc z domu kupić samochód lub podpisać umowę o kredyt hipoteczny a wszelkie formalności, łącznie z zawarciem umowy mogą być dokonywane elektronicznie to konsumenci na razie wykazują się pewną wstrzemięźliwością w tego rodzaju zakupach on-line. Nie ma obecnie powszechnej świadomości, że podpis elektroniczny to coś naprawdę niezbędnego. Pewną barierą są też wysokie koszty funkcjonowania systemu. Samo wydanie klucza prywatnego to wydatek rzędu 5-10 USD za użytkownika.Do tego należy doliczyć koszty oprogramowania

wahające się między 10 a 100 USD od osoby. Zatem nowa technologia wcale nie musi przynieść firmom znacznych oszczędności w związku z eliminacją wytwarzania i przechowywania papierowych dokumentów.

---

§ 5
ROZWIĄZANIA PRAWNE W UNII EUROPEJSKIEJ

Regulacja prawna podpisu elektronicznego na poziomie Unii Europejskiej była koniecznością, aby zharmonizować, w zakresie wynikającym z kompetencji Komisji Europejskiej, minimalne ramy prawne dla podpisu elektronicznego tak, aby różnice uregulowań pomiędzy krajami członkowskimi nie naruszały zasad swobody przepływu towarów i usług w rynku wewnętrznym.

Działając na podstawie art. 47 § 2 oraz art. 55 i 95 Traktatu powołującego Wspólnotę Europejską, 13 grudnia 1999 r. Parlament Europejski i Rada przyjęły Dyrektywę nr 1999/93/WE w sprawie ram wspólnotowych dla podpisu elektronicznego. Stanowi ona pierwszy przykład dyrektywy o tak zwanym Light and flexible approach. Oznacza to, w rozumieniu Komisji Europejskiej, że rynek zachowuje się rozsądnie i poza minimalnymi uregulowaniami prawnymi, niezbędnymi dla zapewnienia swobody przepływu towarów i usług, nie ma konieczności regulacji wszystkich elementów funkcjonowania podpisu elektronicznego.

Pierwotnym źródłem inspiracji dla projektu były wstępne prace nad jednolitymi regułami międzynarodowymi dotyczącymi podpisu elektronicznego, jakie zostały podjęte przez Komisję ds. Międzynarodowego Prawa Handlowego Organizacji Narodów Zjednoczonych w 1996 r.. W 1997 r. Komisja Europejska opublikowała komunikat zatytułowany: "Zapewnić bezpieczeństwo i zaufanie w komunikacji elektronicznej. W stronę europejskich ram dla podpisu cyfrowego i szyfrowania", a następnie przedstawiła projekt dyrektywy. Przyjęty tekst jest rezultatem kompromisu politycznego państw członkowskich. Członkowie Unii Europejskiej byli zobowiązani przenieść do swojego porządku prawnego postanowienia tej dyrektywy do 19 lipca 2001r.

Celem tej dyrektywy jest stworzenie jednolitych podstaw prawnych dla podpisu elektronicznego, które zapewnią sprawne funkcjonowanie rynku wewnętrznego Wspólnot Europejskich w tej materii. W zamyśle Komisji nowe ramy prawne obejmując zespół kryteriów prawnego uznania podpisu elektronicznego ułatwią działanie handlu elektronicznego i pozwolą konsumentom i podmiotom gospodarczym w Europie na lepsze włączenie się i korzystanie z globalnej sieci.

Dyrektywa ta stanowi warunek bezpieczeństwa prawnego transakcji elektronicznych i z tego względu warunkuje rozwój handlu elektronicznego. Jak wskazano w preambule do dyrektywy, te nowe formy podpisu będą stosowane w sektorze publicznym w kontaktach z administracją krajową i wspólnotową oraz w kontaktach pomiędzy tymi administracjami, jak również z obywatelami i podmiotami gospodarczymi, na przykład: przy okazji przetargów publicznych, w regulowaniu należności fiskalnych, przekazywaniu składek na ubezpieczenie społeczne lub zdrowotne itp. Stosowanie podpisu elektronicznego będzie się coraz bardziej rozwijać mnożąc okoliczności i warunki, w jakich stosowanie tej formy czynności prawnych, zrównane w skutkach prawnych z dotychczas stosowanymi, będzie stanowić równoprawną formę w obrocie gospodarczym.

