PROPOZYCJE LEGISLACYJNE W ZAKRESIE UZNANIA ELEKTRONICZNEJ WYMIANY DOKUMENTÓW (EDI) JAKO RÓWNOWAŻNEJ OBIEGOWI DOKUMENTÓW PAPIEROWYCH

Raport Zespołu ds. Dokumentu Elektronicznego
Rady Koordynacyjnej ds. Teleinformatyki

Praca grupy ekspertów pod kierunkiem
dr inż. Jacka Piotrowskiego

wrzesień 1996

Spis treści:

Załącznik 2.
Wzór umowy EDI proponowany przez Komisję Europejską

Załącznik 3.
Ustawa o podpisie cyfrowym stanu Utah. Tytył 46, Rozdział 3 (1996)
Zasady ogólne. Kodeks postępowania administracyjnego stanu Utah. R154-10

Załącznik 4.
Przegląd wybranych regulacj prawnych i rozwiązań organizacyjnych związanych z dematerializacją faktury.

PROPOZYCJE LEGISLACYJNE W ZAKRESIE UZNANIA ELEKTRONICZNEJ WYMIANY DOKUMENTÓW (EDI) JAKO RÓWNOWAŻNEJ OBIEGOWI DOKUMENTÓW PAPIEROWYCH

STRESZCZENIE

Raport Zespołu ds. Dokumentu Elektronicznego
Rady Koordynacyjnej ds. Teleinformatyki

Praca grupy ekspertów pod kierunkiem
dr inż. Jacka Piotrowskiego

wrzesień 1996

Spis treści:

Wprowadzenie

Elektroniczna wymiana dokumentów (EDI - Electronic Data Interchange[1]) jest technologią oddziaływającą w istotny sposób na współczesną działalność gospodarczą i administracyjną. Unia Europejska, która w 1993 roku rozpoczęła swój program IDA (Interchange of Data between Administrations), realizuje aktualnie w jego ramach 33 projekty związane z kulturą, służbami celnymi, ochroną środowiska, ochroną zdrowia, zamówieniami publicznymi, ubezpieczeniami społecznymi i sprawozdawczością statystyczną. Obok tych europejskich działań centralnych, poszczególne kraje rozwinięte wprowadzają coraz szerzej udogodnienia stosowania dokumentu elektronicznego.

Opóźnienia we wprowadzaniu elektronicznej wymiany dokumentów w Polsce powodują powstanie następujących zagrożeń:

- utrudnienie procesu integracyjnego Polski z Unią Europejską, wynikające z narastających barier technologicznych i braku możliwości współpracy przy wykorzystaniu środków teleinformatycznych;
- utrudnienie handlu zagranicznego i międzynarodowej współpracy gospodarczej, wynikające z braku zdolności do uczestniczenia w systemach EDI partnerów zagranicznych;
- utrudnienie świadczenia w Polsce nowych usług bezpośrednio związanych z EDI;
- niezdolność do obniżenia kosztów działalności gospodarczej i administracyjnej, poprzez wykorzystanie EDI.

Elektroniczna wymiana danych wprowadza do istniejącej praktyki dwa nowe zjawiska:

- zanik tradycyjnej, papierowej formy dokumentu (jako oryginału i ewentualnie kopii) i zastępowanie go zapisem elektronicznym (cyfrowym), którego wszystkie kopie są technicznie nierozróżnialne;
- wymianę tak utworzonych zapisów (komunikatów) drogą telekomunikacyjną, pomiędzy zainteresowanymi stronami.

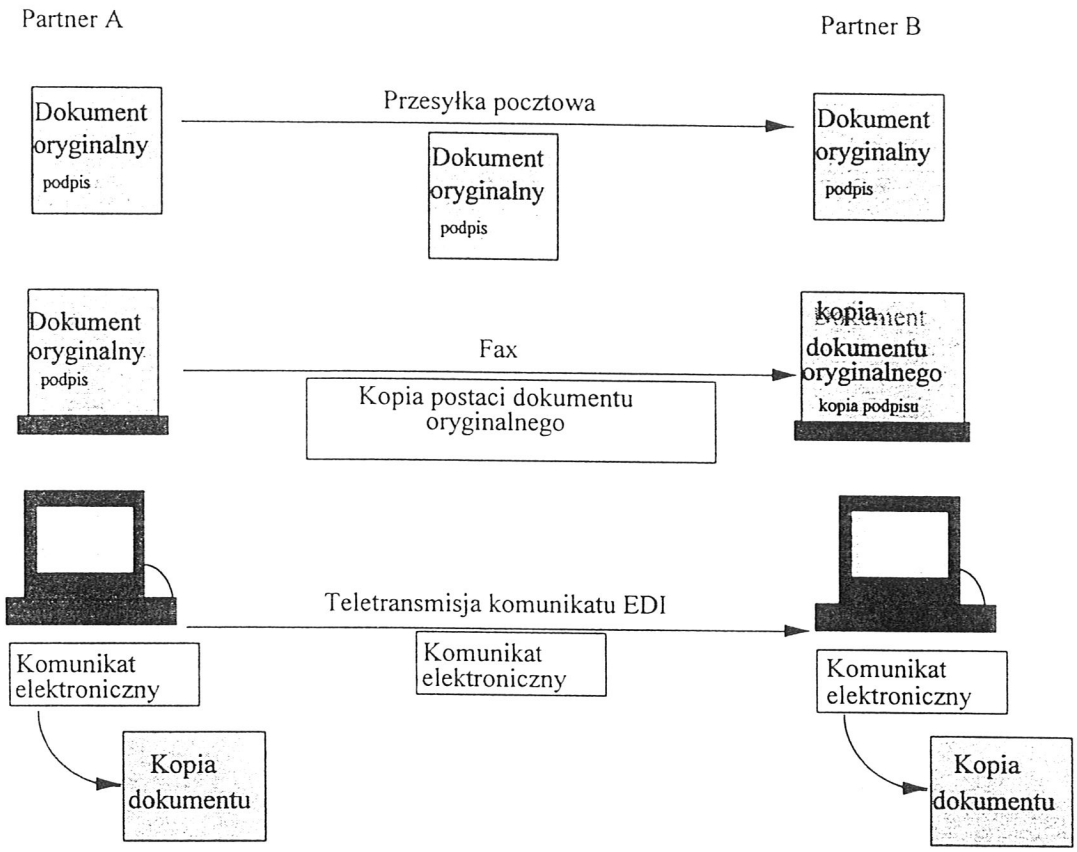
Z tych cech wynikają bariery towarzyszące wprowadzaniu EDI, które można podzielić na 4 grupy:

- prawne - ogólne
- prawne - szczegółowe (dotyczące poszczególnych typów dokumentów)
- organizacyjne
- techniczne

[1] termin ten ostatnio zastępowany jest przez określenie bardziej ogólne: Electronic Commerce - Elektroniczna gospodarka

Podstawowe bariery prawne

Chociaż w nazwie EDI eksponuje się fakt wymiany, to jednak podstawowe problemy prawne wynikają z zaniku tradycyjnej, papierowej formy dokumentu (jako oryginału i ewentualnie kopii) i zastępowanie go zapisem elektronicznym (cyfrowym), którego wszystkie kopie są technicznie nierozróżnialne. Powoduje to pośrednio brak możliwości użycia podpisu odręcznego, związanego z nośnikiem papierowym. Zjawiska te ilustruje poniższy rysunek:



Regulacje prawne wprowadzające formalne wymagania na postać dokumentów powstały z następujących pobudek:

a) w celu ułatwienia rozstrzygania ewentualnych sporów wprowadza się wymóg istnienia wiarygodnych dowodów woli stron i zaistniałych faktów;

b) w celu ochrony stron przed nieuświadomionymi konsekwencjami swych czynów, wprowadza się wymóg czytelnej i jasnej formy wyrażania przyjętych przez strony zobowiązań.

Komunikaty elektroniczne, ze względu na swą niematerialną i komputerową formę w swej ogólnej postaci nie spełniają tych wymagań. W związku z tym, od wielu lat poszukuje się nowych rozwiązań, pozwalających na uzyskanie przez nie pożądanych własności. **Poszukiwania te prowadzone są w 2 kierunkach:**

a) **wprowadzenia odpowiedniego ogólnego ekwiwalentu podpisu odręcznego, możliwego do zastosowania w odniesieniu do danych w formie elektronicznej;**

b) **wprowadzenia specyficznych, dodatkowych warunków dla elektronicznych kopii wybranych grup dokumentów, które umożliwiają ich wykorzystanie w praktyce w sposób wiarygodny i wystarczająco efektywny.**

W większości krajów Europy, ustawodawca określa własnoręczny (odręczny) podpis jako niezbędny element autoryzujący dokument (a to z kolei wyklucza formę elektroniczną dokumentu). Od tej zasady autoryzacji pojawiają się jednak coraz liczniejsze wyjątki:

- kraje akceptujące jedynie podpis odręczny:

  - **Francja**
    akceptuje jedynie podpis odręczny (z wykluczeniem np. krzyżyka);
  - **Niemcy**
    dokument musi być sporządzony na papierze, z podpisem odręcznym stron;
  - **Szwecja**
    wymaga podpisu odręcznego.

- kraje, które w wyjątkowych przypadkach dopuszczają inne formy podpisu:

  - **Norwegia**
    dopuszcza enumeratywnie użycie podpisu cyfrowego w wybranych przypadkach (bankowość, emisja akcji, transport międzynarodowy i dokumenty celne);
  - **Portugalia**
    wymaga podpisu odręcznego, za wyjątkiem dokumentów celnych;

- kraje, które ogólnie nie wymagają odręczności podpisu:

  - **Dania, Holandia, Włochy, Irlandia, Norwegia**
    nie wymagają odręczności podpisu;
  - **Stany Zjednoczone**
    Jednolity Kodeks Handlowy (UCC), będący stanowym aktem prawnym w Stanach Zjednoczonych, definiuje "podpis" jako "dowolny symbol utworzony lub zastosowany przez stronę z istniejącą intencją do uwierzytelnienia treści". Najdalej idącą regulacją wydaje się ustawa o podpisie cyfrowym (Title 46, Chapter 3 (1996)) stanu Utah, która zaczęła obowiązywać od marca 1996 roku, stanowiąca o równoważności podpisu cyfrowego i podpisu odręcznego na papierze we wszystkich przypadkach przewidzianych prawem.

W drugiej grupie rozwiązań, wprowadzane modyfikacje prawne najczęściej dotyczą elektronicznej formy faktury. Możemy tu zaobserwować następujące przypadki:

- **Polska** - nie dopuszcza elektronicznej formy faktury:
  - faktura musi mieć postać papierową (prawo podatkowe);
  - wszystkie dowody księgowe otrzymane drogą teletransmisji muszą uzyskać postać trwale czytelną (ustawa o księgowości);

- **Włochy** - dopuszczenie faktury elektronicznej w 1990 r.:
  - faktura u nadawcy powinna mieć postać papierową[2];
  - faktura o odbiorcy może mieć postać elektroniczną;
  - u odbiorcy tworzony jest rejestr zbiorczy otrzymanych faktur w sposób czytelny na nośniku trwałym.

- **Francja** - dopuszczenie faktury elektronicznej w 1991 r:

[2] w 1995 Włochy zniosły wymóg tworzenia kopii papierowej u nadawcy. Z ogólnych doniesień wynika, że przez cały dotychczasowy okres dopuszczenia faktur w postaci elektronicznej nie zanotowano żadnego przypadku z tym związanego, rozstrzyganego sądownie, incydentu.

- użytkownicy EDI muszą uzyskać certyfikat autoryzacyjny dla swych systemów informatycznych;
- faktura u nadawcy i u odbiorcy może mieć postać elektroniczną;
- nadawca i odbiorca tworzy rejestr streszczeń nadanych i odebranych faktur w sposób czytelny na nośniku trwałym;
- na żądanie istniejące dane muszą być wystarczające do odtworzenia faktury w sposób czytelny.

- **Belgia** - dopuszczenie faktury elektronicznej w 1994 r.:
  - użytkownicy EDI muszą zgłosić fakt wykorzystywania elektronicznej postaci faktury;
  - użytkownicy powinni posiadać i przechowywać pełną dokumentację używanego systemu informatycznego;
  - nadawca i odbiorca tworzy rejestr streszczeń nadanych i odebranych faktur w sposób czytelny na nośniku trwałym;
  - nadawca i odbiorca podaje w deklaracji liczbę otrzymanych i nadanych faktur w rozbiciu na kontrahentów.

Drugorzędne bariery prawne

Mniej istotne bariery prawne mogą pojawić się w odniesieniu do przechowywania dokumentu i jego czytelności.

Rygory prawne dotyczące przechowywania mogą dotyczyć następujących aspektów:
- **wymaganego czasu przechowywania,**
- **postaci w jakiej przechowywany jest dokument,**
- **rozróżnienia pomiędzy oryginałem a kopią.**

Jedną z istotnych cech dokumentu jako dowodu jest jego **czytelność dla organu rozstrzygającego** - czyli w ogólnym przypadku - sądu. W tym kontekście wartość dowodowa komunikatów EDI może być podważana z trzech powodów: ze względu na postać elektroniczną komunikatu pierwotnego, ze względu na użycie kodów (najczęściej liczbowych) w miejsce tekstów jawnych i ze względu na szyfrowanie danych stosowane jako ochrona poufności przesyłanej informacji. Wykorzystanie kryptografii może być również w danym kraju niedopuszczalne bez uzyskania odpowiednich zezwoleń.

Bariery prawne istniejące w Polsce

Przeszkody prawne związane z zastępowaniem dokumentów tradycyjnych dokumentami EDI mogą mieć dwojaką postać:
- jeśli wymóg istnienia dokumentu tradycyjnego ma w danym kraju charakter normy bezwzględnie obowiązującej (w stosunku do użytkowników EDI), to mówimy o zakazie stosowania EDI;
- jeśli wymóg istnienia dokumentu tradycyjnego jest normą względnie obowiązującą, tzn. strony mogą od tego wymogu odstąpić akceptując negatywne tego skutki (najczęściej oznacza to brak mocy dowodowej dokumentu w formie elektronicznej utworzonego w zastępstwie dokumentu tradycyjnego), to mówimy o utrudnieniach w stosowaniu EDI.

Ogólnie, polskie prawodawstwo wymaga podpisu odręcznego dla zachowania formy pisemnej czynności prawnej. W odniesieniu do podstawowych dokumentów występujących w działalności gospodarczej i administracyjnej również ustawowo wymaga się podpisów odręcznych. **Wybrane przykłady regulacji wprowadzających zakaz użycia dokumentów EDI to:**

- **Dowód księgowy dokumentujący przejęcie lub przekazanie składnika majątkowego (...) musi zawierać podpis wystawcy dowodu oraz osoby której wydano lub od której przejęto składniki majątkowe.**
- **Faktura VAT musi być sporządzona pisemnie i zawierać podpis wystawcy.**

Utrudnienia w stosowaniu dokumentów w formie elektronicznej to:

- **dla czynności gdzie transfer dóbr przekracza 2 000 zł forma pisemna jest zastrzeżona dla celów dowodowych (*ad probationem*).** Oznacza to, że niedochowanie tej formy nie powoduje nieważności dokonanej transakcji lecz taki skutek, że w razie sporu niedopuszczalny jest w zasadzie dowód ze świadków i z przesłuchania stron dla wykazania, że czynność prawna została dokonana.

Proponowane rozwiązania

Po przeanalizowaniu różnych wariantów możliwych rozwiązań w zakresie elektronicznej wymiany i archiwizowania dokumentów elektronicznych oraz dokonaniu przeglądu rozwiązań prawnych w różnych krajach postuluje się oparcie elektronicznej wymiany dokumentów na następujących zasadach:

I. Rozwiązania doraźne:

1. **regulowanie kwestii nie wymagających interwencji w istniejący porządek prawny w drodze umowy pomiędzy zainteresowanymi stronami;**
2. **opracowanie lub zainicjowanie opracowania sektorowych zasad oraz wytycznych stosowania EDI i archiwizacji dokumentów elektronicznych, w tym wzorców umów EDI i niezbędnych wymagań na ochronę komunikatów EDI;**

II. Rozwiązania podstawowe:

1. **dokonanie przeglądu i ewidencji tych dokumentów, dla których istniejący zakaz stosowania formy elektronicznej stanowi istotną niedogodność dla podstawowych podmiotów życia gospodarczego i administracyjnego w Polsce;**
2. **wprowadzenie odpowiednich zmian w przepisach wykonawczych, w celu zlikwidowania istniejących barier w stosowaniu EDI i elektronicznej archiwizacji w odniesieniu do konkretnych dokumentów, dla których ograniczenia dadzą się usunąć tą drogą;**
3. **wystąpienie w trzech przypadkach z inicjatywą ustawodawczą (patrz niżej), w postaci nowelizacji istniejących regulacji ustawowych;**

III. Rozwiązanie perspektywiczne:

rozpoczęcie przygotowań do wprowadzenia w Polsce ustawy nadającej ogólną moc prawną podpisowi cyfrowemu.

Propozycje legislacyjne w zakresie uznania elektronicznej wymiany dokumentów jako równoważnej obiegowi dokumentów papierowych

W miarę możliwości należy dążyć do zmian regulacji na płaszczyźnie sektorowej, jednakże nie zawsze jest to możliwe. **Wydaje się, że w trzech przypadkach występuje konieczność dokonania regulacji na szczeblu ustawy:**

- **Niezbędna wydaje się modyfikacja aktualnie obowiązującej Ustawy o rachunkowości, mająca na celu dopuszczenie stosowania dowodów księgowych w formie elektronicznej. Dodatkowo należy określić zasady interpretacji technicznej pojęcia „trwały nośnik danych" występującego w tej ustawie.**
- **Niezbędna wydaje się modyfikacja aktów wykonawczych, ograniczających użycie elektronicznej faktury VAT.** Ponieważ nawet w gronie krajów akceptujących elektroniczny format faktury, stosowane rozwiązania są bardzo różnorodne, należy powołać odpowiedni zespół ekspercki, który dokona ich przeglądu i oceny, oraz zaproponuje właściwe dla Polski rozwiązania.
- **Należy w przypadkach koniecznych dopuścić do obrotu na prawach oryginału odpowiednio uwierzytelnioną kopię papierową dokumentów elektronicznych (każdy uwierzytelniony wydruk będzie oryginałem lub będzie istniała możliwość uwierzytelnienia w specjalny sposób tylko jednego wydruku, a wszystkie pozostałe wydruki, odpowiednio autoryzowane będą już kopiami).** Tego typu regulacja jest niezbędna w przypadku, gdy dokument elektroniczny będzie występował także w obiegu zewnętrznym tzn. poza kręgiem podmiotów objętych regulacją sektorową lub umową wymiany.

Inne bariery hamujące rozwój EDI w Polsce i aktualnie prowadzone działania zmierzające do ich usunięcia

Korzyści jakie poszczególny użytkownik uzyska ze stosowania EDI mogą być zbyt małe, jeśli musi on pokonać istotne przeszkody organizacyjne i ponieść związane z tym nakłady.

Z punktu widzenia użytkownika wprowadzenie EDI wymaga:

- określenia struktury i znaczenia poszczególnych elementów komunikatów,
- uzgodnienia zasad wymiany komunikatów drogą teletransmisji,
- wyposażenia uczestników wymiany w odpowiednie oprogramowanie i sprzęt,
- uzgodnienia i stosowania niezbędnych środków ochrony.

Wydaje się, że w optymalnej sytuacji koszty związane z wprowadzeniem EDI powinny być ograniczone do kosztów zakupu oprogramowania i sprzętu realizującego wymianę. Oznacza to, że wszystkie pozostałe elementy powinny być określone w skali ogólnej w sposób kompleksowy.

Właściwe rekomendacje dotyczące struktury i interpretacji elementów komunikatów EDI

Po okresie rozkwitu lokalnych i konkurencyjnych standardów (takich jak np. X.12, SWIFT, ODETTE), w powszechnym przekonaniu nastąpił okres pełnej akceptacji standardu powszechnego w postaci UN/EDIFACT (wspomniano już wcześniej o wprowadzaniu tego standardu w krajach

Unii Europejskiej). Standard ten potwierdził swą przydatność i powoli obejmuje swym zakresem coraz to nowe elementy EDI: ochronę komunikatów, przetwarzanie interakcyjne itp. Jego struktura jest określona normą międzynarodową ISO (ISO 9735, polski odpowiednik to PN-92/T-20091). W Polsce przyszli użytkownicy EDI (zarówno z grona niezależnych podmiotów gospodarczych jak i instytucji państwowych) powinni być stale informowani o istnieniu tego standardu i jego zaletach. Jednocześnie Polska powinna być aktywnie obecna w gronie państw pracujących nad tym standardem w ramach grupy WP.4 ONZ. W tej dziedzinie sytuacja nie tylko nie ulega poprawie, ale wręcz pogarsza się.

Standard EDIFACT jest opracowywany w sposób uniwersalny i w odniesieniu do potrzeb międzynarodowego grona użytkowników. W kontekście poszczególnych zastosowań branżowych, szczególnie dla systemów krajowych konieczna jest adaptacja wzorców ogólnych do specyficznych potrzeb. Ten proces, określany jako definiowanie substandardów komunikatów wzorcowych i podręczników ich użytkowania (MIG - Message Implementation Guidelines) powinien być w Polsce jak najszybciej zakończony. Aktualnie związane z tym prace realizowane są w 3 ośrodkach: EDIPOL i CEDIP opracowały i wdrażają grupę substandardów dla sektora przemysłowego i motoryzacji, Instytut Logistyki i Magazynowania adaptuje dla potrzeb handlu substandardy zalecane przez EANCOM, grupa tematyczna wyłoniona przez Związek Banków Polskich opracowuje substandardy dla potrzeb bankowości, zaś Narodowy Bank Polski przy współpracy z Francusko-Polską Wyższą Szkołą Nowych Technik Informatyczno-Komunikacyjnych (aktualnie przekształconą w Instytut Technik Telekomunikacyjnych i Informatycznych - ITTI) prowadzi zaawansowane prace związane z bankowymi systemami EDI zarządzanymi przez NBP. **Ogólnie jednak prace te przebiegają zbyt wolno i nie są w odpowiedni sposób wspomagane finansowo. Dodatkowo powinno zostać powołane ogólnokrajowe ciało koordynujące, czuwające nad zgodnością tworzonych substandardów (np. na wzór EDIFRANCE we Francji) i ich stosowaniem w nowotworzonych systemach. Rolę taką mogłaby pełnić Rada ds Teleinformatyki lub CEDIP (Centrum EDI - Polska), który aktualnie pełni taką rolę w stosunku do sektora przemysłowego. Jednocześnie, zgodnie ze swym celem statutowym, Rada ds Teleinformatyki powinna oceniać wszelkie inicjatywy ustawodawcze pod kątem ich zgodności z ogólną promocją technologii EDI.**

Operatorzy usług dodanych, ułatwiających wymianę komunikatów drogą teletransmisji

Powszechną w krajach rozwiniętych praktyką jest oferowanie usług dotyczących wymiany komunikatów pomiędzy uczestnikami systemów EDI przez zewnętrznych usługodawców. Są to tzw. usługi dodane (VAN - value added networks), towarzyszące powszechnym lub prywatnym sieciom teletransmisyjnym. Przykładami tego typu sieci są IBM GN (IBM Global Network), GEIS (General Electric Information Services), Amadeus, Allegro i wiele innych (wymienić tu należy również czeską firmę EDITEL CZ). Operatorzy usług dodanych biorą na siebie obsługę klienta (zainstalowanie terminala i modułu wymiany), podłączenie do sieci telekomunikacyjnej, ewentualną konwersję postaci komunikatu, archiwizację komunikatów i oczywiście ich przesłanie do adresata (za pomocą własnej sieci lub poprzez publiczne sieci transmisji danych). W Polsce dwóch operatorów - Bankowe Przedsiębiorstwo Telekomunikacyjne TELBANK i Telekomunikacja Polska S.A. - stworzyło pewne ułatwienia dla wymiany EDI, udostępniając usługę wymiany poczty elektronicznej w standardzie X.400 (a TP S.A. przygotowuje do wdrożenia standard X.435 oraz usługi globalnego katalogu w standarzie X.500). Są to jednak jedynie usługi elementarne, które dla wygody użytkownika powinny być znacznie bardziej rozbudowane.

EDIPOL utworzył też ostatnio ośrodek usług dodanych VANPOL dla potrzeb sektora przemysłowego. **Usługi te rozwinęłyby się znacznie, gdyby organy administracji państwowej i samorządowej wprowadziły systemy EDI dla własnych potrzeb, istotnie poszerzając krąg zainteresowanych tą technologią.**

Instytucje certyfikujące związane z EDI

Dematerializacja dokumentów i wykorzystanie systemów teletransmisji wprowadzają pewne zagrożenia i w interesie użytkowników muszą być one powiązane z wykorzystaniem właściwych środków ochrony. Te środki to ochrona bezpośrednia komunikatów w trakcie transmisji, ochrona ich poufności, ochrona sieci teletransmisyjnych przed awariami itp. Instytucje nadrzędne, których dotyczą wymieniane dokumenty elektroniczne (służby podatkowe, celne, bankowość) również pragną zmniejszyć ryzyko nieautoryzowanych modyfikacji komunikatów w trakcie generacji lub archiwizacji. **Z tego powodu należy powołać odpowiednie organy dla weryfikacji stosowanych systemów EDI jak i rekomendacji określonych środków ochrony.** Organy te mogłyby powstać np. przy współpracy z Stowarzyszeniem Księgowych w Polsce.

W przypadku powszechnego użycia podpisu cyfrowego jako środka autoryzacji dokumentów elektronicznych pojawia się konieczność udostępniania wszystkim zainteresowanym tzw. „kluczy publicznych" użytkowników, za pomocą których można potwierdzić autentyczność podpisu. Najwygodniejszym rozwiązaniem jest udostępnianie tych kluczy drogą teletransmisji, a to wymaga stworzenia odpowiednich centrów dystrybucji (rejestrów kluczy) i przechowywania ich w formie uniemożliwiającej ich modyfikację. Taka forma nosi nazwę certyfikatu klucza publicznego a tworzenie certyfikatów powinno być powierzone odpowiednim, zaufanym organom. W Polsce Telekomunikacja Polska S.A. uruchomiła usługę globalnie dostępnego katalogu w standardzie X.500, która może służyć do przechowywania certyfikatów. **Brak jest jednak powszechnie dostępnych organów certyfikujących (chociaż istnieją one już dla potrzeb zamkniętych grup użytkowników - np. dla systemu ELIXIR KIR S.A.).**

Wyposażenie techniczne

W odniesieniu do sprzętu sytuacja jest w miarę dobra i ulega stałej poprawie. Dostępność sieci telekomunikacyjnych (szczególnie sieci POLPAK po ostatnich modernizacjach, sieci TELBANK) można uznać za zadawalającą. Postęp jaki dokonuje się w zakresie urządzeń teletransmisyjnych wykorzystujących standardową, komutowaną sieć telefoniczną spowodował, że są to już urządzenia stosunkowo tanie i jednocześnie zapewniające wystarczającą dla zastosowań EDI szybkość transmisji. Wydaje się, że za podstawową barierę techniczną można uznać brak polskich modułów EDI, za wyjątkiem zastosowań związanych z elektroniczną bankowością i przemysłem. **Ten brak wynika prawdopodobnie z braku odpowiednio dużego na nie popytu, a to wynika z kolei z braku szerokiego programu promocji EDI i wykorzystania tej techniki w centralnych systemach wymiany danych.**

Wstęp

Informatyka masowa wchodzi w XXI wiek z nowym wyzwaniem - "Użytkownicy wszystkich komputerów - komunikujcie się". Czyje i jakie potrzeby komunikacja ta będzie zaspokajać i kto będzie jej organizatorem ? - oto pytania oczekujące na odpowiedź. Nie ulega wątpliwości, że jedną z takich potrzeb, która może istotnie odmienić funkcjonowanie gospodarki i administracji jest elektroniczna wymiana dokumentów - EDI. Przez dokument rozumie się tu informację w postaci sformalizowanej (co pozwala na jego jednoznaczną interpretację), któremu obie strony wymiany przypisują pewną wagę, niezależnie od konkretnej treści. Jak dotychczas, nasze życie mija wśród dokumentów, a w zasadzie wśród ich pieczołowicie tworzonych i przesyłanych papierowych kopii. Elektroniczne odpowiedniki dokumentów są jednak coraz powszechniej stosowane, stwarzając zupełnie nowe możliwości - i problemy.

1. Zagrożenia wynikające z braku wprowadzania elektronicznej wymiany dokumentów (EDI) w Polsce

Elektroniczna wymiana dokumentów (EDI - Electronic Data Interchange[1]) jest technologią oddziaływającą w istotny sposób na współczesną działalność gospodarczą i administracyjną. Unia Europejska, która w 1993 roku rozpoczęła swój program IDA (Interchange of Data between Administrations), realizuje aktualnie w jego ramach 33 projekty związane z kulturą, służbami celnymi, ochroną środowiska, ochroną zdrowia, zamówieniami publicznymi, ubezpieczeniami społecznymi i sprawozdawczością statystyczną. Obok tych europejskich działań centralnych, poszczególne kraje rozwinięte wprowadzają coraz szerzej udogodnienia stosowania dokumentu elektronicznego.

Opóźnienia we wprowadzaniu elektronicznej wymiany dokumentów w Polsce powodują powstanie następujących zagrożeń:

- utrudnienie procesu integracyjnego Polski z Unią Europejską, wynikające z narastających barier technologicznych i braku możliwości współpracy przy wykorzystaniu środków teleinformatycznych;
- utrudnienie handlu zagranicznego i międzynarodowej współpracy gospodarczej, wynikające z braku zdolności do uczestniczenia w systemach EDI partnerów zagranicznych;
- utrudnienie świadczenia w Polsce nowych usług bezpośrednio związanych z EDI;
- niezdolność do obniżenia kosztów działalności gospodarczej i administracyjnej, poprzez wykorzystanie EDI.

1.1 Utrudnienie procesu integracyjnego - elektroniczna wymiana dokumentów jako powszechnie przyjęta technologia w krajach Unii Europejskiej

Unia Europejska oraz jej kraje członkowskie w szybki sposób tworzą właściwe środowisko techniczne, organizacyjne i prawne dla powszechnego, bardzo szerokiego wprowadzenia EDI.

Program IDA (Interchange of Data between Administrations - Trans-European data communication networks between administrations), rozpoczęty w 1993 roku ma doprowadzić do stworzenia podstaw „społeczeństwa informacyjnego", zdolnego w pełni wykorzystać atuty powstającej globalnej „infostrady". W ramach programu IDA do 1996 roku, wszystkie podstawowe organy administracyjne Unii i krajów członkowskich będą połączone siecią poczty elektronicznej w standardzie X.400. Na bazie tej usługi komunikacyjnej opracowanych jest wiele projektów systemów tematycznych: Europejska Sieć Informacji i Obserwacji (EIONET) Europejskiej Agencji Środowiskowej EEA (European Environment Agency), sieć wymiany informacji o produktach farmaceutycznych Europejskiej Agencji Oceny Leków (EMEA - European Medicine

[1] termin ten ostatnio zastępowany jest przez określenie bardziej ogólne: Electronic Commerce - Elektroniczna gospodarka

Evaluation Agency), sieć wymiany informacji o zatrudnieniu (EURES - European Employment Services), sieć wymiany informacji o ubezpieczeniach socjalnych (TSS/SOSENET - Telematics for Social Security/ Social Security Network), system wymiany informacji o zamówieniach publicznych (SIMAP - Systeme d'information sur les Marches Publics). Szczególne interesujący jest system wymiany informacji statystycznych DSIS (Distributed Statistical Information Services), który ma służyć wszystkim zainteresowanym szybkim dostępem do informacji statystycznej i połączy takie instytucje jak EUROSTAT, urzędy statystyczne krajów członkowskich UE, kraje EFTA, urzędy administracji publicznej i odbiorców informacji statystycznej. System ten w swoich założeniach zakłada wymianę komunikatów EDI w standardzie EDIFACT. Szczególnie rozbudowane są plany dotyczące systemów celnych - realizuje się tu między innymi projekty: QUOTA (kwotowe ograniczenia importowe wobec krajów nie-członkowskich UE), TRAIC, EBTI (jednolita taryfowa polityka celna), TRANSIT (automatyzacja obsługi celnej), SCENT/CIS (system wymiany danych celnych i podatkowych), VIES (system wymiany danych o podatkach VAT) i wiele innych.

Jednym z bardziej zaawansowanych projektów jest EDIBOP, którego celem jest zbieranie danych statystycznych o bilansach płatniczych w handlu zagranicznym.

Grupa ds. komunikatów statystycznych MD6 opracowała w standardzie EDIFACT dla potrzeb tego systemu specjalną grupę komunikatów:

- BOPCUS - deklaracja rozliczeń zagranicznych zrealizowanych przez klientów dokonywana przez bank;
- BOPBNK - deklaracja rozliczeń zagranicznych zrealizowanych w imieniu własnym przez bank;
- BOPDIR - deklaracja rozliczeń własnych dokonywana przez przedsiębiorstwo;
- BOPINF - informacja przesyłana dla banku z chwilą uzyskania informacji przez klienta o należnościach do uzyskania w rozliczeniach z partnerem zagranicznym;
- BOPSTA/BOPMES - informacje zbiorcze przekazywane przez bank centralny organizacjom międzynarodowym lub innym bankom centralnym.

EUROSTAT, instytucja odpowiedzialna w Unii Europejskiej za zbieranie i przetwarzanie danych statystycznych, jest głównym koordynatorem tych prac.

Program EDIBOP we Francji

Bank Francji wprowadził komunikaty EDIBOP w swoim systemie EDI. Komunikat BOPDIR jest wykorzystywany od 1 marca 1995. Grupa robocza złożona z przedstawicieli dużych przedsiębiorstw opracowała w związku z tym podręcznik stosowania (MIG - Message Implementation Guide) tego komunikatu. Przekaz następuje przy wykorzystaniu usług poczty elektronicznej ATLAS 400, a stosowanie ochrony jest opcjonalne. Oparta jest ona o moduł SecurBDF Banku Francji, zapewniający usługi integralności i poufności.

Bank Francji wraz z pozostałymi bankami francuskimi (zrzeszonymi w grupie EDIFINANCE EDI-FRANCE i CFONB) opracowały podręczniki stosowania dla komunikatów BOPCUS i BOPBNK. Ich stosowanie mało rozpocząć się we wrześniu/październiku 1995 roku.

Komunikat BOPSTA został już przetestowany w wymianie z instytucjami międzynarodowymi. Powinien on był wejść do użytku od 1995 dla wymiany danych z EUROSTAT, Europejskim Instytutem Monetarnym i innymi.

Wszystko to sprawia, że w ramach Unii Europejskiej elektroniczna forma wymiany dokumentów staje się nieodwołalnie jednym ze standardowych, powszechnie stosowanych rozwiązań. Oznacza to, że również Polska będzie musiała przystosować się do tych wymagań w ramach swego procesu integracyjnego. Im wcześniej to nastąpi, tym koszty tej transformacji będą mniejsze. Jednocześnie tym szybciej pojawią się korzyści uczestnictwa w ogólnych europejskich systemach wymiany informacji.

1.2 Utrudnienia w handlu zagranicznym - elektroniczny dokument jako powszechnie wprowadzana technologia w wewnątrzkrajowej wymianie danych w Europie Zachodniej

W raporcie europejskiego programu TEDIS, za najbardziej ważne w zastosowaniach EDI uznane zostały następujące dokumenty:

- dokumenty przewozowe,
- faktury,
- dokumenty celne,
- kontrakty ubezpieczeniowe,
- weksle,
- dokumenty związane z działaniem podmiotów gospodarczych,
- dokumenty procesowe (np. pozwy).

W wielu krajach dla znacznej ich części akceptuje się użycie formy elektronicznej. Dla przykładu, sytuacja w odniesieniu do elektronicznej postaci faktury przedstawia się w Europie następująco:

- **Polska** - nie dopuszcza elektronicznej formy faktury
- **Włochy** - dopuszczenie faktury elektronicznej w 1990 r.
- **Francja** - dopuszczenie faktury elektronicznej w 1991 r.
- **Belgia** - dopuszczenie faktury elektronicznej w 1994 r.

Bardzo radykalną reformę wprowadziła w tej dziedzinie Francja. Ustawa z dn. 11.02.1994 (Loi no 94-126) wprowadziła obowiązek akceptacji elektronicznej formy dokumentów wymienianych z podmiotami gospodarczymi przez wszystkie organy administracji państwowej. W ślad za tą regulacją prawną stworzono odpowiedni standard telekomunikacyjny - normę TEDECO a operator telekomunikacyjny France Telecom uruchomił odpowiednią usługę transferu danych (Service TEDECO). Wszystkie bardziej znaczące instytucje państwowe były już w 1994 r. połączone systemem TEDECO: Skarb Państwa, Ministerstwo Finansów, Ministerstwo Ubezpieczeń Socjalnych, Ministerstwo Pracy, Ministerstwo Edukacji, Dyrekcja Generalna ds. Podatków, Dyrekcja Generalna ds. Cła, Księgowość Publiczna i wiele innych. W rok po uruchomieniu system był wykorzystywany przez 1000 użytkowników. Jednocześnie we Francji w wielu sektorach wykorzystywane są specyficzne systemy EDI, dotyczące np. wymiany danych pomiędzy

bankami i ich klientami (francuska seria standardów bankowych ETEBAC 1,2,3,4 i 5) czy obsługi sektora handlu - system ALLEGRO (ok. 2000 użytkowników w końcu 1995 roku).

Te przemiany są dowodem na to, że w praktyce gospodarczej Europy Zachodniej wykorzystanie formy elektronicznej dokumentów staje się coraz bardziej powszechne, szczególnie wśród dużych podmiotów gospodarczych. Przyjęcie takiej formy wymiany danych powoduje, że firmy te wybierają swoich kooperantów również wśród użytkowników EDI. Ogranicza to w istotny sposób konkurencyjność polskich firm na tych rynkach.

1.3 Brak możliwości do świadczenia w Polsce usług bezpośrednio związanych z EDI

Wiele współczesnych zaawansowanych usług staje się możliwych jedynie przy wykorzystaniu środków telekomunikacyjnych. Jednym z najbardziej spektakularnych przykładów jest tu elektroniczna bankowość dzięki której możliwa jest zdalna współpraca między klientem a bankiem. W Polsce popularność elektronicznej bankowości bardzo szybko rośnie. Według dziennika Rzeczpospolita, w końcu 1995 roku już 23 banki oferowały tę usługę, stosując do jej realizacji ok. 16 różnych produktów informatycznych. Ten dynamiczny rozwój potwierdza, że techniki teleinformatyczne są skuteczne i efektywne również w naszym kraju. W wypadku elektronicznej bankowości wynika to z następujących faktów:

- większość instytucji gospodarczych posiada już dobrze rozwinięte systemy komputerowe i fachową kadrę informatyczną,
- instytucje usługowe (w tym wypadku banki), napotykają na trudności w oferowaniu rozbudowanej i powszechnie dostępnej sieci agencji, umożliwiających bezpośredni kontakt z klientami,
- duża liczba bezpośrednio obsługiwanych klientów w powiązaniu z ograniczeniami lokalowymi prowadzi do znacznych utrudnień w oferowaniu szybkiej i sprawnej ich obsługi,
- usługi pocztowe w Polsce wprowadzają znaczne opóźnienia w wymianie dokumentów, towarzyszącej tradycyjnej, zdalnej, współpracy klienta z usługodawcą (bankiem).