Cel i zasięg dyrektywy

Dyrektywa europejska na temat ram wspólnotowych dla podpisu elektronicznego ma na celu ułatwienie korzystania oraz prawne uznanie podpisu elektronicznego (art. 1). Przyjęte zostało podejście funkcjonalne do podpisu elektronicznego, które można odnaleźć w ustawach wzorcowych w sprawie handlu elektronicznego przyjętego przez Komisję ds. Międzynarodowego Prawa Handlowego Organizacji Narodów Zjednoczonych (CNUDCI). Dyrektywa ma na celu ustanowienie ram prawnych dla podpisu elektronicznego oraz usług certyfikacji. Paragraf 2 tego artykułu wyklucza z zakresu dyrektywy "aspekty związane z zawieraniem oraz ważnością umów oraz innymi wymaganiami prawnymi, jeżeli ustawodawstwo krajowe lub wspólnotowe zawiera wymagania formalne w tym zakresie". Dyrektywa nie odnosi się również do zasad oraz ograniczeń używania dokumentów, które przewidują ustawodawstwa krajowe i wspólnotowe.

W preambule dyrektywy odnajdujemy również zapis o wykluczeniu z jej zasięgu sieci zamkniętych, których funkcjonowanie w wymianie gospodarczej może być regulowane zgodnie z zasadami swobody

kontraktowania. Jednakże podpis elektroniczny stosowany w obrębie takich sieci winien korzystać z takich samych gwarancji dopuszczalności jako dowód przed sądami powszechnymi, jak podpis elektroniczny regulowany dyrektywą, stosowany w sieciach otwartych.

Postanowienia dyrektywy, nie wykraczają poza kompetencje Komisji i pozostawiają państwom członkowskim pole manewru co do ewentualnego rozszerzenia zasięgu uregulowań prawnych dotyczących podpisu elektronicznego.

Niektórzy ustawodawcy europejscy wprowadzili uregulowania nowatorskie, a czasem nawet rewolucyjne w tej dziedzinie. Na przykład we Francji przy okazji dyskusji w Senacie nad ustawą nr 2000-230 z 13 marca 2000 r. w sprawie dostosowania przepisów o dowodzie do technologii informacyjnych oraz w sprawie podpisu elektronicznego, wprowadzono przepisy pozwalające na tworzenie i przechowywanie na nośnikach elektronicznych "aktów autentycznych" (akty prawne, do których sporządzenia potrzebna jest interwencja notariusza lub urzędnika państwowego) w warunkach określonych przez dekret Rady Państwa. Należy jednakże wskazać, że przyjęcie tego dekretu nie nastąpi szybko, praktyczne wprowadzenie w życie tego zapisu wymaga bowiem jeszcze długich prac i konsultacji eksperckich oraz przygotowania notariuszy do realizacji tego zadania.

Istotnym zapisem dyrektywy jest artykuł 3.7, który przewiduje, że stosowanie podpisu elektronicznego w sektorze publicznym może być poddane dodatkowym wymaganiom. Wymagania te muszą jednak spełniać kryteria obiektywności, przejrzystości, proporcjonalności oraz niedyskryminacji i nie powinny stanowić przeszkody do świadczenia usług ponadgranicznych dla obywateli. Można je stosować jedynie w szczególnych celach, takich jak specyficzne potrzeby związane z administracją fiskalną lub socjalną.

Definicje wg Dyrektywy UE

Artykuł 2.3 dyrektywy definiuje podpisującego jako "każdą osobę, która dysponuje urządzeniem do tworzenia podpisu na swój własny użytek lub użytek instytucji, lub osoby fizycznej, lub prawnej, którą reprezentuje". Definicja ta jest interpretowana bardzo szeroko, mowa jest bowiem tutaj o "każdej osobie", co pozwala przypuszczać, że obejmuje ona osoby fizyczne i prawne. Zresztą w komunikacie z 8 października 1997 r. Komisja zaproponowała, aby "klucze mogły być

przyznawane osobom prywatnym lub prawnym (na przykład spółkom z ograniczoną odpowiedzialnością)". Niektóre ustawodawstwa europejskie dokonały takiej właśnie interpretacji. Podpis osób prawnych jest dopuszczalny w prawie brytyjskim i włoskim, możliwość taką przewiduje również projekt ustawy belgijskiej. W ustawie wzorcowej CNUDCI na temat handlu elektronicznego termin "osoba" obejmuje zarówno osoby fizyczne, jak i prawne.Oznacza to, że osoba prawna może dysponować podpisem elektronicznym oraz odpowiadającym mu certyfikatem, który będzie wskazywał nazwę osoby prawnej bez wskazania reprezentującej ją osoby fizycznej.