Brak właściwego środowiska dla rozwoju EDI powoduje jednak, że aplikacje elektronicznej bankowości realizowane są przez każdy bank indywidualnie, bez wykorzystania rozwiązań standardowych - zarówno w odniesieniu do postaci komunikatów, jak i środków ochrony oraz usług komunikacyjnych. Skutki tego braku standaryzacji są powszechnie odczuwalne: klienci korzystający z usług kilku banków muszą posiadać oddzielny system dla każdego banku, banki ponoszą dodatkowe koszty wynikające z opracowywania rozwiązań indywidualnych, realne jest ryzyko, że w przypadku zbyt słabego systemu ochrony w jednym systemie i udanych fałszerstw z tym związanych, klienci utracą zaufanie również do innych systemów.

Realizacja pewnych form działalności gospodarczej jest bardzo trudna lub w ogóle nie możliwa bez wykorzystywania EDI. Jest tak np. dla cyklu produkcyjnego JIT (Just In Time), czy planowania zaopatrzenia MRP (Material Requirement Planning). Przy tym sposobie organizacji wytwarzania, producent finalny wymaga od swych kooperantów bardzo dużej sprawności działania, terminowości i poprawności dostaw - co bez EDI jest bardzo trudne do spełnienia. W

Polsce wymagania takie występują na razie przede wszystkim w przemyśle motoryzacyjnym, ale produkcja w trybie JIT wykazała swą przydatność w wielu innych branżach.

Niedostateczna promocja EDI jest również jednym z powodów braku w Polsce usług wykorzystujących ogólnodostępne, centralne rejestry danych, np.: rejestr czeków i rachunków zastrzeżonych, skradzionych dowodów tożsamości, pojazdów itp. Nie trzeba nikogo przekonywać, że systemy te są niezwykle użyteczne i stosunkowo proste w realizacji[2].

Wysoki koszt działalności gospodarczej i administracyjnej

Rozwój elektronicznej wymiany danych w świecie, zarówno w odniesieniu do działalności gospodarczej jak i administracyjnej, wynika z bardzo istotnych korzyści ekonomicznych. Wiele niezależnie prowadzonych badań wykazuje, że w wypadku dokumentu elektronicznego można uzyskać ok. 25 % redukcję kosztów administracyjnych i kosztów przechowywania i odszukiwania dokumentów archiwizowanych. Takie oszczędności występują przy spełnieniu następujących warunków:

- liczba dokumentów jest duża, a ich przetwarzanie daje się łatwo zautomatyzować,

- usługi telekomunikacyjne są tanie i powszechnie dostępne,

- obie strony wymiany wyposażone są w sprzęt informatyczny.

W Polsce, podobnie jak w innych krajach Europy, warunki takie już zachodzą i nasz system gospodarczy ponosi straty wynikające z zaniechania stosowania EDI. Dotyczy to przede wszystkim obiegu wszelkiego rodzaju dokumentów masowo wymienianych pomiędzy podmiotami gospodarczymi, oraz pomiędzy tymi podmiotami a organami Państwa. Są to wszelkiego rodzaju deklaracje statystyczne, celne, podatkowe, dotyczące ubezpieczeń społecznych itp. Bardzo istotną grupą tego typu dokumentów jest sprawozdawczość w ramach państwowej służby zdrowia.

Inną niedogodnością wynikającą z braku EDI jest wydłużenie czasu przetwarzania wymienianych dokumentów, co ogólnie zwalnia tempo życia gospodarczego kraju. Dotyczy to przede wszystkim obiegu dokumentów płatniczych, ale również, choć w mniejszym stopniu ofert, dokumentów przewozowych, faktur, zamówień itp.

Wydaje się, że poważne straty w Polsce ponoszone są z powodu stosowania rozwiązań zastępczych w miejsce centralnych rejestrów danych (wraz z elektroniczną formą ich aktualizacji i obsługi zapytań). W wielu wypadkach powiadomienie poszczególnych urzędów pocztowych lub oddziałów banków o kradzieży czeku jest tak kosztowne, że poszkodowany woli narazić się na straty wynikające z realizacji skradzionego czeku. Jednocześnie stale pojawiają się lokalne inicjatywy tworzenia rejestrów dotyczących ewidencji pojazdów, zastrzeżeń czeków czy dokumentów identyfikacyjnych.

Niestety brak jest jeszcze szerokiej oferty polskich produktów EDI. W wielu wypadkach przy wprowadzaniu usług EDI konieczne jest więc wykorzystanie stosunkowo kosztownych produktów zagranicznych. Sytuacja ta wystąpiła w odniesieniu do elektronicznej bankowości czy EDI w motoryzacji, gdzie znaczna część użytkowników EDI zdecydowała się na zakup oprogramowania

[2] „Złapani za numer" Polityka, nr 37 z 14.09.96 - opis centralnej bazy dokumentów skradzionych zrealizowanych w Holandii

zagranicznego. Oczywiście, w początkowym okresie sytuacja taka jest naturalna i wynika z nowatorskiego charakteru produktu. Jednak zbyt duże opóźnienie w opracowaniu polskiej oferty produktów EDI jest gospodarczo bardzo niekorzystne. Jak się wydaje, wynika to z braku skutecznego propagowania tej tematyki i braku zachęty dla inwestycji w tej dziedzinie, np. poprzez zamówienia ze strony administracji publicznej.

2. Podstawowe bariery we wprowadzaniu EDI w Polsce

Bariery towarzyszące wprowadzaniu EDI można podzielić na 4 grupy:

- prawne - ogólne
- prawne - szczegółowe (dotyczące poszczególnych typów dokumentów)
- organizacyjne
- techniczne

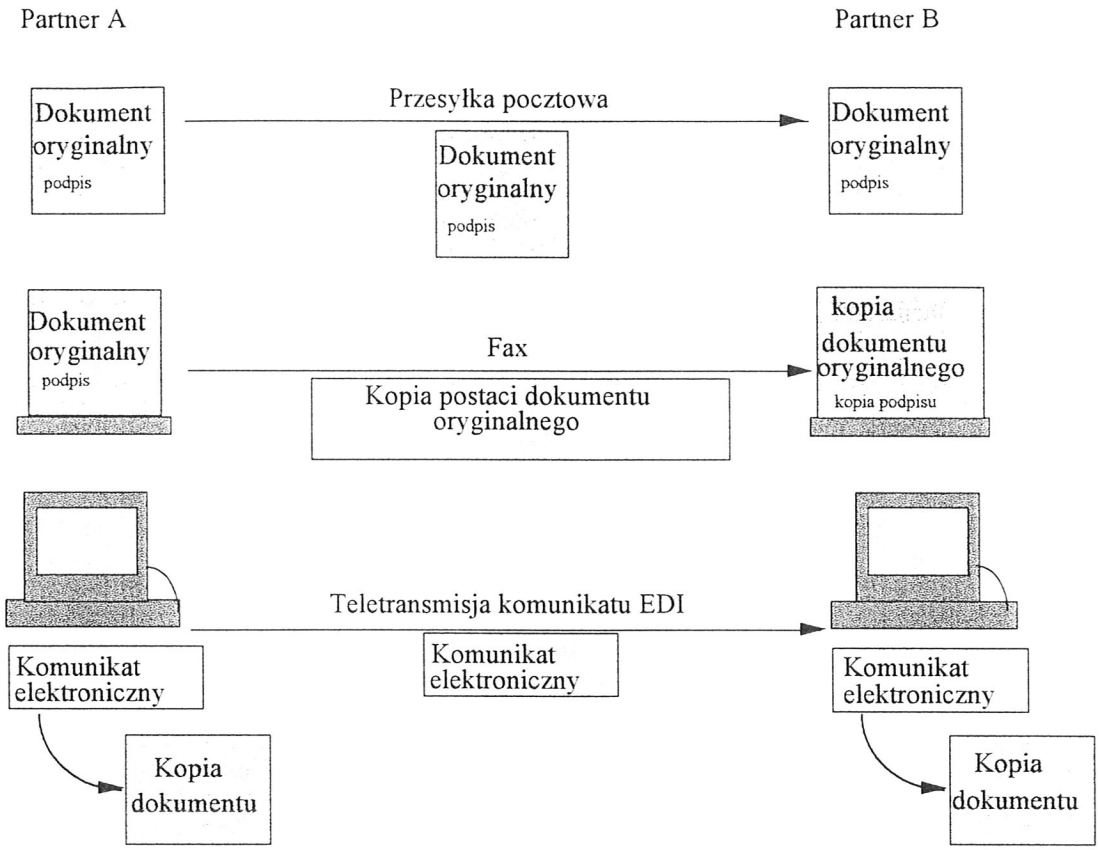
Zostaną one tu kolejno omówione.

2.1 Bariery prawne

Elektroniczna wymiana danych wprowadza do istniejącej praktyki dwa nowe zjawiska:

- zanik tradycyjnej, papierowej formy dokumentu (jako oryginału i ewentualnie kopii) i zastępowanie go zapisem elektronicznym (cyfrowym), którego wszystkie kopie są technicznie nierozróżnialne;
- wymianę tak utworzonych zapisów (komunikatów) drogą telekomunikacyjną, pomiędzy zainteresowanymi stronami.

Chociaż w nazwie EDI eksponuje się fakt wymiany, to jednak podstawowe problemy prawne dotyczą braku tradycyjnego oryginału dokumentu. Na rysunku 1. przedstawiono to obrazowo. Nie jest istotne tutaj w jaki sposób odbywa się wymiana, chociaż oczywiście implikuje ona formę dokumentu. Żaden przepis prawa nie określa, że przesyłanie dokumentu odbywać się powinno przy pomocy kuriera, faksu czy przy zastosowaniu urządzeń elektronicznych.. Tak więc w tym zakresie prawo nie stawia żadnych ograniczeń. Problem, jaki pojawia się w związku z przesyłaniem dokumentów w formie elektronicznej sprowadza się do wartości prawnej uzyskanej u odbiorcy kopii (zawierającej kopię treści dokumentu i ewentualnie kopię podpisu w wypadku faksu, lub elektroniczną kopię nadanego komunikatu w wypadku EDI). Tak więc w dalszej części rozważań główny nacisk położony został na sam problem występowania dokumentu w formie elektronicznej i problem kopii utworzonych na podstawie zapisów elektronicznych.



Rys. 1. Zanikanie oryginału i dokumentu podczas przesyłania go różnymi technikami wymiany informacji

Różne mogą być skutki niewłaściwej formy dokumentu. W praktyce prawnej, dokumenty bądź potwierdzają istniejący stan faktyczny, bądź też zawierają oświadczenia woli stron, czyli obejmują swoją treścią dokonanie czynności prawnej. W tym zakresie przepisy nie pozostawiają stronom zupełnej dowolności, albowiem przewidują dla dokonania niektórych rodzajów czynności prawnych konieczność dochowania formy pisemnej. Czasami są to normy bezwzględnie obowiązujące (jak np. wymóg pisemnego sporządzenia umowy kredytowej), przeważnie jednak są to normy względnie obowiązujące, tzn. strony mogą niedochować tej formy dla danej czynności.

Różne są jednak konsekwencje takiego zachowania. Z interesującego nas punktu widzenia będzie tutaj chodziło o wymianę dokumentów, potwierdzających czynności przysparzające i obciążające. W Polsce, w przypadku czynności gdzie transfer dóbr przekracza 2 000 zł forma pisemna jest zastrzeżona dla celów dowodowych (ad probationem). Oznacza to, że niedochowanie tej formy nie powoduje nieważności dokonanej transakcji, lecz taki skutek, że w razie sporu niedopuszczalny jest w zasadzie dowód ze świadków lub z przesłuchania stron dla wykazania, że czynność prawna została dokonana (chyba, że strony wyrażą na to zgodę, co w świetle istniejącego pomiędzy nimi sporu jest mało prawdopodobne, lub dokonanie czynności zostanie uprawdopodobnione w innym dokumencie, bądź też sąd uzna to za konieczne ze względu na szczególne okoliczności sprawy).

Przeszkody prawne związane z zastępowaniem dokumentów tradycyjnych dokumentami EDI mogą więc mieć dwojaką postać:

- jeśli wymóg istnienia dokumentu tradycyjnego ma charakter normy bezwzględnie obowiązującej (w stosunku do ewentualnych użytkowników EDI), to mówimy o zakazie stosowania EDI;
- jeśli wymóg istnienia dokumentu tradycyjnego jest normą względnie obowiązującą, tzn. strony mogą od tego wymogu odstąpić akceptując negatywne tego skutki (najczęściej oznacza to brak mocy dowodowej dokumentu w formie elektronicznej utworzonego w zastępstwie dokumentu tradycyjnego), to mówimy o utrudnieniach w stosowaniu EDI.

Problemy te są powszechne i na wstępie zostaną omówione w odniesieniu do sytuacji panującej w rozwiniętych krajach europejskich i Stanach Zjednoczonych.

2.2 Ogólne występujące bariery prawne dotyczące EDI

Elektroniczna wymiana dokumentów jest już praktycznie wykorzystywana w świecie od kilkunastu lat. Jest to okres wystarczający aby zebrać doświadczenia i dokonać pewnych podsumowań. Pod tym względem, najbardziej owocnym był europejski program TEDIS (Trade Electronic Data Interchange Systems), finansowany ze środków Unii Europejskiej i rozpoczęty w 1987 roku. W trakcie realizacji fazy II tego programu przeprowadzono kompleksową analizę dotyczącą aspektów prawnych EDI w krajach członkowskich Unii Europejskiej oraz w krajach EFTA (łącznie objęła ona 19 krajów europejskich), zakończoną w 1993 roku[3].

Pomimo istniejącego ogólnego założenia maksymalnej liberalizacji zasad prowadzenia działalności gospodarczej, ustawodawcy większości krajów ograniczają pełną swobodę kształtowania form wzajemnych stosunków stron z następujących przyczyn:

a) w celu ułatwienia rozstrzygania ewentualnych sporów obowiązuje wymóg istnienia wiarygodnych dowodów woli stron i zaistniałych faktów;

b) w celu ochrony stron przed nieuświadomionymi konsekwencjami swych czynów, obowiązuje wymóg czytelnej i jasnej formy wyrażania przyjętych przez strony zobowiązań.

Działając z pobudek (a) wprowadzono wymóg istnienia trwałych i czytelnych dowodów, autoryzowanych własnoręcznym podpisem autora lub osoby przyjmującej odpowiedzialność za treść dowodu. Ten wymóg, mało uciążliwy w okresie dokumentów papierowych, stoi w sprzeczności z elektroniczną formą przesyłania i przechowywania komunikatów (dokumentów) EDI, oraz stawia pod dużym znakiem zapytania wartość dowodową komunikatów EDI w wypadku sporu odbiorcy z nadawcą.

W wyniku regulacji utworzonych z powodu (b) wprowadzono wymóg formy pisemnej umowy i jej podpisania przez wszystkie strony związane postanowieniami umowy. Te wymagania uniemożliwiają procedurę zawierania umów na drodze wymiany komunikatów EDI, a więc w sposób najbardziej efektywny i naturalny dla podmiotów pragnących posługiwać się tą formą wymiany informacji.

---

[3] TEDIS PHASE II: Report on Authentication, Storage and Use of Codes in EDI Messages, vol. I, II, III

W świetle wyników analizy przeprowadzonej w ramach TEDIS II, najbardziej istotne dla EDI przeszkody prawne w większości krajów europejskich, dotyczą następujących aspektów:

- stosowania komunikatów EDI jako elektronicznych odpowiedników dokumentów tradycyjnych,
- przechowywania komunikatów EDI i problemów braku fizycznie rozróżnialnego oryginału,
- użycia kodów i szyfrowania w komunikatach EDI.

Te zagadnienia zostaną dalej kolejno omówione. Na zakończenie zaś przedstawiono zagadnienia związane z samą wymianą komunikatów pomiędzy uczestnikami. Należy tu zaznaczyć, że używany w kontekście tego opracowania termin "komunikat EDI" ma w zasadzie znaczenie bardziej uniwersalne i może być traktowany jako równoważny do pojęcia "dokumentu elektronicznego".

Użycie komunikatów EDI jako dokumentów.

Problem prawne dotyczące komunikatów EDI pojawiają się wtedy, gdy tą drogą przesyłane są dokumenty, których forma (najczęściej z powodów (a) lub (b) opisanych w poprzednim punkcie) jest prawnie określona. W raporcie TEDIS, za najbardziej istotne dla EDI uznane zostały następujące, prawnie określone, dokumenty :

- dokumenty przewozowe,
- faktury,
- dokumenty celne,
- kontrakty ubezpieczeniowe,
- weksle,
- dokumenty związane z działaniem podmiotów gospodarczych,
- dokumenty procesowe (np. pozwy).

W ustawodawstwach analizowanych krajów wymagana jest w ich przypadku autoryzacja (czyli zagwarantowanie integralności ich zawartości oraz identyfikacja autora uniemożliwiająca jednocześnie wyparcie się przez niego tego faktu). Środki służące do tego celu w dotychczasowej praktyce to:

- odręczny podpis na dokumencie,
- odręczny podpis uwierzytelniony przez świadka, najczęściej notariusza,
- złożenie oryginału w depozyt u wiarygodnej osoby trzeciej (najczęściej notariusza).

Dodatkowe uwierzytelnienie przez wiarygodną osobę trzecią często służy dodatkowym celom: wskazania czasu utworzenia dokumentu i rejestracji tego dokumentu, w celu zapewnienia istnienia odpowiednio chronionego oryginału.

We wszystkich analizowanych krajach wymagany prawem podpis miał na celu:

- osobistą identyfikację dokonaną przez autora dokumentu, posiadającą cechę niezaprzeczalności,
- wyrażenie akceptacji podpisującego co do treści dokumentu i wynikających stąd skutków,
- uświadomienie podpisującemu momentu (będącego chwilą złożenia podpisu) od którego dokument wywiera skutki prawne,
- nadanie dokumentom cech, zmniejszając obawy osób trzecich co do jego prawdziwości,

- potwierdzenie kompletności dokumentu i zabezpieczenie przed modyfikacjami.

Aby osiągnąć te cele w dotychczas istniejących warunkach technicznych, powszechnym jest wymaganie w stosowanych regulacjach prawnych, aby dokument był autoryzowany własnoręcznym podpisem, co pośrednio implikuje użycie do jego zapisu nośnika trwałego, na którym podpis może być złożony. Komunikaty EDI w formie elektronicznej nie spełniają takich wymagań.

Rozwiązania problemów prawnych dotyczących autoryzacji komunikatów EDI spotykane w praktyce

W większości krajów Europy, ustawodawca określa własnoręczny podpis jako niezbędny element autoryzujący dokument (a to z kolei wyklucza formę elektroniczną dokumentu). Od tej zasady autoryzacji pojawiają się coraz liczniejsze wyjątki. I tak przykładowo:

- kraje akceptujące jedynie podpis odręczny:

  - **Francja**
    akceptuje jedynie podpis odręczny (z wykluczeniem np. krzyżyka);
  - **Niemcy**
    dokument musi być sporządzony na papierze, z podpisem odręcznym stron;
  - **Szwecja**
    wymaga podpisu odręcznego.

- kraje, które w wyjątkowych przypadkach dopuszczają inne formy podpisu:

  - **Norwegia**
    dopuszcza enumeratywnie użycie podpisu cyfrowego w wybranych przypadkach (bankowość, emisja akcji, transport międzynarodowy i dokumenty celne);
  - **Portugalia**
    wymaga podpisu odręcznego, za wyjątkiem dokumentów celnych;

- kraje, które ogólnie nie wymagają odręczności podpisu:

  - **Dania, Holandia, Włochy, Irlandia, Norwegia**
    nie wymagają odręczności podpisu;
  - **Stany Zjednoczone**
    Jednolity Kodeks Handlowy (UCC), będący stanowym aktem prawnym w Stanach Zjednoczonych, definiuje "podpis" jako "dowolny symbol utworzony lub zastosowany przez stronę z istniejącą intencją do uwierzytelnienia treści". Najdalej idącą regulacją wydaje się ustawa o podpisie cyfrowym (Title 46, Chapter 3 (1996)) stanu Utah, która zaczęła obowiązywać od marca 1996 roku, stanowiąca o równoważności podpisu cyfrowego i podpisu odręcznego na papierze we wszystkich przypadkach przewidzianych prawem.

Użytkownicy stosujący technikę EDI, a więc tworzący dokumenty w formie elektronicznej w krajach bez odpowiednich dla EDI regulacji prawnych, wybierają w praktyce jedną z trzech strategii działania:

a) uznają, że przesyłane komunikaty EDI nie będą miały wartości dowodowej, a w wypadku sporu sądowego będzie on rozstrzygany bez ich wykorzystania jako dowodu w sprawie;

b) postanawiają na drodze umowy, że komunikaty EDI mają dla nich tę samą moc dowodową jak odpowiednie dokumenty, które zastępują,

c) stosują podwójny obieg dokumentów, tworząc dokumenty tradycyjne obok komunikatów EDI.

Oceniając przedstawione powyżej strategie należy stwierdzić, że jeśli grono użytkowników EDI jest małe (np. jest to para uczestników) i obdarzają się oni dużym zaufaniem to pierwsza strategia jest najprostszą i najczęściej stosowaną. Dowodem jest np. fakt, że w 1995 roku 85 % podmiotów wykorzystujących EDI w Belgii nie zawarło w tym celu żadnej specjalnej umowy. Strategia ta jest niedopuszczalna, jeśli uczestnicy wymiany nie mają wobec siebie aż tak dużego zaufania lub brak właściwej formy wymienianych dokumentów pociąga za sobą określone konsekwencje karne lub inne negatywne konsekwencje finansowe (np. w wypadku komunikatów EDI zastępujących fakturę lub dokumenty celne).

Druga strategia jest użyteczna, jeśli grono użytkowników EDI jest zamknięte i wymóg zawarcia odrębnej umowy (na piśmie, potwierdzonej własnoręcznym podpisem) nie jest istotnym utrudnieniem, a czasami jest wręcz pożądany. Umowa o wymianie EDI może być tworzona przez uczestników na podstawie istniejących wzorców (które są jednak najczęściej przeznaczone dla systemów EDI w zastosowaniach handlowych) lub z uwzględnieniem indywidualnej specyfiki systemu. Strategia ta zawodzi jednak, jeśli techniką EDI mają być przesyłane dokumenty, których zakres użycia wykracza poza krąg uczestników związanych umową EDI. Jednym z praktycznie użytecznych środków zaradczych, może być próba rozszerzenia umowy na wszystkich zainteresowanych. Najczęściej tymi dodatkowymi partnerami są organy administracji państwowej (służby celne, służby podatkowe itp.). Klasycznym przykładem już tu wspominanym jest Francja, gdzie ustawowo zobowiązuje się organa administracji do akceptacji dokumentów w formie elektronicznej na warunkach ustalonych w umowie.

Strategia trzecia jest potencjalnie najbardziej uniwersalna, ale pozbawia użytkowników części korzyści wynikających z technologii EDI, a korzyści ekonomiczne są najczęściej głównym motywem ich działania.

Obok wymienionych powyżej strategii przystosowania się do istniejących warunków, zarówno na poziomie poszczególnych krajów, jak i Unii Europejskiej, trwają prace nad taką modyfikacją istniejącego prawodawstwa które, nie rezygnując z zalet autoryzacji omówionych w punkcie 1.1.1, umożliwiło by ogólne wykorzystanie techniki EDI. Inicjatywy te w pierwszym rzędzie zmierzają do zniesienia nakazów uniemożliwiających wykorzystanie komunikatów EDI jako dokumentów prawnie wymaganych, a następnie mają na celu nadanie komunikatom EDI wartości dowodowej. Polega to na określeniu w jakich warunkach technicznych dokumenty elektroniczne spełniają określone wymagania formalne, lub też na postulowaniu ogólnego zniesienia tych wymagań (jeśli nie niesie to negatywnych skutków).

Jako środki równoważne (lub w komercyjnie właściwy sposób zastępujące) dokumenty z podpisem odręcznym proponuje się (propozycje uporządkowano od najbardziej ograniczonych do najdalej idących):

a) wprowadzenie legalizacji oprogramowania służącego do tworzenia, przesyłania i odbioru w formie elektronicznej wybranych dokumentów (najczęściej faktury), rejestracji

użytkowników tej techniki i nałożenie wymogu tworzenia streszczeń na papierze, najczęściej autoryzowanych podpisem tradycyjnym;

b) tworzenie i przesyłanie wybranych dokumentów w formie elektronicznej "z zachowaniem komercyjnie uzasadnionych środków ochrony" (artykuł 4A Jednolitego Kodeksu Handlowego Stanów Zjednoczonych UCC4A), lub na zasadach kształtowanych odrębną umową (Francja);

c) wykorzystanie Zaufanej Trzeciej Strony (TTP - Trusted Third Party), jako wiarygodnego organu rozstrzygającego spory na podstawie przechowywanych kopii wszystkich wymienianych komunikatów (propozycje zawarte we wnioskach realizatorów programu TEDIS II);

d) podpis cyfrowy, jako uniwersalną technikę równoważną we wszystkich przypadkach podpisowi odręcznemu (patrz załącznik 1. - ustawa stanu Utah).

Przykładami rozwiązań typu (a) są obowiązujące w znacznej liczbie krajów europejskich zasady przesyłania faktury w formie elektronicznej.

Możemy tu zaobserwować następujące przypadki:

- **Polska** - nie dopuszcza elektronicznej formy faktury:
  - faktura musi mieć postać papierową (prawo podatkowe);
  - wszystkie dowody księgowe otrzymane drogą teletransmisji muszą uzyskać postać trwale czytelną (ustawa o księgowości);
- **Włochy** - dopuszczenie faktury elektronicznej w 1990[4] r.:
  - faktura u nadawcy powinna mieć postać papierową[5];
  - faktura o odbiorcy może mieć postać elektroniczną;
  - u odbiorcy tworzony jest rejestr zbiorczy otrzymanych faktur w sposób czytelny na nośniku trwałym.
- **Francja** - dopuszczenie faktury elektronicznej w 1991 r.[6]:
  - użytkownicy EDI muszą uzyskać certyfikat autoryzacyjny dla swych systemów informatycznych;
  - faktura u nadawcy i u odbiorcy może mieć postać elektroniczną;
  - nadawca i odbiorca tworzy rejestr streszczeń nadanych i odebranych faktur w sposób czytelny na nośniku trwałym;
  - na żądanie istniejące dane muszą być wystarczające do odtworzenia faktury w sposób czytelny.
- **Belgia** - dopuszczenie faktury elektronicznej w 1994 r.[7]:
  - użytkownicy EDI muszą zgłosić fakt wykorzystywania elektronicznej postaci faktury;
  - użytkownicy powinni posiadać i przechowywać pełną dokumentację używanego systemu informatycznego;
  - nadawca i odbiorca tworzy rejestr streszczeń nadanych i odebranych faktur w sposób czytelny na nośniku trwałym;

---

[4] patrz załącznik 4 niniejszego raportu

[5] w 1995 Włochy zniosły wymóg tworzenia kopii papierowej u nadawcy. Z ogólnych doniesień wynika, że przez cały dotychczasowy okres dopuszczenia faktur w postaci elektronicznej nie zanotowano żadnego przypadku z tym związanego, rozstrzyganego sądownie, incydentu.

[6] patrz załącznik 4 niniejszego raportu

[7] patrz załącznik 4 niniejszego raportu

- nadawca i odbiorca podaje w deklaracji liczbę otrzymanych i nadanych faktur w rozbiciu na kontrahentów.

Rozwiązanie typu (b) jest o tyle interesujące, że przykład UCC4A dotyczy wymagań dla systemu transferu środków pieniężnych (EFT), a więc jest jednym z rozwiązań sprawdzonych praktycznie w bankowych systemach EDI o dużych wymaganiach co do ochrony. Na bazie tej regulacji działają w USA największe systemy elektronicznych rozliczeń pieniężnych - FedWire (system rozliczeń Banku Rezerw Federalnych) i CHIPS (Nowojorska Izba Rozliczeniowa).

Przede wszystkim UCC4A podważa procedurę weryfikacji jedynie ręcznego podpisu z wzorcem jako "wystarczającej" procedury ochrony zapewniającej wiarygodność zlecenia, a nawet w oficjalnym komentarzu odrzuca technikę weryfikację podpisu odręcznego jako jedynej zasady weryfikacji autentyczności dokumentu. W to miejsce wprowadza dwie możliwości:

- zlecenie płatnicze uznaje się za uwierzytelnione względem zleceniodawcy, jeśli nastąpi to na zasadach prawnych definiujących pełnomocnictwo (technika tradycyjna),
- uwierzytelnienie nastąpi w dobrej wierze na drodze komercyjnie uzasadnionej procedury ochrony (technika proponowana dla zleceń w formie elektronicznej).

Procedura ochrony w ustaleniach UCC 4A jest określana umową pomiędzy bankiem i klientem i służy:

- do weryfikacji czy zlecenie płatnicze, korekta zlecenia lub odwołanie zlecenia jest zgodne z wolą klienta,
- do detekcji błędów w trakcie transmisji, występujących w treści zlecenia płatniczego lub wiadomości.

Ustawa stara się określić warunki uznania danej procedury ochrony za "komercyjnie uzasadnioną", tak aby w jak największym stopniu wspomóc postępowanie sądowe. Ocena czy dane środki ochrony można uznać jako "komercyjne uzasadnione" , powinna być przeprowadzana na podstawie :

- woli klienta przekazanej bankowi (co do pożądanych przez niego środków ochrony),
- zwyczajów klienta znanych bankowi (takich jak wielkość, typ i częstotliwość zleceń płatniczych normalnie składanych przez klienta),
- alternatywnych środków ochrony oferowanych klientowi przez bank,
- środków ochrony stosowanych ogólnie przez podobnych klientów i banki.

Z definicji, za środki "komercyjnie uzasadnione" uznaje się również te, które zostały wybrane na drodze następującego postępowania:

- bank oferuje klientowi proponowane przez siebie środki ochrony,
- klient rezygnuje z tej oferty na korzyść innej, wybranej przez siebie, jednocześnie wyrażając zgodę na piśmie na obciążanie go skutkami sfałszowanych zleceń, uwierzytelnionych przez procedurę którą proponuje. W tym wypadku, UCC 4A nie wymaga stosowania "komercyjnie uzasadnionych środków ochrony", stawiając wyżej wolność klienta od "rozsądku prawodawców".

Występująca w wariancie (c) Zaufana Trzecia Strona (TTP), proponowana jako alternatywa do podpisu cyfrowego przez autorów raportu programu TEDIS II, jest instytucją świadczącą następujące usługi:

- rejestruje uczestników wymiany EDI;
- otrzymuje od nadawców i rozsyła odbiorcom komunikaty EDI, opatrując je ewentualnie wiarygodnym datownikiem;

- zachowuje kopie komunikatów i wydaje poświadczenia ich istnieniu, zawartości, nadawcach i adresatach;

Należy tu również wspomnieć, że Komisja Europejska w ramach programu TEDIS sfinansowała również projekt EDIRA, mający na celu określenie międzynarodowych zasad współpracy pomiędzy TTP.

Podpis cyfrowy występujący w wariancie (d), ma szanse stać się ogólnie uznanym równoważnikiem podpisu odręcznego (został już uznany za taki w Ustawie o podpisie cyfrowym stanu Utah - patrz załącznik 3.). Ma on prawie wszystkie cechy funkcjonalne podpisu odręcznego: jest prosty w użyciu (oczywiście dla użytkowników EDI), jednoznacznie identyfikuje posiadacza (ma własność niezaprzeczalności nadania), musi być stosowany po zakończeniu tworzenia podpisywanego tekstu, a więc psychologicznie w tym samym momencie co podpis ręczny. Jednocześnie znacznie przewyższa podpis ręczny w odniesieniu do prostoty procedury weryfikacji autentyczności podpisu i integralności (niezmienności) treści podpisanej. Jego jedyną wadą jest jego przyporządkowanie do "rzeczy którą posiada autor dokumentu", a nie do "osoby autora".

Na zakończenie należy wspomnieć, że cytowany tu raport TEDIS II podaje, że w analizowanych krajach jak dotychczas nie wystąpił precedens procesu sądowego w sprawie EDI. Jest to bardzo optymistyczna informacja dla potencjalnych użytkowników.

Przechowywanie komunikatów EDI

Formalne wymagania przechowywania dokumentów istotnych dla EDI

Podobnie jak w wypadku tworzenia i przesyłania dokumentów, również proces przechowywania dokumentów jest często poddany rygorom prawnym. Dotyczą one następujących aspektów:

- wymaganego czasu przechowywania,
- postaci w jakiej przechowywany jest dokument,
- rozróżnienia pomiędzy oryginałem a kopią.

Czas wymaganego przechowywania wynika z roli jaką pełni dany dokument i trwałości wynikających z niego zobowiązań. W kontekście dokumentów związanych z EDI ustawodawstwo określa najczęściej 3 typy dokumentów: dokumenty ogólne, dokumenty prawa handlowego, dokumenty prawa księgowego/podatkowego.

Nawet w obrębie krajów europejskich wymagane okresy przechowywania dla tych typów dokumentów są bardzo zróżnicowane (patrz tabela 1.) :

Kraj	reguła ogólna	prawo handlowe	prawo fiskalne
Polska			5 lat
Belgia	30 lat		10 lat
Dania	20 lat		5 lat - ogólnie 1 rok - dowody papierowe po zaksięgowaniu elektronicznym
Wlk. Brytania	12 lat	6 lat	6 lat
Francja	30 lat		10 lat 3 lata - faktury elektroniczne na nośnikach magnetycznych
Niemcy	30 lat		10 lat
Grecja	20 lat	10 lat	6 lat
Włochy	10 lat	10 lat	10 lat
Holandia	20 lat	10 lat	10 lat
Finlandia	10 lat		10 lat
Szwajcaria	10 lat	10 lat	10 lat
Norwegia	10 lat		10 lat
Szwecja	10 lat	10 lat	10 lat

Tabela 1. Obowiązujące okresy przechowywania różnego typu dokumentów w wybranych państwach europejskich

Dodatkowe wymagania formalne dotyczące przechowywania kopii dokumentów, określają właściwą kopię jako wierną i trwałą. Jeśli tylko dokument źródłowy jest akceptowany w postaci elektronicznej, to uzyskanie kopii o takich własnościach nie przedstawia poważniejszego problemu. Współczesne systemy komputerowe i stosowane w nich zabezpieczenia przed błędami losowymi dają w zasadzie pełną gwarancję wierności tworzonych na nośnikach zewnętrznych kopii danych (w zakresie ochrony przed zniekształceniami przypadkowymi). Również cechę trwałości (w rozważanym tu przedziale czasu 5-10 lat) posiadają wszystkie stosowane współcześnie nośniki magnetyczne i optyczne.

Należy jednak zwrócić tu uwagę na niejednokrotnie mylne rozumienie terminu trwałości i łączeniu go z cechą wierności. Otóż w naszym mniemaniu trwałość oznacza wymaganie, aby informacja zapisana początkowo na danym nośniku jako wierna (zgodna z oryginałem) nie uległa samoistnej zmianie (np. zanikowi, który może wystąpić w przypadku użycia jako nośnika papieru światłoczułego). Własność wierności natomiast jest wymaganiem, aby informacja utrwalona była zgodna z oryginalną. Biorąc pod uwagę tak zdefiniowane cechy, komputerowe nośniki jednokrotnie zapisywalne (WORM, CD-ROM) nie są zasadniczo różne od powszechnie używanych nośników magnetycznych wielokrotnego zapisu. Trwałość informacji na takich nośnikach magnetycznych, prawidłowo przechowywanych, jest zupełnie wystarczająca dla potrzeb archiwizacji w okresie 5 - 10 lat (a nawet znacznie dłużej).

Podstawowym problemem jest jednak spełnienie wymogu wierności w odniesieniu do manipulacji intencjonalnych, czyli świadomych ingerencji modyfikujących zawartość

przechowywanych danych. Niestety, i w jednym i drugim przypadku wymóg zapewnienia wierności zapisanej informacji, bez stosowania dodatkowych środków ochrony, nie może być spełniony. W wypadku nośników magnetycznych nieautoryzowana modyfikacja polega na zmianie zawartości bez zmiany nośnika, w przypadku nośników z zapisem jednokrotnym nieautoryzowana modyfikacja jest możliwa poprzez zamianę nośnika z oryginalną informacją na nieodróżnialny nowy nośnik z informacją zmodyfikowaną. Jedyną więc różnicą między tymi typami nośników jest dodatkowa uciążliwość techniczna towarzysząca nieautoryzowanym modyfikacjom danych na nośnikach jednokrotnie zapisywalnych, polegająca na konieczności uzyskania dostępu do nowego egzemplarza nośnika i do odpowiednich urządzeń zapisujących. Przy aktualnym rozpowszechnieniu środków zapisu na nośnikach typu WORM i CD-ROM i stosunkowo niskiej ich cenie, nawet w środowisku zastosowań biznesowych (nie mówiąc już o bankowych czy militarnych), ryzyko takiej możliwości jest znaczne. Jak z tego wynika, problem wierności kopii dokumentów EDI ponownie sprowadza się: do zagadnienia autoryzacji przechowywanego komunikatu umożliwiającej wykrycie modyfikacji, do autoryzacji nośnika na którym komunikaty te są zapisane w sposób trwały (np. podpis bezpośredni na płycie CD-ROM) lub do zapewnienia ochrony dostępu do danego nośnika (np. poprzez ołowianą plombę chroniącą dostęp do danych zapisanych w pamięci fiskalnej). Ponieważ jednak nie występuje tu konieczność teletransmisji, tradycyjne środki ochrony (takie jak ochrona fizyczna czy autoryzacja podpisem płyt lub kaset) są możliwe do zastosowania w praktyce.

Częstym rozwiązaniem jest przyjęcie wymogu stosowania jednoczesnego dwóch form archiwizacji: tworzenia kopii najbardziej istotnych danych na nośniku papierowym autoryzowanym tradycyjnym podpisem i tworzeniu pełnej kopii danych na nośniku komputerowym (dowolnym). Daje to z jednej strony istotne oszczędności w koszcie przechowywania pełnych danych i zachowanie przez kopiującego zdolności do szybkiego ich wyszukiwania, z drugiej strony, przy pomocy technik tradycyjnych i tanich zabezpiecza wiarygodność tych informacji, które mogą być przedmiotem celowej manipulacji (najczęściej są to kwoty i daty występujące na dokumentach źródłowych). Przykładem takich rozwiązań są właśnie regulacje prawne dotyczące archiwizacji faktur elektronicznych.