Dyrektywa definiuje podpis elektroniczny jako "dane w formie elektronicznej załączone lub logicznie połączone z innymi danymi elektronicznymi i które służą jako metoda autoidentyfikacji" (art. 2.1). Definicja ta obejmuje całość technik pozwalających na realizację drogą elektroniczną funkcji podpisu klasycznego, to jest: identyfikację podpisującego oraz wyrażenie przez niego woli przystąpienia do zawartości podpisywanej wiadomości. Definicja ta odzwierciedla wolę Komisji zdefiniowania podpisu elektronicznego w sposób, który pozwala na objęcie wszelkich szczególnych technik podpisu elektronicznego, jeżeli pozwalają one samodzielnie lub w kombinacji na spełnienie funkcji podpisu.

Dyrektywa zawiera rozróżnienie pomiędzy terminami "podpis elektroniczny" oraz szczególną techniką podpisu elektronicznego "zaawansowanym podpisem elektronicznym" (art. 2.2.). W zakres tej definicji wchodzi podpis, który spełnia następujące wymagania:

a) należy wyłącznie do sygnatariusza,
b) pozwala na identyfikację sygnatariusza,
c) jest stworzony przy użyciu środków, które pozostają pod wyłączną kontrolą sygnatariusza,
d) jest połączony z danymi, do których się odnosi w taki sposób, że wszelka późniejsza modyfikacja tych danych jest możliwa do wykrycia.

Wybór terminu "zaawansowany podpis elektroniczny" jest wyborem neutralności technicznej, co pozwoli na uniknięcie jego szybkiego zdezaktualizowania oraz otwiera drogę do poszukiwań nowych technik podpisu.

Nie ulega jednak wątpliwości, że obecnie jedynie metoda podpisu cyfrowego opartego na kryptografii asymetrycznej odpowiada definicji

zaawansowanego podpisu elektronicznego w rozumieniu dyrektywy. Prace normalizacyjne prowadzone na forum międzynarodowym wskazują, że określenie poziomu bezpieczeństwa podpisu elektronicznego mającego spełniać wymagania zaawansowanego podpisu elektronicznego może faworyzować karty z mikroprocesorami jako metodę bezpieczniejszą.

Skutki prawne podpisu elektronicznego wg. Dyrektywy UE

Dyrektywa reguluje również skutki prawne podpisu elektronicznego. Cel ten spełnia art. 5, który zawiera dwie klauzule: równouprawnienia oraz zakazu dyskryminacji.

- klauzula równouprawnienia (art. 5.1) zmierza do równouprawnienia zaawansowanego podpisu elektronicznego z podpisem odręcznym, jeśli spełnione są następujące warunki: podpis musi mieć oparcie w certyfikacie określonym w art. 2.10 dyrektywy oraz musi być stworzony za pomocą bezpiecznej metody, takiej, jaką przewiduje aneks nr 3 do dyrektywy. Oznacza to, że podpis elektroniczny powinien być uznany za dowód przed organami sądowymi i powinien mieć taką samą siłę dowodu jak podpis odręczny. Klauzula ta odnosi się wyłącznie do zaawansowanego podpisu elektronicznego.

- klauzulę niedyskryminacji (5.2) stosuje się, jeśli warunki, jakim podlega klauzula równouprawnienia, nie są spełnione. Państwa członkowskie są zobowiązane do czuwania, aby odmowa skuteczności prawnej i dopuszczalności jako dowodu w sądzie podpisu elektronicznego nie była umotywowana jedynie tym, że podpis jest w formie elektronicznej lub nie towarzyszy mu kwalifikowany certyfikat, nie towarzyszy mu certyfikat wydany przez dostawcę usług certyfikacji akredytowany zgodnie z dyrektywą lub nie jest stworzony przez bezpieczną metodę tworzenia podpisów.

Warunki dopuszczalności i ważności zaawansowanego podpisu elektronicznego

Dopuszczalność przedstawienia przed sądem dokumentu podpisanego elektronicznie oraz zakwalifikowanie podpisu jako zaawansowanego zależy od spełnienia warunków związanych z: certyfikatem, dostawcą usług certyfikacji i procesem tworzenia podpisu elektronicznego.