Dodatkowe wymagania pojawiają się, jeśli komunikaty EDI zawierają dane poddane ochronie jako dobra osobiste. Występuje wtedy wymaganie stosowania należytych środków ochrony (które dotyczy również dokumentów papierowych), a jednocześnie elektroniczna forma informacji zwiększa zagrożenia utraty poufności. W tym wypadku użytkownicy EDI muszą podporządkować się istniejącym ogólnym wymogom ustawowym dotyczącym ochrony danych osobowych przechowywanych w postaci elektronicznej.

Kolejnym, ostatnim problemem jest pojawiający się w pewnych przypadkach wymóg stanowiący, że jedynie oryginał dokumentu prowadzi do określonych skutków prawnych. Jest to szczególnie częste w zastosowaniach bankowych, gdzie dokument stanowi dowód określonych zobowiązań finansowych (czeki, weksle, akcje i tym podobne dokumenty). Dokument w formie elektronicznej ma sobie właściwą własność równoważności kopii, a więc nie umożliwia tworzenia odróżnialnego od kopii oryginału. Jednocześnie jednak dotychczasowa praktyka obrotu dokumentami papierowymi tego typu wykazała, że technika oryginału papierowego ma również swoje wady, takie jak np. podatność na zniszczenie fizyczne, które w tym wypadku prowadzi często do utraty praw majątkowych, lub podatność na fałszerstwo, co zmusza do stosowania dodatkowych kosztownych zabezpieczeń dokumentów. Stąd też w wielu krajach stosuje się już zdematerializowane formy takich dokumentów, zastępując technikę anonimowo posiadanego

oryginału, przez prowadzenie rejestru osób posiadających określone prawa wynikające z dematerializowanych dokumentów. Rejestry te prowadzi instytucja pełniąca funkcje Zaufanej Trzeciej Strony. Chociaż ich wprowadzenie jest związane z poważnym wysiłkiem organizacyjnym i materialnym, to w wypadku dokumentów o dużej wartości i stosunkowo rzadko zmieniających właścicieli, technika ta jest uznawana za w pełni efektywną. W Polsce przykładem tego typu rejestru jest Centralny Rejestr Bonów Skarbowych oraz rejestr przewidziany dla dematerializacji Świadectw Udziałowych PPP.

Powszechne wprowadzenie podpisu cyfrowego również wprowadza podobne wymagania, gdyż odbiorca, chcący zweryfikować otrzymany podpis nadawcy musi posłużyć się jego kluczem publicznym, przy czym musi mieć pewność, że kopia klucza którą użyje jest zgodna z oryginałem utworzonym i posiadanym przez nadawcę. Taką pewność można uzyskać stosując odpowiednio zabezpieczone formy przekazywania kluczy publicznych pomiędzy nadawcami a odbiorcami, lub też przez wprowadzenie Zaufanej Trzeciej Strony, prowadzącej rejestr kluczy zgodnych z oryginałami. Tego typu usługę przewidziano w ustawie o podpisie cyfrowym stanu Utah.

Innym spektakularnym przykładem jest zrealizowana już pilotowo w USA koncepcja dematerializacji znaków pieniężnych, najbardziej "tradycyjnego" dokumentu wykorzystującego własności oryginału silnie chronionego przed nieupoważnionym kopiowaniem. Elektroniczna forma pieniędzy - *ecash* - wprowadzona została po raz pierwszy w 1995 roku przez Mark Twain Bank of St. Luis przy współpracy z firmą Digicash Inc. Pieniądze ecash mają postać komunikatów o unikalnej treści zabezpieczonych podpisem cyfrowym i rejestrowanych w centralnym rejestrze prowadzonym przez bank. Beneficjent, po otrzymaniu nowego komunikatu ecash musi zadbać o jego rejestrację na swoim koncie bankowym - pełniącym rolę rejestru centralnego. O tej chwili każda nowa próba dopisania zarejestrowanego komunikatu na czyimkolwiek koncie traktowana jest jako nielegalna. Jedyną dopuszczalną operacją jest wypłata, czyli zgoda uprawnionego użytkownika na obciążenie jego konta kwotą komunikatu. Komunikat uzyskuje wtedy stan "w obiegu" i może być bez pośrednictwa banku przekazywany pomiędzy użytkownikami. Jednak, jak to już wspomniano wcześniej, samo otrzymanie komunikatu ecash (a właściwie jego elektronicznej kopii) nie daje otrzymującemu żadnych praw. Dopiero zakończona powodzeniem wpłata na konto bankowe (czyli weryfikacja czy dany komunikat ma stan "w obiegu" w centralnym rejestrze i jest to pierwsza jego rejestracja jako wpłaty) czyni z posiadacza komunikatu rzeczywistego beneficjenta. Powyższy opis uświadamia jednocześnie zakres wymagań stawianych sieci telekomunikacyjnej, która przy takich zastosowaniach zapewnia łączność pomiędzy uczestnikami systemu i rejestrem centralnym. Jedynie zapewnienie stałego i niezawodnego dostępu do rejestru czyni system praktycznie użytecznym dla użytkowników. Koszt utworzenia i utrzymania takiego systemu jest ceną jaką muszą oni zapłacić w zamian za korzyści związane z dematerializacją.

W wypadku narzuconej prawem konieczności przechowywania dokumentów reprezentowanych przez komunikaty EDI najczęściej nie występuje konieczność wprowadzania zmian w istniejących normach prawnych, o ile wprost nie stanowią one, że jedyną dopuszczalną postacią archiwizowanej kopii jest postać papierowa (lub inna, równie uciążliwa w stosowaniu lub wymagająca znacznych nakładów). Zadbać jedynie należy, aby wszyscy użytkownicy realizowali to zadanie z należytą starannością.

W praktyce, o ile tylko nie pojawia się problem archiwizacji odręcznego podpisu, który jest środkiem zapewniającym niezaprzeczalną autoryzację oryginału archiwizowanego w postaci elektronicznej, w ustawodawstwie państw europejskich i Stanach Zjednoczonych nie ma ograniczeń związanych ze stosowaniem elektronicznej formy archiwów.

Czytelność komunikatów EDI

Jedną z istotnych cech dokumentu jako dowodu jest jego czytelność dla organu rozstrzygającego - czyli w ogólnym przypadku - sądu. W tym kontekście wartość dowodowa komunikatów EDI może być podważana z trzech powodów: ze względu na postać elektroniczną komunikatu pierwotnego, ze względu na użycie kodów (najczęściej liczbowych) w miejsce tekstów jawnych i ze względu na szyfrowanie danych stosowane jako ochrona poufności przesyłanej informacji.

Problemy prawne związane z niematerialną postacią komunikatów EDI

Komunikaty EDI ze swej istoty mają postać elektroniczną, co umożliwia ich przesyłanie drogą teletransmisji. Stąd pojawia się pierwszy problem, czy stanowią one dowód materialny, a następnie czy jest to dokument w formie pisemnej (patrz rysunek 1-1).

W większości krajów Europy praktyka akceptuje dowody uzyskane drogą teletransmisji (telex, faks). Tym niemniej niektóre kraje (np. Finlandia) przygotowują specjalne akty prawne poświęcone problemom wynikającym z faktu odtwarzania u odbiorcy jedynie kopii posiadanego przez nadawcę oryginału.

Kolejny występujący problem to uznanie komputerowego wydruku komunikatu EDI jako dokumentu pisemnego. I znowu, w odniesieniu do tego problemu praktyka prawnicza w Europie różni się znacznie. Podstawowy problem polega na uznaniu dokumentu wygenerowanego przez komputer za dowód lub tylko za domniemanie. Ogólnie uznaje się, że jeśli wydruk został wygenerowany w sposób świadomy przez operatora, to ma wartość dowodową. Jeśli jednak operator taki nie istnieje (co ma miejsce w przypadku wymiany komunikatów EDI), to strona przedstawiająca wydruk jako dowód musi dowieść, że system komputerowy "działał prawidłowo" w chwili tworzenia tego wydruku. Podobnie, strona kwestionująca wydruk komputerowy musi dowieść, że system "działał nieprawidłowo" w trakcie jego tworzenia. Odstępstwa od tej zasady pojawiają się w przypadku dążenia prawodawcy do ochrony interesów strony słabszej, czyli np. osoby fizycznej w sporach z osobami prawnymi. W przypadku kwestionowania przez klienta płatności go obciążającej, a wynikłej z operacji dokonanej przy użyciu kart płatniczych w sposób bezdokumentowy, operator systemu musi udowodnić, że w odniesieniu do kwestionowanej transakcji system działał prawidłowo. Nie jest to jednak generalnie obowiązującą zasadą.

Kodowana treść komunikatów EDI

Jest powszechnie przyjęte, że komunikaty EDI ze względu na dążenie do minimalizacji ich objętości, zawierają kody w miejsce tekstów jawnych. Oczywiście zasady kodowania są ustalane w sposób znany uczestnikom wymiany, ale mogą stanowić problem z chwilą przedstawienia

komunikatu jako dowodu sądowego. Można tu widzieć analogię do tłumaczenia dowodów pisemnych z innych języków, z tym że nie istnieją jeszcze w tej dziedzinie tłumacze przysięgli. Można tu brać pod uwagę dwie możliwości: archiwizacja komunikatów EDI jest realizowana po zastąpieniu kodów tekstami jawnymi lub w procedurze procesowej dopuszcza się użycie eksperta-świadka, który dokonuje odpowiednich konwersji formy komunikatu. Pierwszą ewentualność uznaje się za zdecydowanie mniej korzystną z powodu znacznego przyrostu objętości danych archiwizowanych i utraty zgodności formy komunikatu nadanego i odebranego (gdyż translacja na postać jawną może być wykonana np. w odniesieniu do różnych języków). Należy więc jedynie zapewnić, aby procedura sądowa umożliwiała użycie świadka w charakterze tłumacza (w Polsce rolę tę pełni biegły sądowy), oraz by archiwizacji podlegały nie tylko same komunikaty lecz również katalogi kodów i ich znaczeń.

Szyfrowanie treści komunikatów EDI

Chociaż dotychczas w zastosowaniach komercyjnych utajnianie treści komunikatów EDI nie jest częstą praktyką, to jednak powinno być prawnie dopuszczalne jako potrzeba która potencjalnie może wystąpić. Na ogół, systemy prawne krajów europejskich nie wprowadzają tu ograniczeń, poza Francją, gdzie wymagane jest złożenie deklaracji użycia lub uzyskanie autoryzacji (w zależności od celu w jaki środki te są używane).

Kolejny problem pojawia się, gdy zaszyfrowany komunikat ma stanowić dowód sądowy. Drogi jego rozwiązania są podobne do tych, które dotyczyły użycia kodów. W wypadku kodów, ich znaczenie było jawne i powszechnie znane, w wypadku szyfrogramu, odkodowania może podjąć się tylko osoba znająca klucz, a więc niekoniecznie bezstronna w stosunku do przedmiotu sporu. Praktycznie jednak, w przypadku obu powszechnie wykorzystywanych kryptosystemów - symetrycznego i asymetrycznego, druga strona ma możliwość weryfikacji, czy użyty przez biegłego do odkodowania klucz jest kluczem właściwym. W przypadku systemu symetrycznego obie strony posiadają bowiem ten sam klucz, w przypadku zaś systemu asymetrycznego, druga strona ponownie szyfrując otrzymany komunikat jawny może sprawdzić, czy zostanie utworzony komunikat zaszyfrowany identyczny z komunikatem stanowiącym dowód w sporze.

2.3 Regulacje aktualnie istniejące w Polsce

Polskie uregulowania zostaną krótko zobrazowane przez kilka przykładów. Uregulowania dotyczące problemu dokumentu w postaci elektronicznej pojawiły się m.inn. w następujących aktach prawnych:

1. Rozporządzeniem z dnia 6.02.1992 r. zmieniającym rozporządzenie - Regulamin wewnętrznego urzędowania sądów powszechnych (Dz.U. Nr 16/1992, poz. 67), Minister Sprawiedliwości zezwolił sądom na prowadzenie wszystkich rejestrów sądowych przy zastosowaniu systemu informatycznego opartego o program komputerowy, przy czym sąd musi uprzednio wydać postanowienie o wpisie, w którym ustala treść wpisu, jaka będzie wprowadzona do programu komputerowego.

2. Ustawa z 06.07.1982 r. o księgach wieczystych i hipotece (Dz.U. Nr 19/1982, poz. 147 z późn. zm.) w ustępie 2 artykułu 58 udzieliła Ministrowi Sprawiedliwości delegacji do wydania rozporządzenia dotyczącego zasad wykorzystania systemów informatycznych dla celów prowadzenia ksiąg wieczystych. Minister skorzystał dwukrotnie z tej delegacji:

   a) w § 6 rozporządzenia z dnia 18.03.1992 r. w sprawie wykonania przepisów ustawy o księgach wieczystych i hipotece (Dz.U. Nr 29/1992, poz. 128) Minister Sprawiedliwości dopuścił możliwość prowadzenia ksiąg wieczystych przy zastosowaniu systemu informatycznego opartego o program komputerowy. W tym wypadku wydruki komputerowe zastępują dotychczasowe formularze ksiąg wieczystych, lecz mają do nich zastosowanie odpowiednio przepisy o prowadzeniu ksiąg wieczystych.

   b) przepisy powyższe znajdują także zastosowanie w prowadzeniu ksiąg notarialnych-§ 9 rozporządzenia z dnia 12.04.1991 r. w sprawie prowadzenia ksiąg notarialnych oraz przekazywania na przechowanie dokumentów sądom rejonowym (Dz.U. Nr 33/1991, poz.147).

3. Interesujące jest również rozporządzenie Ministra Finansów z dnia 12 maja 1993 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące, oraz warunków stosowania tych kas przez podatników (Dz.U.Nr 39/93 poz. 178). Rozporządzenie to dotyczy archiwizowania danych, a nie o ich przesyłania. Zdefiniowana została "pamięć fiskalna" (§ 1 ust 2 pkt. 8) oraz wymienione są kryteria techniczne, jakie musi spełniać kasa fiskalna, aby zgromadzone w niej dane mogły być przechowywane (§ 3). Postanowienia te dotyczą przede wszystkim niezbędnych zabezpieczeń, jakie musi posiadać kasa fiskalna przed możliwością mechanicznego zniszczenia danych lub ich zmiany. Funkcję takiego zabezpieczenia mają spełniać plomby ołowiane, które ulegają zniszczeniu w momencie wyjęcia pamięci fiskalnej. Obok bardzo ogólnie określonych wymogów technicznych, rozporządzenie zawiera również postanowienia dotyczące wymagań formalnych, jakim musi sprostać dokument sporządzony przez kasy fiskalne (§ 4 i 5). Jednakże tak jak przypadku innych aktów prawnych traktujących o elektronicznym przetwarzaniu dokumentów, również w odniesieniu do kas fiskalnych istnieje wymóg przeniesienia treści dokumentu elektronicznego na nośnik trwały, tj. papier, czy mikrofilm, albowiem w tym zakresie rozporządzenie odwołuje się do przepisów o rachunkowości (§ 6 pkt. 6).

4. Najobszerniej wykorzystanie komputera przy prowadzeniu dokumentacji reguluje ustawa z dnia 29.09.1994 r. o rachunkowości (Dz.U. Nr 121/1994, poz. 591). Dotyczy ona wszystkich jednostek działających na podstawie prawa bankowego, z wyjątkiem Narodowego Banku Polskiego. Tak jak w poprzednich uregulowaniach, tak i w tym przypadku warunkiem *sine qua non* prowadzenia ksiąg rachunkowych za pomocą komputera jest późniejsze przeniesienie ich na nośnik trwały, czyli domyślnie papier, mikrofilm lub dysk optyczny jednorazowego zapisu, w terminach przewidzianych przez omawianą ustawę.

   Ustawa ta zezwala w zasadzie jednoznacznie na stosowanie elektronicznej wymiany danych przy prowadzeniu ksiąg rachunkowych przy pomocy komputera. W ustępie 5 artykułu 20 dopuszczono stosowanie urządzeń łączności (w związku z brakiem w ustawie punktu eliminującego jakiekolwiek urządzenie łączności należy w tym rozumieć również sieć komputerową, czyli relację "komputer-komputer") do dokonywania w księgach

rachunkowych zapisów. Warunkiem dokonywania takich zapisów jest możliwość stwierdzenia źródła pochodzenia takiego zapisu, tzn. bezsprzeczna możliwość identyfikacji autora zapisu. Drugim wymogiem jest to, aby podczas rejestracji operacji gospodarczej zapis uzyskał trwale czytelną postać odpowiadającą treści dowodu księgowego.

5. Również przepisy bankowe dopuszczają posługiwanie się techniką komputerową, przy prowadzeniu oraz przechowywaniu ksiąg rachunkowych i zapisów księgowych. Nie jest to natomiast możliwe w odniesieniu do dowodów księgowych, które muszą zawierać podpisy wystawców oraz w stosunku do zestawień dowodów księgowych, które z kolei muszą zawierać dwa podpisy: osoby sporządzającej i osoby sprawdzającej zestawienie (zarządzenie Nr 1/19 Prezesa Narodowego Banku Polskiego z dnia 12.02.1991 r. w sprawie jednolitych zasad rachunkowości bankowej - Dz.Urz. NBP Nr 2, poz.3 i Nr 11 poz. 36 i z 1994 r. Nr 1, poz. 1).

Do podstawowych elementów uniemożliwiających użycie formy elektronicznej dokumentu, należy występowanie obligatoryjnego wymogu zastosowania formy pisemnej, połączonego najczęściej z obowiązkiem złożenia na dokumencie własnoręcznego podpisu. Drugim istotnym elementem jest obowiązek archiwizacji dokumentów na nośniku papierowym, który w znacznym stopniu niweluje przydatność elektronicznej ich wymiany. Na przykładzie prawa bankowego przedstawiono poniżej te przepisy, które utrudniają prowadzenie elektronicznej wymiany dokumentów, poprzez nałożenie obowiązku sporządzenia ich w formie pisemnej, bądź też bezpośrednio żądają złożenia własnoręcznego podpisu.

a) W ustawie z dnia 31 stycznia 1989 r. prawo bankowe (Dz.U. Nr 72/1992 poz. 359 z późn. zm.) wymóg formy pisemnej został przewidziany w następujących sytuacjach:

- sporządzenie umowy kredytowej (art.27 ust. 2),
- udzielenie gwarancji bankowej osobom krajowym i zagranicznym pod rygorem nieważności (art. 40 ust. 2),
- dokumenty stwierdzające udzielenie kredytu, jako podstawa wpisu do księgi wieczystej (art. 50 ust. 1),
- księgi banków, wyciągi z tych ksiąg podpisane przez te banki i opatrzone pieczęcią oraz wszelkie w ten sam sposób wystawione oświadczenia zawierające zobowiązania, zwolnienie z zobowiązań, zrzeczenie się praw lub pokwitowanie odbioru należności bądź stwierdzające udzielenie kredytu, jego wysokość i warunki spłaty, które mają moc prawną dokumentów urzędowych oraz stanowią podstawę wpisów w księgach wieczystych i rejestrach publicznych (art. 53 ust. 1),
- księgi, bilanse, rejestry, plany, sprawozdania i inne dokumenty w formie umożliwiającej sporządzenie ich kopii (art. 102 pkt. 2).

b) Zarządzenie Prezesa NBP z dnia 5 listopada 1992 r. w sprawie szczegółowego trybu i form udzielania gwarancji bankowych (M.P. Nr 36 poz. 270). Forma pisemna przewidziana jest dla umowy określającej wierzytelność, która ma zostać zabezpieczona gwarancją, dokumentów niezbędnych dla dokonania oceny zdolności kredytowej, oświadczenie w sprawie proponowanych form zabezpieczenia wierzytelności banku z tytułu udzielenia gwarancji (§ 1 ust. 2). Udzielenie gwarancji, pisemne zapewnienie udzielenia gwarancji,

prowadzenie ewidencji dotyczących gwarancji również sporządzane są w formie pisemnej (§ 3 ust. 2 i § 5).

c) Zarządzenie Nr 5/93 Prezesa NBP z dnia 30 marca 1993 r. w sprawie zasad ogłaszania zweryfikowanych bilansów banków oraz ich rachunków zysków i strat (Dz.Urz. NBP Nr 4 poz. 8). Bilanse banków oraz ich rachunki zysków i strat muszą zostać przygotowane na formularzach, których wzory dołączone są do zarządzenia i, które muszą zostać opatrzone własnoręcznymi podpisami członków kierownictw banków.

d) Załącznik do zarządzenia Nr A/3/92 Prezesa NBP z dnia 17 czerwca 1992 r. (Dz.Urz. NBP Nr 5 poz. 10 i Nr 11 poz. 22), w którym zamieszczono treść regulaminu redyskonta weksli przez NBP, zawiera szereg przepisów ustalających wymóg formy pisemnej:

- sporządzenie w trzech egzemplarzach zestawienia weksli w formie określonej w załączniku nr 1, zawierającej podpis (§ 4 ust.1),

- sporządzenie trzech egzemplarzy zestawienia weksli, jeżeli weksle są składane do redyskonta przy kilku listach, w formie określonej w załączniku nr 2, zawierającej podpis (§ 4 ust.2),

- potwierdzenie odbioru weksli złożonych do redyskonta listem według wzoru stanowiącego załącznik nr 3 do regulaminu i przewidującego złożenie podpisu (§5 i §9),

- przesyłanie oddziałowi banku weksli przesyłką poleconą, przy liście według wzoru stanowiącego załącznik nr 4 do regulaminu zawierającego podpis (§ 10 ust. 2),

- przy indosie pełnomocniczym złożenie podpisu oddziału okręgowego (§ 10 ust. 3),

- przy wekslu zaprotestowanym, jego przesłanie podawcy weksli przesyłką poleconą przy liście według wzoru stanowiącego załącznik nr 5 do regulaminu i zawierającego wymóg postawienia stempla (§ 13),

- obowiązek przedłożenia we właściwych terytorialnie oddziałach okręgowych NBP, przez centrale banków, oświadczenia sporządzonego według wzoru stanowiącego załącznik nr 6 do regulaminu, który przewiduje konieczność złożenia podpisów (§ 15 ust. 1 pkt. 1),

- złożenie we właściwym terytorialnie oddziale okręgowym NBP przez upoważniony do tego przez centralę Banku Gospodarki Żywnościowej oddział wojewódzki tego banku oświadczenia , sporządzonego według wzoru stanowiącego załącznik nr 7 do regulaminu, przewidującego złożenie podpisów (§ 15 ust.1 pkt. 2).

e) Zarządzenie Nr A/1/93 Prezesa NBP z dnia 7 czerwca 1993 r. w sprawie zasad i trybu przyjmowania i wydawania przez Narodowy Bank Polski bonów pieniężnych Narodowego Banku Polskiego i bonów skarbowych w obrocie wtórnym (Dz.Urz. NBP Nr 7 poz. 13), w którym forma pisemna (według załączonego wzoru, na którym należy złożyć podpis) została przewidziana dla czynności związanych z transakcjami kupna-sprzedaży bonów (§ 1). Ponadto forma pisemna została zastrzeżona dla potwierdzenia przyjęcia bonów (§ 2 ust. 2).

f) W zarządzeniu NR A/7/92 Prezesa NBP z dnia 17 grudnia 1992 r. zawierającym "Regulamin aukcyjnego obrotu papierami wartościowymi pomiędzy Narodowym Bankiem Polskim a bankami" (Dz.Urz. NBP Nr 14 poz. 27 z późn. zm.) znajduje się kilka postanowień wymagających dokonania czynności w formie pisemnej:

- nadesłanie telefaksem lub dostarczenie do Centrali NBP (Departament Polityki Pieniężno-Kredytowej) prawidłowo wypełnionych formularzy ofert, co jest warunkiem uczestnictwa w aukcji, zgodnie z załącznikiem nr 1 zawierającym podpisy (§ 4),

- zawiadomienie przez NBP o przyjęciu lub odrzuceniu oferty, na formularzach stanowiących załącznik nr 2 i 3 do regulaminu (§ 9),

- listy zawierające określenie ilości serii i numerów oraz wartości nominalnej i aukcyjnej, przy których powinny być złożone papiery wartościowe, a które muszą zostać podpisane przez osoby uprawnione do składania oświadczeń w zakresie praw i obowiązków majątkowych banku (§ 10 ust. 2),

- "Oferta aukcyjnego zakupu od Narodowego Banku Polskiego papierów wartościowych na ..... dni", która musi zostać podpisana (§ 14 ust. 2 i załącznik).

g) Zarządzenie Nr A/2/93 Prezesa NBP z dnia 22 lipca 1993 r. w sprawie warunków emisji oraz zasad i trybu sprzedaży i wykupu bonów pieniężnych Narodowego Banku Polskiego (Dz.Urz. NBP Nr 10 poz. 17) ustanawia również w kilku przypadkach obowiązek zachowania formy pisemnej:

- pisemne upoważnienie do nadania bonowi charakteru imiennego, podpisane przez osoby upoważnione do podpisywania oświadczeń w zakresie praw i obowiązków majątkowych jednostki będącej posiadaczem bonu (§ 2 ust. 3),

- wniosek właściciela bonu imiennego o jego umorzenie (§ 2 ust. 4),

- "Oferta przetargowa na zakup bonów pieniężnych Narodowego Banku Polskiego", sporządzona według wzoru umieszczonego w załączniku nr 1 (§ 9 ust. 2),

- zawiadomienie przez NBP telefaksem o przyjęciu lub nieprzyjęciu oferty (§ 13 ust. 1 i 2),

- zapłata za bony na podstawie upoważnienia zawartego w ofercie banku (§ 15 ust. 2),

- wydanie przez oferenta jego bankowi dyspozycji płatniczej (§ 15 ust. 3),

- odbiór bonów za pokwitowaniem przez osobę upoważnioną do tego przez oferenta (§ 17 ust 1),

- zapłata za bon w drodze przekazania środków na wskazany przez posiadacza bonu w formie pisemnej (formularz bankowy)-rachunek bankowy, według wzoru stanowiącego załącznik nr 2 i 3 oraz potwierdzenie przez NBP, w formie pisemnej realizacji dyspozycji posiadacza bonu (§ 18 ust 2 pkt. 2 ppkt. a).

h) Zarządzenie Nr 1/91 Prezesa NBP z dnia 12 lutego 1991 r. w sprawie jednolitych zasad rachunkowości bankowej (Dz.Urz. NBP Nr 2, poz. 3 i Nr 11 poz. 36 i z 1994 r. Nr 1 poz.1) przewiduje formę pisemną w następujących przypadkach:

- dowód księgowy, musi posiadać podpis i stempel, jeżeli przewiduje to układ formularza względnie regulują odrębne przepisy (§ 5 ust. 2 pkt. 1 ppkt. e),

- zestawienie dowodów księgowych (§ 6 ust. 2 pkt 1),

- wystawianie dowodów księgowych i ich korekta (§ 9 ust 2, 3, 4)

- obowiązek ustalenia osób uprawnionych do podpisywania i zatwierdzania dowodów księgowych (§ 10 pkt 1).

2.4 Problemy dotyczące EDI wynikające z istniejących regulacji

Jak to już wcześniej komentowano, przeszkody prawne związane z zastępowaniem dokumentów tradycyjnych dokumentami EDI mogą mieć dwojaką postać:

- jeśli wymóg istnienia dokumentu tradycyjnego ma charakter normy bezwzględnie obowiązującej (w stosunku do użytkowników EDI), to mówimy o zakazie stosowania EDI;
- jeśli wymóg istnienia dokumentu tradycyjnego jest normą względnie obowiązującą, tzn. strony mogą od tego wymogu odstąpić akceptując negatywne tego skutki (najczęściej oznacza to brak mocy dowodowej dokumentu w formie elektronicznej utworzonego w zastępstwie dokumentu tradycyjnego), to mówimy o utrudnieniach w stosowaniu EDI.

Polskie prawodawstwo wprowadza zarówno zakazy jak i utrudnienia w stosowaniu EDI. Poniżej zebrano te najważniejsze.

Wybrane zakazy stosowania dokumentów w formie elektronicznej:

1. Dowód księgowy dokumentujący przejęcie lub przekazanie składnika majątkowego (...) musi zawierać podpis wystawcy dowodu oraz osoby której wydano lub od której przejęto składniki majątkowe [8].
2. Faktura VAT musi być sporządzona pisemnie i zawierać podpis wystawcy
3. Bilanse banków i ich rachunki zysków i strat muszą być opatrzone własnoręcznymi podpisami członków kierownictwa tych banków[9]
4. Dokumenty związane z transakcjami bonami pieniężnymi NBP wymagają podpisu[10]
5. Dokumenty związane z transakcjami bonami skarbowymi wymagają podpisu[11]
6. Wyciągi z ksiąg banków, które mają moc prawną oraz stanowią podstawę wpisów w księgach wieczystych i rejestrach publicznych, muszą być podpisane przez te banki i opatrzone pieczęcią[12]
7. Przy zapisach księgowych na podstawie danych uzyskanych za pośrednictwem środków łączności lub magnetycznych nośników danych, uzyskują one trwale czytelną postać odpowiadającą treści dowodu księgowego i możliwe jest stwierdzenie źródła pochodzenia każdego zapisu.[13]
8. Treść dowodów księgowych, za wyjątkiem (...), może być przeniesiona na nośniki optyczne (laserowe) oraz odpowiednie do tego mikrofilmy, pozwalające zachować w trwałej postaci zawartość dowodów.[14]

Wybrane utrudnienia w stosowaniu dokumentów w formie elektronicznej:

---

[8] Ustawa O Rachunkowości, Dz.U. z 1994 r. Nr.121, poz.591

[9] Zarządzenie Prezesa NBP

[10] Zarządzenie Prezesa NBP

[11] Zarządzenie Ministra Finansów

[12] Ustawa Prawo Bankowe, Dz. U. z 1992 r. Nr. 72, poz. 359 z późn. zm.

[13] Ustawa O Rachunkowości op. cit.

[14] Ustawa O Rachunkowości op. cit.

1. W przypadku takich czynności gdzie transfer dóbr przekracza 2 000 zł forma pisemna jest zastrzeżona dla celów dowodowych (*ad probationem*). Oznacza to, że niedochowanie tej formy nie powoduje nieważności dokonanej transakcji lecz taki skutek, że w razie sporu niedopuszczalny jest w zasadzie dowód ze świadków i z przesłuchania stron dla wykazania, że czynność prawna została dokonana. Zwykła forma pisemna stawia wymóg własnoręcznego podpisania dokumentu.[15]

Podane przykłady mają jedynie charakter ilustracyjny, ograniczając się do bankowości i ogólnej działalności gospodarczej. Szeroka ankietyzacja powinna określić, jakie wymagania formalne stanowią przeszkodę we wprowadzaniu EDI w innych sferach działalności gospodarczej i administracyjnej (np. w handlu zagranicznym, służbie zdrowia, różnego rodzaju ewidencji prowadzonych przez organa administracji państwowej i samorządowej, sprawozdawczości, rozliczeniach podatkowych itp.).

W dziedzinie bankowości i handlu podstawowym zakazem dotyczącym elektronicznej wymiany dokumentów, jest wynikający z Ustawy O Rachunkowości zakaz akceptacji dowodów księgowych bez (odręcznego) podpisu. W wypadku, gdy dowodem księgowym jest zlecenie klienta (np. zlecenie przelewu), to użycie tu formy elektronicznej staje się niemożliwe. Podobnie ma się rzecz z fakturą (która dodatkowo najczęściej podlega wymogom wynikającym z dokumentowania obrotu związanego z podatkiem VAT), czy wyciągiem z konta, otrzymanym jako dowód księgowy obcy. Akceptacja faksowej kopii podpisanego oryginalnego dokumentu nie zmienia w niczym sytuacji, gdyż dalej oryginał musi mieć postać pisemną, co wyklucza komunikaty EDI. Jest charakterystyczne, że ustawodawca wprowadzając w swych rozporządzeniach wyjątki od ogólnych zakazów[16], jak dotychczas nie uwzględniania w żaden sposób potrzeb użytkowników EDI.

Wśród ograniczeń dotyczących archiwizacji dokumentów, najbardziej dotkliwym wydaje się wymaganie wyrażone w Ustawie o Rachunkowości, aby archiwizacja dowodów otrzymanych drogą teletransmisyjną następowała w sposób trwale czytelny. Nie stanowiłoby to poważniejszego utrudnienia, gdyby nie dalsze postanowienia Ustawy, w których określenie "trwale czytelny" łączy się jedynie z nośnikami optycznymi i mikrofilmami. Chociaż ceny tego typu nośników i urządzeń z nimi związanych stale maleją, to jednak są one znacznie wyższe od cen urządzeń i nośników magnetycznych. Jednocześnie, zgodnie z uwagami zawartymi w punkcie 3.2.2, z formalnego punktu widzenia, podatność na manipulacje obu typów nośników jest równorzędna.

2.5 Propozycje poprawy sytuacji

Po przeanalizowaniu różnych wariantów możliwych rozwiązań w zakresie elektronicznej wymiany i archiwizowania dokumentów elektronicznych oraz dokonaniu przeglądu rozwiązań prawnych w

[15] Kodeks Cywilny

[16] Minister Finansów w swym rozporządzeniu określającym postać faktury VAT (Dz.U. Nr 39, poz 176) dopuszcza brak podpisu odręcznego np. na fakturach wystawianych nabywcom energii elektrycznej i cieplnej, usług telekomunikacyjnych itp.

różnych krajach postuluje się oparcie elektronicznej wymiany dokumentów na następujących zasadach:

I. Rozwiązania doraźne:

1. regulowanie kwestii nie wymagających interwencji w istniejący porządek prawny w drodze umowy pomiędzy zainteresowanymi stronami;
2. opracowanie lub zainicjowanie opracowania sektorowych zasad oraz wytycznych stosowania EDI i archiwizacji dokumentów elektronicznych, w tym wzorców umów EDI i niezbędnych wymagań na ochronę komunikatów EDI;

II. Rozwiązania podstawowe:

1. dokonanie przeglądu i ewidencji tych dokumentów, dla których istniejący zakaz stosowania formy elektronicznej stanowi istotną niedogodność dla podstawowych podmiotów życia gospodarczego i administracyjnego w Polsce;
2. wprowadzenie odpowiednich zmian w przepisach wykonawczych, w celu zlikwidowania istniejących barier w stosowaniu EDI i elektronicznej archiwizacji w odniesieniu do konkretnych dokumentów, dla których ograniczenia dadzą się usunąć tą drogą;
3. wystąpienie w trzech przypadkach z inicjatywą ustawodawczą (patrz niżej), w postaci nowelizacji istniejących regulacji ustawowych;

III. Rozwiązanie perspektywiczne:

rozpoczęcie przygotowań do wprowadzenia w Polsce ustawy nadającej ogólną moc prawną podpisowi cyfrowemu.

Rozwiązania doraźne

Użytkownicy stosujący technikę EDI w krajach bez odpowiednich dla EDI regulacji prawnych, mogą wybrać następujące strategie działania:

a) w przypadku norm względnie obowiązujących i utrudnień stąd wynikających:

1) uznać, że przesyłane komunikaty EDI nie będą miały wartości dowodowej, a w wypadku sporu sądowego będzie on rozstrzygany bez ich wykorzystania;
2) postanowić na drodze wzajemnej umowy, że komunikaty EDI mają dla stron tę samą moc dowodową co odpowiednie dokumenty, które zastępują,
3) stosować podwójny obieg dokumentów, tworząc dokumenty tradycyjne obok komunikatów EDI.

b) w wypadku zakazu stosowania dokumentów w postaci elektronicznej:

3) stosować podwójny obieg dokumentów, tworząc dokumenty tradycyjne obok komunikatów EDI;

Rozwiązanie typu (1) może być akceptowalne przede wszystkim w odniesieniu do dokumentów o charakterze informacyjnym, nie prowadzących do powstania skutków prawnych. Przykładami mogą być informatory i prospekty bez podanych cen. W kontekście dokumentów bankowych, brak wartości dowodowej wydaje się nie być przeszkodą w odniesieniu do następujących dokumentów:

- wyciągu o obrotach i stanie konta (nie dla celów wpisów w rejestrach publicznych i księgach wieczystych), jeśli dla odbiorcy nie ma on stanowić dowodu księgowego;
- zbiorczej informacji dla klienta o posiadanych środkach;
- informacji banku o oferowanych usługach.

Dokumenty te mogą być wymieniane bez żadnych regulacji prawnych lub umownych.

W odniesieniu do bardziej istotnych dokumentów, do których należą np.:

- potwierdzenie operacji (uznaniowej, obciążeniowej);
- zlecenie płatnicze (nie jako dowód księgowy);
- międzybankowe zlecenie płatnicze (nie jako dowód księgowy);
- zlecenie płatnicze do banku centralnego (jako dowód księgowy);
- zlecenie giełdowe lub przetargowe;
- potwierdzenie operacji giełdowej lub przetargowej;
- zlecenie rejestracji praw do dokumentu dematerializowanego;
- zapytanie do centralnego rejestru;
- odpowiedź z centralnego rejestru

najbardziej uzasadnione będzie nadanie im mocy dowodowej na zasadzie umowy między stronami. Umowa taka nie powinna być odczuwana przez uczestników jako dodatkowe obciążenie. To rozwiązanie, stosowane jest np. w ramach systemu elektronicznej wymiany komunikatów płatniczych ELIXIR:

"Uczestnik oraz KIR S.A. zobowiązują się informacje otrzymywane z wykorzystaniem urządzeń i oprogramowania, o których mowa w § 3 ust. 2 pkt 2, (...,) traktować na równi z czekami i poleceniami przelewu, (...) - a także uznają, że mogą one stanowić podstawę do sporządzania wtórnych dokumentów księgowych"[17]

W odniesieniu do użytkowników EDI podległych Ustawie O Księgowości, dokumenty w ten sposób otrzymane nie mogą stanowić dowodów księgowych (patrz [18]), chyba że znajdzie tu zastosowanie przepis z art. 20 pkt.4 (patrz [19]), mówiący zasadach postępowania w wypadku uzasadnionego braku możliwości uzyskania zewnętrznych, obcych dowodów źródłowych. Niestety, utworzony wtedy księgowy dowód zastępczy musi mieć podpis wystawcy dowodu, czyli upoważnionego przedstawiciela klienta, gdyż nie może tu mieć zastosowania art. 21 pkt.4 (patrz [20]), pozwalający na zastępowanie podpisów znakami identyfikującymi, ale tylko w odniesieniu do dowodów, które nie dokumentują przekazania lub przejęcia składnika majątkowego. Można też rozważać posługiwanie się rozwiązaniami zastępczymi, zmniejszającymi uciążliwość podwójnego obiegu dokumentów, np. przez zastosowanie dowodów księgowych zbiorczych, tworzonych jednokrotnie na zakończenie okresów ewidencyjnych (np. dekad lub miesięcy).