W załączniku nr I do dyrektywy zostały określone wymagania co do niezbędnych informacji, które muszą się znaleźć w certyfikatach "kwalifikowanych". Załącznik nr II zawiera wymagania, jakie muszą

spełniać dostawcy usług certyfikacji wydający certyfikaty "kwalifikowane". Natomiast w załączniku nr III znalazły się wymagania minimalne dotyczące gwarancji, jakie muszą być zapewnione przez bezpieczną metodę tworzenia podpisu elektronicznego.

Proces akredytacji instytucji certyfikujących

Tworzenie zaawansowanych podpisów elektronicznych będzie się opierało na dobrowolnym systemie akredytacji instytucji świadczących usługi certyfikacji.

---

§ 6
DYREKTYWA UE A ROZWIĄZANIA PRAWNE PAŃSTW EUROPEJSKICH

Państwa europejskie, które w pełnym lub niepełnym zakresie wprowadziły przepisy dotyczące podpisów elektronicznych, to m.in. : RFN, Hiszpania, Irlandia oraz Czechy, a także Austria, Belgia, Francja, Finlandia, Słowacja i Słowenia.

Na uwagę zasługuje w tej grupie RFN, której gospodarka systematycznie i intensywnie przygotowuje się do wdrażania technologii informatycznych na szeroką skale. Niemieckie ustawy: z 1 sierpnia 1997 r. (jest to szerszy akt prawny odnoszący się do usług multimedialnych pod tytułem Informations-und Kommunikationsdienste-GesetzIuKDG, Art. 3 Signaturgesetz - SigG) oraz z 22 lipca 1997 r. (Signaturgesetz uzupełniona przez SignaturVerordnung) odróżnia to, iż posługują się kategoria podpisu cyfrowego, a nie elektronicznego. Definiują one podpis cyfrowy jako oparty na zasadzie dwóch kluczy (do kodowania oraz dekodowania), prywatnego i publicznego, ale otwarte są i na inne procedury podpisu. SigG nie zakłada mocy prawnej podpisu cyfrowego na równi z podpisem własnoręcznym na zasadzie powszechnej. To ograniczenie skuteczności prawnej podpisu cyfrowego zostało już poprawione.

Regulacje niemieckie ustanawiają nadzór oraz kontrole nad usługami certyfikacyjnymi, w tym na szczeblu federalnym, i postulują przymus akredytacyjny, co zostało wszakże zmienione ze względu na przepisy dyrektywy UE 99/93, zakładające jedynie dobrowolna akredytacje.

W Republice Czeskiej oraz Irlandii przyjęto rozwiązania oparte na dyrektywie unijnej z 13 grudnia 1999 r. Dla przykładu, w ustawie irlandzkiej (The Electronic Commerce Act 2000) definicje podpisów elektronicznych sformułowano dokładnie tak, jak czyni to dyrektywa UE (1999/93/EEC). W Hiszpanii regulacje dotyczące podpisu cyfrowego uchwalono jeszcze przed dyrektywa unijna (dekret królewski 14/99 z 17 września 1999 r. - ustawa o podpisie cyfrowym). Według regulacji hiszpańskiej zaawansowany podpis elektroniczny, w istocie określony jako podpis cyfrowy, ma tę sama moc prawna, co podpis odręczny.

Na tle porównawczym zwraca uwagę, ze regulacje dotyczące podpisów elektronicznych sprzed uchwalenia dyrektywy UE 99/93 nawiązują do kategorii podpisu cyfrowego, podczas gdy ustawy późniejsze posługują się pojęciem "podpis elektroniczny".

---

§ 7
POLSKA USTAWA O PODPISIE ELEKTRONICZNYM

Przyjęta 27.07.2001 ustawa o podpisie elektronicznym powstała w wyniku blisko 9 miesięcznych prac nad projektami wniesionymi przez grupę posłów oraz projektem rządowym. Prace w Sejmowej Podkomisji Nadzwyczajnej toczyły się z licznym udziałem ekspertów ze środowisk informatycznych (Polskie Towarzystwo Informatyczne; Polska Izba Informatyki i Telekomunikacji), bankowych (Narodowy Bank Polski, Związek Banków Polskich). Zasadniczymi celami w trakcie prac nad kształtem ustawy było dostosowanie polskiego prawa do wymagań społeczeństwa informatycznego i zachowanie zgodności ze standardami europejskimi zawartymi w Dyrektywie Unii Europejskiej.