---

[17] Umowa uczestnictwa w systemie rozliczeń ELIXIR prowadzonych przez Krajową Izbę Rozliczeniową S.A.
[18] Ustawa O Księgowości op. cit
[19] Ustawa O Księgowości op. cit
[20] Ustawa O Księgowości op. cit

Należy zauważyć, że czasami pojawiają się tu możliwości rozwiązań sektorowych. Np. w stosunku do cech formalnych bankowego dowodu księgowego stosowanego w NBP Prezes NBP może zaniechać wymogu podpisu (i stempla) na podstawie odrębnych przepisów.

Jak wynika z powyższych zestawień, w odniesieniu do podstawowych podmiotów gospodarczych (tam gdzie należy spodziewać się największych korzyści z wprowadzenia EDI) istotną grupę dokumentów stanowią te, które mogą być stosowane w formie komunikatów EDI jedynie z zachowaniem równoległego obiegu dokumentów tradycyjnych - np. faktury i innych dowodów księgowych. W przypadku systemów o podwójnym obiegu dokumentów, pierwszym dokumentem otrzymywanym przez użytkowników jest komunikat elektroniczny. W związku z tym, uczestnicy na drodze umowy muszą określić jego znaczenie prawne. Uczestnicy powinni również określić zasady na jakich rozstrzygać będą przypadki rozbieżności pomiędzy komunikatem elektronicznym, a uzyskaną następnie wersją właściwą dokumentu. Konieczność stosowania podwójnego obiegu dokumentów (oraz podwójnej archiwizacji) pozbawia uczestników wymiany EDI znacznej części korzyści ekonomicznych i forma ta może być akceptowana jedynie jako przejściowa.

Jak wynika z tej analizy, do czasu uzyskania właściwych rozwiązań legislacyjnych, główny ciężar stworzenia właściwych zasad działania systemów EDI spoczywa na umowie. W wypadku stosunkowo nowej technologii jaką jest EDI, negatywne skutki działania nawet niewielkiej grupy instytucji, które będą działać legalnie ale nierozważnie, mogą mieć dotkliwe następstwa. W związku z tym wydaje się, że niezbędnym jest opracowanie pewnych wzorców i norm dotyczących EDI, które będą ułatwiały wdrażanie EDI w polskiej praktyce. Nie muszą to być jednak akty prawne, a jedynie zalecenia lub wytyczne opracowane przez organizacje lub instytucje obdarzone właściwym autorytetem środowiska. Zalecenia te powinny określać najbardziej istotne cechy dokumentu elektronicznego, systemów wymiany dokumentów i zasad ich przechowywania. Poniżej omówiono je w sposób bardzo skrótowy.

Umowa

Na istniejącym etapie wdrażania EDI w wielu wypadkach wystarczającym i jednocześnie najprostszym regulatorem stosunków pomiędzy uczestnikami wymiany będzie umowa. Przede wszystkim powinna być ona jasna i rozpoczynać się od zdefiniowania pojęć, które jeszcze obecnie nie występują powszechnie w praktyce prawniczej. Powinna ona określać w sposób dokładny zobowiązania stron w zakresie dokonywanej wymiany.

Umowy mogą mieć charakter uzupełniający w stosunku do konkretnych usług merytorycznych (np. umowa o akceptacji zleceń przesyłanych drogą elektroniczną jako umowa uzupełniająca do umowy o prowadzeniu rachunku bankowego), lub mieć charakter generalny - dotyczący akceptacji wszystkich dokumentów wymienianych w formie elektronicznej (np. umowa o akceptowaniu wymiany EDI w ramach prowadzenia działalności handlowej, ubezpieczeniowej lub tp.). Ze względu na złożoność i brak doświadczeń w tej dziedzinie, istotną pomocą powinny tu być wzorce umów standardowych, opracowywane dla szerokiego grona użytkowników EDI na bazie rekomendacji międzynarodowych.

Ogólne zasady stosowania EDI i archiwizacji dokumentów elektronicznych

Bardzo istotną rolę w propagowaniu EDI i minimalizacji przeszkód w stosowaniu tej technologii może odegrać opracowanie ogólnych zasad stosowania EDI w odniesieniu do poszczególnych grup użytkowników. Zasady takie istnieją na poziomie międzynarodowym[21], należy je jednak przystosować do warunków polskich i odpowiednio rozpropagować.

Standard takiej umowy powinien być wypadkową pracy zespołu prawników i inżynierów, z racji istniejącego ścisłego związku pomiędzy zagadnieniami prawnymi i technicznymi (według opinii ekspertów niepożądane i wręcz niedopuszczalne jest sporządzenie umowy ramowej przez prawników, natomiast części technicznej zawartej w aneksach przez techników, gdyż w większości przypadków okazuje się, że te dwa elementy nie są z sobą zharmonizowane, a niekiedy wręcz wzajemnie się wykluczają). W umowie ramowej o elektronicznej wymianie dokumentów powinny się znaleźć bezwzględnie takie elementy, jak:

- określenie uczestników wymiany
- definicje użytych w niej pojęć (szczególnie wobec braku, w większości przypadków, definicji tych pojęć w aktach prawnych)
- sposób identyfikacji autora komunikatu
- określenie wartości dowodowej dokumentów elektronicznych przesyłanych pomiędzy uczestnikami
- określenie ważności i wymagalności zobowiązań powstałych przy wykorzystaniu dokumentów elektronicznych
- określenie zasad ochrony i uwierzytelnienia komunikatów oraz odpowiedzialności uczestników w wypadku pomyłek, błędów lub fałszerstw,
- sposoby rozstrzygania ewentualnych sporów i ewentualne wskazanie (bądź wykreowanie) organu, który będzie rozstrzygał,
- postanowienia dotyczące daty wejścia umowy w życie, akcesu ewentualnych innych uczestników wymiany, zmiany umowy i ich wygaśnięcia.

Inne elementy, takie jak konieczność tworzenia potwierdzeń odbioru komunikatów, zdefiniowania momentu i miejsca który uznaje się za chwilę i miejsce nadania oraz chwilę i miejsce odbioru komunikatów nie są specyficzne dla systemów EDI, ale mogą być przez uczestników wymiany wprowadzone do umowy, lub co jest częściej spotykane, do jej aneksów.

W międzynarodowych propozycjach wzorców takiej umowy, postuluje się, aby postanowienia dotyczące aspektów technicznych znajdowały się w aneksach do umowy - tzw. załącznikach technicznych. Zapewnia to przejrzystość umowy oraz w miarę możliwości, ułatwia zadanie zarówno prawnikom, jak i inżynierom, przy opracowaniu dobrego i spójnego kontraktu.

Wydaje się, że najbardziej pilną sprawą jest określenie rekomendacji dla użytkowników EDI co do niezbędnego zakresu ochrony komunikatów, tak aby w ramach swobody w kształtowaniu reguł działania systemów EDI poprzez umowy, strony przestrzegały zasad przezorności, które powinny charakteryzować poszczególne grupy użytkowników, a przede wszystkim sektor bankowy. Inicjatywa Związku Banków Polskich zmierzająca do opracowania takich wytycznych może stanowić tu istotny postęp. W przekonaniu autorów tego opracowania, jako rozwiązanie rekomendowane ochrony integralności i niezaprzeczalności powinna zostać wybrana technika podpisu cyfrowego. Przewidując, że grono użytkowników tej techniki będzie szybko liczebnie

---

[21] UN/ECE RECOMMENDATION No. 26 - Model Interchange Agreement for the International Commercial Use of Electronic Data Interchange (załącznik 1. opracowania); wzór umowy EDI proponowany przez Unię Europejską (rekomendacja nr 94/820/CE z dnia 19 października 1994 r.) (załącznik 2. opracowania).

wzrastać, należy już dziś stworzyć właściwe warunki organizacyjne do jej szerokiej implementacji. Temu celowi służą przede wszystkim ogólnie dostępne rejestry certyfikatów z kluczem publicznym i powołanie organów certyfikujących, wiarygodnie tworzących takie certyfikaty. W Polsce prekursorem w stosowaniu tej techniki jest KIR w ramach systemu ELIXIR. Być może instytucja ta może stanowić zaplecze organizacyjne dla pierwszego powszechnie dostępnego organu certyfikującego, zaś TELBANK może utworzyć powszechnie dostępny rejestr certyfikatów, bazując na swych usługach X.400 i X.500. Propozycje zawarte w Ustawie o podpisie cyfrowym stanu Utah mogą stanowić istotną pomoc w opracowaniu zasad działania tego typu instytucji w Polsce.

Format dokumentu elektronicznego

Należy dążyć do ujednolicenia struktury dokumentów elektronicznych, co spowoduje obniżenie kosztów i zwiększenie niezawodności oprogramowania EDI. Nie ulega wątpliwości, że preferowanym formatem powinien być standard EDIFACT.

Identyfikacja autora

W wypadku zastosowań sektorowych stosowane są najczęściej lokalne zasady ogólnej identyfikacji uczestników wymiany (np. banków lub klientów banków określanych przez numery swych rachunków bankowych). Należy jednak dążyć do jednolitej i jednoznacznej identyfikacji uniwersalnej. Jednym ze standardów który zasługuje na rozważenie jest standard adresacji zgodny z normą X.500, przyjęty m.in. w ustawie o podpisie cyfrowym stanu Utah. Jako oznaczenia kodowe mogą być wykorzystywane kody lokalizacyjne EAN.

Autoryzacja dokumentu elektronicznego

W praktyce stosuje się aktualnie dwie techniki autoryzacji dokumentów: przez użycie podpisu cyfrowego lub przez tworzenie kopii przechowywanych przez Zaufaną Trzecią Stronę. Ta pierwsza technika jest zdecydowanie bardziej skuteczna, szczególnie w Polsce gdzie jak dotychczas nie istnieją operatorzy świadczący usługi Zaufanej Trzeciej Strony.

Oprogramowanie i środki ochrony

Określenie osób odpowiedzialnych za właściwe funkcjonowanie systemu EDI i właściwą jego dokumentację jest bardzo istotnym elementem. Oprogramowanie systemów EDI powinno sprostać wymaganiom odpowiednich norm, w szczególności gdy chodzi o wymianę dokumentów w sektorze bankowym, w którym następuje transfer środków finansowych. Dlatego też należałoby wprowadzić wymóg uzyskiwania certyfikatu, dopuszczającego takie oprogramowanie do użytku. Podobnie, należy określić odpowiednie normy ochrony danych i procesu komunikacji. Należy dążyć również do certyfikacji środków ochrony wykorzystywanych w tego typu systemach. Należy jasno określać odpowiedzialność stron wymiany w wypadku fałszerstwa lub innych nadużyć. Dobrym przykładem takich regulacji jest cytowany już artykuł 4A kodeksu UCC.

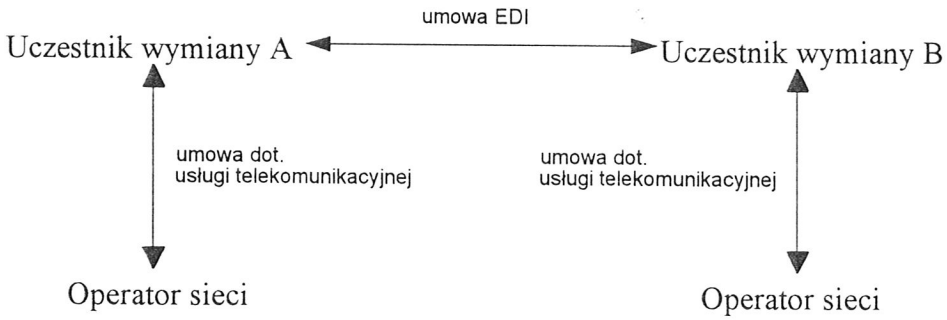
Archiwizacja dokumentów

Określenie osób odpowiedzialnych za archiwizowanie dokumentów elektronicznych i zarządzanie nimi jest równie istotne jak w odniesieniu do osób obsługujących sam system EDI. Należy postulować wprowadzenie przepisów określających właściwe przechowywanie dokumentów na

nośnikach elektronicznych. Podstawowymi cechami powinna być wierność i trwałość kopii, należy jednak wyeliminować żądania odwołujące się do określonej technologii (tak jak to ma miejsce w Ustawie o Rachunkowości). W wypadku przechowywania komunikatów autoryzowanych (np. podpisem cyfrowym), wymagania dotyczące właściwej archiwizacji stają się znacznie łatwiejsze do spełnienia.

Relacje pomiędzy uczestnikami wymiany a operatorem sieci lub innymi usługodawcami

Przy wymianie dokumentów elektronicznych istnieją w zasadzie dwie kategorie podmiotów, a mianowicie: uczestnicy wymiany (dwóch lub więcej) oraz operator usługi komunikacyjnej, pełniący rolę pośrednika (rys.2). Relacje pomiędzy uczestnikami wymiany EDI powinny być, jak to omówiono wcześniej, określone w drodze oddzielnej umowy. Należy również dążyć do tego, by operator dostosował swe usługi do specyficznych potrzeb EDI, określając ich zakres w odpowiedniej umowie z uczestnikiem wymiany. Wzajemna odpowiedzialność stron musi być tam jasno i formalnie określona.



Rys. 2. Strony biorące udział w wymianie EDI

Rozwiązania podstawowe

Przegląd i ewidencja dokumentów istotnych dla EDI, dla których istnieją zakazy lub ograniczenia w stosowaniu formy elektronicznej

Jak to wspomniano wcześniej, istniejące aktualnie zakazy dotyczą następujących podstawowych dokumentów istotnych dla EDI:

- faktur;
- dokumentów, pełniących rolę dowodów księgowych.

Lista ta jest oczywiście niepełna i powinna być uzupełniona w wyniku prac grup roboczych, związanych z poszczególnymi sektorami działalności gospodarczej i administracyjnej. W odniesieniu do potrzeb sektora bankowego, prace te w znacznej części zostały wykonane z inicjatywy NBP.

Propozycje legislacyjne w zakresie uznania elektronicznej wymiany dokumentów jako równoważnej obiegowi dokumentów papierowych

Po określeniu istotnej dla EDI grupy dokumentów, należy opracować propozycje możliwych zmian w przepisach wykonawczych, znoszące występujące ograniczenia. Zmiany te najczęściej będą dotyczyły:

- zniesienia wymagań odręcznego podpisu i związanej z tym formy papierowej dokumentu;
- zezwolenia na stosowanie formy elektronicznej dokumentu, z określeniem wymagań dotyczących zasad przesyłania i archiwizacji;
- zniesienia zakazu lub ograniczeń archiwizacji dokumentów w formie elektronicznej.

Dla potrzeb rozwiązań sektorowych, należy wykorzystać opracowane rekomendacje ogólne, określające niezbędne wymagania dotyczące ochrony komunikatów EDI, zasad ich ewidencji, archiwizacji, kopiowania w formie bezpośrednio czytelnej itp.

W miarę możliwości należy dążyć do zmian regulacji na płaszczyźnie sektorowej, jednakże nie zawsze jest to możliwe. Wydaje się, że w trzech przypadkach występuje konieczność dokonania regulacji na szczeblu ustawy:

- Niezbędna wydaje się modyfikacja aktualnie obowiązującej Ustawy o rachunkowości, mająca na celu dopuszczenie stosowania dowodów księgowych w formie elektronicznej. Dodatkowo należy określić zasady interpretacji technicznej pojęcia „trwały nośnik danych" występującego w tej ustawie.
- Niezbędna wydaje się modyfikacja aktów wykonawczych, ograniczających użycie elektronicznej faktury VAT. Ponieważ nawet w gronie krajów akceptujących elektroniczny format faktury, stosowane rozwiązania są bardzo różnorodne, należy powołać odpowiedni zespół ekspercki, który dokona ich przeglądu i oceny, oraz zaproponuje właściwe dla Polski rozwiązania.
- Należy w przypadkach koniecznych dopuścić do obrotu na prawach oryginału odpowiednio uwierzytelnioną kopię papierową dokumentów elektronicznych (każdy uwierzytelniony wydruk będzie oryginałem lub będzie istniała możliwość uwierzytelnienia w specjalny sposób tylko jednego wydruku, a wszystkie pozostałe wydruki, odpowiednio autoryzowane będą już kopiami). Tego typu regulacja jest niezbędna w przypadku, gdy dokument elektroniczny będzie występował także w obiegu zewnętrznym tzn. poza kręgiem podmiotów objętych regulacją sektorową lub umową wymiany.

Rozwiązania perspektywiczne

Jak to wynika z analizy problemów prawnych dotyczących EDI w krajach europejskich i z dotychczasowych doświadczeń polskich, podstawowym problemem związanym z elektroniczną formą dokumentu jest problem jego autoryzacji. Opracowanie technologii podpisu cyfrowego uczyniło jednak z tego zagadnienia nie tyle problem techniczny a przede wszystkim organizacyjny. Ustawa stanu Utah o podpisie cyfrowym wydaje się przełomem, który stworzył konkretne warunki administracyjne i organizacyjne, umożliwiające uczynienie z podpisu cyfrowego techniki równoważnej podpisowi odręcznemu (tu należy nadmienić, że technika weryfikacji autentyczności tylko za pomocą porównania odręcznego podpisu z wzorcem została przez

ustawodawcę amerykańskiego uznana jako całkowicie niewystarczającą w zastosowaniach bankowych - patrz uwagi do UCC4A w rozd. 1., podobnie zresztą jest i w Polsce). Taka równoważność znosi właściwie wszystkie bariery prawne ograniczające powszechne stosowanie EDI. Z tego względu taką regulację prawną należy uznać za rozwiązanie docelowe. Ponieważ są to rozwiązania nowe i jeszcze nie znane polskiemu środowisku, jako załącznik do niniejszej pracy przytoczono pełny tekst Ustawy i Ogólne zasady jej stosowania (Załącznik 3.). Poniżej zamieszczono też komentarz do rozwiązań w niej proponowanych.

Ustawa o podpisie cyfrowym stanu Utah

Celem omawianej ustawy, stanowiącej część Kodeksu stanu Utah (tytuł 46, rozdział 3 jest uregulowanie kwestii prawnych związanych z posługiwaniem się podpisem elektronicznym w działalności handlowej). Artykuł 102 ustawy wylicza cele takiej właśnie regulacji uzasadnionej gospodarczo, chodzi w niej bowiem o ułatwienie handlu poprzez wykorzystanie komunikacji elektronicznej. Ponieważ wiarogodność dokumentu potwierdza podpis pod nim umieszczony, konieczne jest zapewnienie maksymalnego bezpieczeństwa w posługiwaniu się podpisem cyfrowym. Ustawa ma więc na celu stworzenie barier ograniczających możliwość fałszowania podpisów cyfrowych i redukujących oszustwa w wymianie handlowej. Kolejnym celem jest wprowadzenie w sferze prawnej odpowiednich standardów Międzynarodowego Związku Telekomunikacji (ITU) np. X.509. Konieczne jest także wypracowanie jednolitych zasad związanych z poświadczaniem i pewnością komunikatów elektronicznych.

Podstawowymi elementami wprowadzanymi przez ustawę są:

- certyfikat, umożliwiający każdemu weryfikację prawdziwości otrzymanego podpisu cyfrowego;
- licencjonowany organ cerytyfikujący, tworzący certyfikaty na podstawie procedury certyfikacyjnej i informacji uzyskiwanej od podpisującego;
- rejestr, ogólnodostępny katalog certyfikatów.