W dniu 11 października 2001 Prezydent RP podpisał ustawę o podpisie elektronicznym sposobem tradycyjnym oraz elektronicznie.

15 listopada br. opublikowano (Dz. U 130 poz. 1450) ustawę o podpisie elektronicznym. Z mocy art. 59 ust. 1 Ustawa wchodzi w życie 9 miesięcy po opublikowaniu, czyli 16 sierpnia 2002. W tym dniu, dzięki zmianie przepisu art. 60 kc, podpis elektroniczny zaistnieje w sposób pełny jako środek wyrażania oświadczenia woli ponieważ, zgodnie z nowym brzmieniem art. 78 ust 2:
"Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy

ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej."

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym staje na stanowisku, że w obrocie prawnym będzie mógł być stosowany każdy rodzaj podpisów elektronicznych. Jedynie jednak kwalifikowana postać bezpiecznego podpisu elektronicznego będzie mieć charakter równorzędny z podpisem własnoręcznym. Stosowne zmiany w kodeksie cywilnym przewidują, że elektroniczne oświadczenia woli opatrzone bezpiecznym podpisem elektronicznym weryfikowanym z pomocą kwalifikowanego certyfikatu są równoważne zachowaniu formy pisemnej z podpisem własnoręcznym. Skutki prawne wywoła jednak wyłącznie podpis złożony w okresie ważności certyfikatu. Dlatego też każdy z uczestników obrotu może i powinien sprawdzić ważność certyfikatu drugiej strony (co nie wyłącza ryzyka związanego z ewentualnym unieważnieniem certyfikatu). Ustawa dopuszcza również zwykły podpis elektroniczny, który nie jest równoważny własnoręcznemu, lecz będzie stanowił dowód podległy swobodnej ocenie sądu. W ślad za Dyrektywą 1999/93/EC ustawa stanowi, że zwykłemu podpisowi elektronicznemu nie będzie można odmówić ważności i skuteczności wyłącznie ze względu na jego elektroniczną formę. Jako osobną kategorię wprowadzono znakowanie czasem zrównane z formą tzw. daty pewnej. Ten rodzaj podpisu będzie miał duże znaczenie dowodowe, gdyż bezpieczny podpis elektroniczny jest ważny tylko, jeśli został złożony w okresie ważności certyfikatu.

Bezpieczny podpis elektroniczny musi być przyporządkowany wyłącznie do (jednej) osoby fizycznej składającej podpis. Powinien być sporządzany za pomocą podlegających wyłącznej kontroli tej osoby bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu. Musi być powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych będzie rozpoznawalna. Podpisy elektroniczne będą mogły posiadać zarówno osoby fizyczne, jak i prawne. W tym ostatnim przypadku posługiwać się nimi będzie mogła wyłącznie oznaczona osoba fizyczna. Ustawa nie daje innej możliwości elektronicznego podpisu osób prawnych a także wyłącza podpis grupy osób. Jak się wydaje możliwe technologicznie i prawnie będzie wielokrotne podpisanie dokumentu elektronicznego przez poszczególne osoby fizyczne. Osoba fizyczna może złożyć podpis elektroniczny w imieniu osoby prawnej, innej osoby

fizycznej lub jednostki organizacyjnej nie posiadającej osobowości prawnej. Zmiana po stronie osoby reprezentującej firmę powodować będzie konieczność unieważnienia poprzedniego i wydania nowego podpisu. Ponieważ podobnie jak w przypadku kart płatniczych trudno całkowicie wykluczyć pozyskanie karty z kluczem prywatnym oraz wyłudzenia PIN-ów pamiętać należy, że ryzyko dokonywanych czynności obciążać będzie właściciela. Zasadniczo odpowiedzialność wystawcy certyfikatu ograniczona będzie do sytuacji, gdy dane w certyfikacie będą niezgodne z prawdą.

Nowa ustawa o podpisie elektronicznym zawiera szereg przepisów o charakterze administracyjnym dotyczących infrastruktury certyfikacyjnej. Wyłącznie działalność w charakterze kwalifikowanego podmiotu certyfikującego podlegać będzie wpisowi do rejestru podmiotów kwalifikowanych i przed rozpoczęciem działalności wymagać będzie przeprowadzenia obligatoryjnej kontroli. Ustawa nie przewiduje dobrowolnej akredytacji dla podmiotów z poza kręgu podmiotów kwalifikowanych. Certyfikat wydany przez podmiot świadczący usługi certyfikacyjne, nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium, może zostać zrównany pod względem prawnym z kwalifikowanymi certyfikatami wydanymi przez podmiot certyfikujący, mający siedzibę lub świadczący usługi w Polsce pod warunkiem uzyskania akredytacji. Dopuszczalne będzie gwarantowanie przyjęcia odpowiedzialności przez podmiot polski za działalność certyfikacyjną podmiotu zagranicznego. Uznanie polskiego podpisu elektronicznego w innych jurysdykcjach zależeć będzie z zasady od podpisania stosownych umów.

Przepisy ustawy zostały sformułowane w sposób neutralny technologicznie. Stąd istotne znaczenie będą miały szczegółowe rozwiązania przepisów rozporządzeń wykonawczych do ustawy, które określą m.in. wymogi jakie muszą spełniać bezpieczne urządzenia służące złożeniu lub weryfikacji podpisów elektronicznych. W praktyce od treści rozporządzeń zależeć będzie dostosowanie starych czy opracowanie nowych aplikacji. Od rozporządzeń zależeć będzie czy nośnikiem bezpiecznego podpisu będzie karta procesorowa czy również plik lub dyskietka oraz jakie warunki będą musiały być zachowane dla złożenia podpisu z pomocą komputera lub komórki. Dopuszczalne będą rozwiązania inne niż najpopularniejszy obecnie i gotowy do stosowania podpis cyfrowy. Oprócz podpisów opartych na asymetrycznej kryptografii

obecna ustawa umożliwi wykorzystanie rozwiązań biometrycznych lub innych wypracowanych później. Wydanie rozporządzeń wykonujących przepisy ustawy o podpisie elektronicznym może, ale nie musi nastąpić przed wejściem w życie nowego prawa.

W ciągu roku Minister Finansów dostosuje przepisy o opłatach skarbowych za czynności administracyjne (znaczki skarbowe). Banki i organy władzy publicznej mają dwa lata na dostosowanie swojej działalność w zakresie świadczenia usług związanych z podpisem elektronicznym oraz wykorzystania systemów teleinformatycznych związanych ze świadczeniem usług. Jednakże organy władzy publicznej mają cztery lata od wejścia w życie ustawy na udostępnienie odbiorcom usług certyfikacyjnych wnoszenia podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy wymagają składania ich w określonej formie lub według określonego wzoru. Możliwość zdalnego wnoszenia podań, składania deklaracji podatkowych nie nastąpi natychmiast wraz z początkiem obowiązywania nowej ustawy i wymagać będzie stopniowego dostosowania prawa. Nie należy oczekiwać ułatwień w dostępie do urzędów oraz zmian w formie obrotu nieruchomościami, prawie rodzinnym oraz w zakresie weksli oraz czeków.

Podpisem elektronicznym będą mogły być podpisane jedyne dokumenty sporządzone w formie elektronicznej, bez względu na to, na jakim nośniku będą przenoszone (za pomocą sieci, CD-Romu, czy dyskietki). Nie będzie możliwe podpisanie dokumentu papierowego podpisem elektronicznym. W projektach ustawy nie przewiduje się, aby umowy zawarte z użyciem podpisu elektronicznego mogły zastąpić umowy zawierane w formie aktu notarialnego. Nie będzie więc dopuszczalne zawarcie umowy kupna sprzedaży nieruchomości za pośrednictwem Internetu. Niektóre czynności, takie jak sporządzenie testamentu czy zawarcie małżeństwa, również będą wymagać odręcznego podpisu.

Istotnym mankamentem nowej ustawy jest brak zmian w przepisach kodeksu postępowania cywilnego. W szczególności nie zmieni się sposób wprowadzania dokumentów elektronicznych jako dowodu do procesu cywilnego. Jak się wydaje w przypadku sporu dokument podpisany elektronicznie nadal będzie przedkładany sądowi w formie wydruku, będącego jedynie początkiem dowodu na piśmie. Braki zmian w kodeksie postępowania administracyjnego będą w znacznej mierze do usunięcia w

drodze nowej wykładni istniejącego prawa. Ustawa stanowi konieczny warunek i ważny krok naprzód w zakresie elektronicznego obrotu prawnego w naszym kraju. Wczesne wykorzystanie korzyści elektronicznej administracji i gospodarki zależeć będzie jednak od zmiany świadomości oraz zdecydowanej woli politycznej i nakładów przeznaczanych na te cele.

FF & LL