Podpis cyfrowy musi być weryfikowany pod względem autentyczności i ważności. Temu właśnie służy certyfikat wydawany przez organ certyfikujący posiadający ważną licencję. Licencję taką wydaje Wydział Podmiotów Gospodarczych i Kodeksu Handlowego. Zajmuje się on jako organ administracyjny obsługą podmiotów prowadzących działalność gospodarczą. W innych Stanach funkcje te sprawuje sekretarz stanu. Ustawa stanowić może wzór dla innych stanów i nazwa wydziału nie jest wiążąca - nie chodzi o powołanie nowego organu, ale o przyznanie nowych kompetencji.

Organem certyfikującym ustawa nazywa organ wydający certyfikaty, od którego wymaga spełnienia określonych warunków, aby mógł otrzymać oraz utrzymać licencję. Wymagania te wiążą się z kwestiami finansów, personelu i złożeniem odpowiednich gwarancji (art.201). Specyficznym organem certyfikującym jest Wydział Urzędu, nie jest to jednak jego główna rola. Powinien on jedynie uruchamiać mechanizmy funkcjonowania infrastruktury podpisu elektronicznego. Powinien on nakreślać linię działania, która pozwoliłaby na rozszerzanie funkcjonowania tej formy podpisu.

Certyfikat jest zapisem komputerowym identyfikującym organ certyfikujący, określającym lub identyfikującym osobę, przez którą został podpisany. Musi także zawierać klucz publiczny podpisującego i podpis cyfrowy organu certyfikującego.

Podpis cyfrowy jest w ustawie definiowany jako przetworzenie komunikatu za pośrednictwem asymetrycznego kryptosystemu tak, aby osoba posiadająca komunikat wyjściowy i klucz publiczny podpisującego mogła sprawdzić, czy zastosowany klucz prywatny odpowiada kluczowi publicznemu oraz czy od momentu przetworzenia nie dokonano w komunikacie jakichkolwiek zmian.

Wszelka wymiana handlowa we współczesnym świecie opierać się musi na podstawowej zasadzie swobody umów. Posługiwanie się nią ułatwia także wdrożenie cyfrowego podpisu, ponieważ strony mogą umówić się co do ważności posługiwania się nim, tym samym eliminując nierozwiązany ustawowo problem mocy dowodowej. Dlaczego zatem, mimo takich możliwości w ramach umów między partnerami w ustawie Stanu Utah pojawia się forma certyfikatu? Otóż zgodnie z wolą ustawodawcy certyfikat służy zwiększeniu wiarogodności podpisu cyfrowego. Można zaryzykować stwierdzenie, że forma taka zastępuje, czy jest ekwiwalentem notarialnego potwierdzenia podpisu ręcznego. Certyfikat powinien wydać organ posiadający ważną licencję, niemniej jej brak nie powoduje nieważności certyfikatu, a jedynie inne konsekwencje w przypadku roszczeń związanych z wykrytymi nieprawidłowościami.

Ustawa Stanu Utah nadaje istotne konsekwencje prawne podpisowi cyfrowemu (część 4 ustawy). Stwierdza mianowicie jego równorzędność z podpisem odręcznym. Aby wymóg podpisu wynikający z przepisów prawa lub wiążący się z określonymi skutkami (w razie jego braku czynność prawna może być uznana za nieważną lub dokument będzie obciążony brakiem mocy dowodowej) został spełniony, podpis cyfrowy musi być weryfikowany przy pomocy klucza publicznego zamieszczonego w certyfikacie (ważnym i wydanym przez licencjonowany organ certyfikujący). Ponadto został on złożony w celu podpisania komunikatu, a odbiorca musi być przekonany co do ważności dokonanej czynności i legalnego stosowania prywatnego klucza. Ponieważ odbiorcy dotyczy ryzyko fałszerstwa podpisu, powinien on kierować się rozsądnym zaufaniem w danych okolicznościach, co może stanowić przedmiot postępowania w razie sporu. Dlatego ustawa przewiduje możliwość nieuznania wiarygodności podpisu cyfrowego, o czym odbiorca powinien powiadomić podpisującego wraz z podaniem uzasadnienia swojej decyzji. Jednocześnie Ustawa postuluje wprowadzenia do certyfikatu informacji o "zalecanym limicie zaufania", czyli o gwarantowanej kwocie odszkodowania, do jakiej organ certyfikujący zobowiązany jest pokryć ewentualne straty osobie która zawierzyła certyfikatowi, o ile nieprawdziwość faktów w certyfikacie wynikała z winy organu certyfikującego.

W omawianej wyżej ustawie widać wyraźnie motywy, którymi kierował się ustawodawca. We współczesnej wymianie handlowej potrzeba maksymalnych ułatwień służących szybkości dokonywania transakcji, przejrzystości dokumentów i jasno określonej odpowiedzialności. Te handlowe i zdroworozsądkowe przesłanki nie mogą jednak przesłaniać zagrożeń wiążących się z niedoskonałością przyjętych rozwiązań. Dlatego trzeba mieć na względzie ochronę interesów partnerów i handlowe bezpieczeństwo dokonywanych transakcji. Wydaje się, że na te oczekiwania odpowiada ustawa o podpisie cyfrowym, która poprzez prawne uznanie podpisu cyfrowego ułatwia komunikowanie się partnerów zgodnie z osiągnięciami techniki, a z drugiej strony poprzez system certyfikowania jako możliwości weryfikacji i potwierdzenia podpisu zapewnia właściwe bezpieczeństwo takiej wymiany.

3. Inne bariery hamujące rozwój EDI w Polsce i działania zmierzające do ich pokonania

Omawiane wcześniej korzyści jakie poszczególny użytkownik uzyska ze stosowania EDI mogą być zbyt małe, jeśli musi on pokonać istotne przeszkody organizacyjne i ponieść związane z tym nakłady.

Jak już wspomniano, wprowadzenie EDI wymaga:

- określenia struktury i znaczenia poszczególnych elementów komunikatów,
- uzgodnienia zasad wymiany komunikatów drogą teletransmisji,
- wyposażenia uczestników wymiany w odpowiednie oprogramowanie i sprzęt,
- uzgodnienia i stosowania odpowiednich środków ochrony.

Wydaje się, że w optymalnej sytuacji koszty związane z wprowadzeniem EDI powinny być ograniczone do kosztów zakupu oprogramowania i sprzętu realizującego wymianę. Oznacza to, że wszystkie pozostałe elementy powinny być określone w sposób kompleksowy w skali ogólnej.

Pomimo dotychczasowego niewielkiego zainteresowania organów państwa problematyką EDI, w Polsce ukształtowało się już silne środowisko wspierające tą technologię w sposób niezależny od rozwiązań centralnych. Do wiodących ośrodków promujących EDI należą m.inn.:

EDIPOL - instytucja, od momentu likwidacji Fundacji „Polska Eksportuje" jest silnie zaangażowana w prace ONZ na standardem EDIFACT i w promocję tego standardu w Polsce, szczególnie w zakresie polonizacji katalogów komunikatów standardowych. Dzięki niej powstała pierwsza grupa użytkowników EDI w sektorze motoryzacyjnym;

Uniwersytet Łódzki, Zakład Analizy i Projektowania Systemów - dzięki organizowanym od 1993 roku corocznie przez prof. M. Niedźwiedzińskiego Krajowym Konferencjom EDI powstała w Polsce możliwość szerokiego upowszechniania EDI i doświadczeń w jej wdrażaniu;

Instytut Logistyki i Magazynowania, Centrum Kodów Kreskowych - instytucja ta podjęła się stworzenia polskiego zbioru rekomendacji dla stosowania komunikatów standardowych w zastosowaniach handlowych, bazujących na standardzie EANCOM

Francusko-Polska Wyższa Szkoła Nowych Technik Informatyczno-Komunikacyjnych, Centrum Badań i Analiz (ostatnio przekształcone w Instytut Technik Telekomunikacyjnych i Informatycznych) - zespół ekspertów tej instytucji dokonał analizy zasad wdrażania EDI w środowisku bankowym i opracował na potrzeby NBP szereg rozwiązań wzorcowych. Wraz z ILiM realizuje Centrum Informacji o Towarach, będący pierwszą krajową próbą wprowadzenia ogólnodostępnego systemu EDI w handlu;

Centrum EDI - Polska - organizacja zapewniająca promocję i tworząca forum wymiany poglądów i doświadczeń związanych z wdrażaniem EDI, powstała na bazie sekcji PLODETTE oddziału warszawskiego SIMP.

3.1 Bariery organizacyjne

Właściwe rekomendacje dotyczące struktury i interpretacji elementów komunikatów EDI

Chociaż początkowo systemy EDI powstawały jako systemy zamknięte, wykorzystujące standardy proponowane przez uczestnika dominującego w danym systemie wymiany, to obecnie rozwiązanie takie należy uznać za anachroniczne i nieefektywne. Wynika to z istnienia UN/EDIFACT - dojrzałego, uniwersalnego standardu opracowanego w ramach ONZ . Jego struktura jest określona normą międzynarodową (ISO 9735, polski odpowiednik to PN-92/T-20091). Jak to już wspomniano wcześniej, zarówno na poziomie Unii Europejskiej (przykładem jest tu system EDIBOP) jak i w poszczególnych krajach standard ten jest powszechnie wdrażany i stosowany. Nawet tak związana dotychczas z własnym, wewnętrznym standardem komunikatów instytucja jak S.W.I.F.T (ponad 3 000 użytkowników, ponad 1,2 miliona komunikatów dziennie) od 1991 prowadzi prace nad umożliwieniem wymiany komunikatów EDIFACT w swej sieci (projekt SWIFT EDI). W Polsce przyszli użytkownicy EDI (zarówno z grona niezależnych podmiotów gospodarczych jak i instytucji państwowych) powinni być stale informowani o istnieniu tego standardu i jego zaletach. Jednocześnie Polska powinna być stale obecna w gronie państw pracujących nad tym standardem w ramach grupy WP.4 ONZ. W tej dziedzinie sytuacja nie tylko nie ulega poprawie, ale wręcz pogarsza się.

Jak już wspomniano, standard EDIFACT jest opracowywany w sposób uniwersalny i w odniesieniu do potrzeb międzynarodowego grona użytkowników. W kontekście poszczególnych zastosowań branżowych, szczególnie dla systemów krajowych konieczna jest adaptacja wzorców ogólnych do specyficznych potrzeb. Ten proces, określany jako definiowanie substandardów komunikatów wzorcowych i podręczników ich użytkowania (MIG - Message Implementation Guidelines) powinien być w Polsce jak najszybciej zakończony. Aktualnie związane z tym prace realizowane są w 3 ośrodkach: EDIPOL opracował i wdraża grupę substandardów dla sektora przemysłu, Instytut Logistyki i Magazynowania adaptuje dla potrzeb handlu substandardy zalecane przez EANCOM, a grupa tematyczna wyłoniona przez Związek Banków Polskich, przy współpracy z CEDIP i EDIPOL opracowuje substandardy dla potrzeb bankowości. Prace te przebiegają zbyt wolno i nie są w odpowiedni sposób wspomagane finansowo. Dodatkowo powinno zostać powołane ogólnokrajowe ciało koordynujące, czuwające nad ogólną zgodnością tworzonych substandardów (np. na wzór EDIFRANCE we Francji). Rolę taką mogłaby pełnić Rada ds Teleinformatyki lub CEDIP (Centrum EDI - Polska), który aktualnie pełni taką rolę w stosunku do sektora przemysłowego. Jednocześnie, zgodnie ze swym celem statutowym, Rada ds Teleinformatyki powinna oceniać wszelkie inicjatywy ustawodawcze pod kątem ich zgodności z ogólną promocją technologii EDI.

CEDIP jako jedno z głównych swych zadań przyjął promocję, upowszechnianie i wymianę doświadczeń we wdrażaniu EDI. W ramach tej działalności, przy wsparciu finansowym z funduszy Phare rozpoczął organizację 8 regionalnych konferencji, których celem jest jak najszersza popularyzacja EDI w Polsce.

Operatorzy usług dodanych, ułatwiających wymianę komunikatów drogą teletransmisji

Powszechną w krajach rozwiniętych praktyką jest oferowanie usług dotyczących wymiany komunikatów pomiędzy uczestnikami systemów EDI przez zewnętrznych usługodawców. Są to tzw. usługi dodane (VAN - value added networks), towarzyszące powszechnym lub prywatnym sieciom teletransmisyjnym. Jednym z najbardziej znanych na świecie operatorów tego typu usługi jest towarzystwo S.W.I.F.T (Society for Worldwide Interbank Financial Telecomunication), będące operatorem własnej, ogólnoświatowej sieci SWIFT. Jest to system wyspecjalizowany dla obsługi wymiany komunikatów pomiędzy instytucjami finansowymi. Przykładami sieci ogólnodostępnych są sieci IBM GN (IBM Global Network), GEIS (General Electric Information Services), Amadeus, Allegro i wiele innych (może wymienić tu należy również czeską firmę EDITEL CZ). Operatorzy usług dodanych biorą na siebie obsługę klienta (zainstalowanie terminala i modułu wymiany), podłączenie do sieci telekomunikacyjnej, ewentualną konwersję postaci komunikatu, archiwizację komunikatów i oczywiście ich przesłanie do adresata (za pomocą własnej sieci lub poprzez publiczne sieci transmisji danych). W Polsce dwóch operatorów Bankowe Przedsiębiorstwo Telekomunikacyjne TELBANK i Telekomunikacja Polska S.A. stworzyło pewne ułatwienia dla wymiany EDI, udostępniając usługę wymiany poczty elektronicznej w standardzie X.400 (a TP S.A. przygotowuje również wdrożenie standardu X.435 oraz z dostępem do usług globalnego katalogu X.500). Są to jednak jedynie usługi elementarne, które dla wygody użytkownika powinny być znacznie bardziej rozbudowane. EDIPOL utworzył też ostatnio ośrodek usług dodanych VANPOL dla potrzeb sektora przemysłowego. Usługi te rozwinęłyby się znacznie, gdyby organy administracji państwowej i samorządowej wprowadziły systemy EDI dla własnych potrzeb, istotnie poszerzając krąg zainteresowanych tą technologią.

Instytucje certyfikujące związane z EDI

Dematerializacja dokumentów i wykorzystanie systemów teletransmisji wprowadzają pewne zagrożenia i w interesie użytkowników muszą być one powiązane z wykorzystaniem właściwych środków ochrony. Te środki to ochrona bezpośrednia komunikatów w trakcie transmisji, ochrona ich poufności, ochrona sieci teletransmisyjnych przed awariami itp. Instytucje nadrzędne, których dotyczą wymieniane dokumenty elektroniczne (służby podatkowe, celne, bankowość) również pragną zmniejszyć ryzyko nieautoryzowanych modyfikacji komunikatów w trakcie generacji lub archiwizacji. Z tego powodu w wielu krajach powołuje się odpowiednie organy dokonujące weryfikacji stosowanych systemów EDI jak i rekomendujące stosowanie określonych środków ochrony. Tego typu ocenę prowadzi się przede wszystkim w stosunku do systemów finansowo-księgowych wykorzystujących fakturę w postaci zdematerializowanej. Przykładem zaś standaryzacji środków ochrony w EDI może być francuski standard bankowy ETEBAC 5. Organy te mogłyby powstać w Polsce np. przy współpracy ze Stowarzyszeniem Księgowych w Polsce.

W przypadku powszechnego użycia podpisu cyfrowego jako środka weryfikacji wiarygodności dokumentów elektronicznych pojawia się konieczność udostępniania wszystkim zainteresowanym tzw. „kluczy publicznych" użytkowników, za pomocą których można potwierdzić autentyczność podpisu. Najwygodniejszym rozwiązaniem jest udostępnianie tych

kluczy drogą teletransmisji, a to wymaga stworzenia odpowiednich centrów dystrybucji (rejestrów kluczy) i przechowywania ich w formie uniemożliwiającej ich modyfikację. Tak forma nosi nazwę certyfikatu klucza publicznego a tworzenie certyfikatów powinno być powierzone odpowiednim, zaufanym organom. W Polsce Telekomunikacja Polska S.A. uruchomiła usługę globalnie dostępnego katalogu w standardzie X.500, która może służyć do przechowywania certyfikatów. Brak jest jednak powszechnie dostępnych organów certyfikujących (chociaż istnieją one już dla potrzeb zamkniętych grup użytkowników - np. dla systemu ELIXIR KIR S.A.).

3.2 Bariery techniczne

Ostatnią, ale nie najmniej ważną barierą jaką musi pokonać użytkownik EDI jest zakup odpowiedniego sprzętu i oprogramowania. W odniesieniu do sprzętu sytuacja jest w miarę dobra i ulega stałej poprawie. Dostępność sieci telekomunikacyjnych (szczególnie po ostatnich modernizacjach sieci POLPAK) można uznać za zadawalającą. Postęp jaki dokonuje się w zakresie urządzeń teletransmisyjnych wykorzystujących standardową, komutowaną sieć telefoniczną spowodował, że są to już urządzenia stosunkowo tanie i jednocześnie zapewniające wystarczającą dla zastosowań EDI szybkość transmisji. Wydaje się, że za podstawową barierę techniczną można uznać brak polskich modułów programowej obsługi EDI, za wyjątkiem zastosowań związanych z elektroniczną bankowością i przemysłem. Ten brak wynika prawdopodobnie z niewielkiego na nie popytu, a to wynika z kolei z braku szerokiego programu promocji EDI i wykorzystania tej techniki w tworzonych centralnych systemach wymiany danych.

Załącznik 1.

Wzór umowy EDI proponowany przez Komisję Gospodarczą ONZ ds. Europy

Organizacja Narodów Zjednoczonych E

Rada Gospodarczo-Społeczna [1]

DOSTĘP OGRANICZONY
HANDEL /WP.4 / R.1133
17 stycznia 1995 r.
TYLKO WERSJA ANGIELSKA

KOMISJA GOSPODARCZA ONZ DS. EUROPY

KOMITET DS. ROZWOJU HANDLU
Grupa Robocza ds. Upraszczania
Międzynarodowych Procedur Handlowych

(Pozycja nr 12 we wstępnym porządku Posiedzenia Ekspertów ds. Składników Danych i Automatycznej Wymiany Danych (G.E.1) Sesja nr 51, 21-22 marca 1995 r. oraz Pozycja nr 9 we wstępnym porządku Posiedzenia Ekspertów ds. Procedur i Dokumentacji (G.E.2) Sesja nr 51, 23 marca 1995 r.

WSTĘPNA PROPOZYCJA UN/ECE

HANDLOWE WYKORZYSTANIE UMÓW O WYMIANIE WZAJEMNEJ W ZAKRESIE ELEKTRONICZNEJ WYMIANY DANYCH

##########

Raport przedłożony przez Sprawozdawców Prawnych *

* Niniejszy dokument jest reprodukowany w formie, w jakiej został otrzymany przez sekretariat.

GE. 95 - 30081

WSTĘPNA PROPOZYCJA UN/ECE

HANDLOWE WYKORZYSTANIE UMÓW O WYMIANIE WZAJEMNEJ W ZAKRESIE ELEKTRONICZNEJ WYMIANY DANYCH

##########

(Wersja wstępna przedłożona przez Sprawozdawców Prawnych)

1. Niniejszy dokument zostaje przedłożony na podstawie Projektu nr 4.1 w ramach Programu Działania dotyczącego Handlowych i Prawnych Aspektów Rozwoju Handlu, przyjętego przez Grupę Roboczą ds. Upraszczania Międzynarodowych Procedur Handlowych, a przedstawionego w raporcie HANDEL/WP.4/R.697.

2. W ramach tego programu, przedstawionego w raporcie HANDEL/WP.4/R.697, "Projekt nr 4.1: Umowy o Wzajemnej Wymianie Danych" w części stanowił, co następuje:

> "4.1.1 Cel
> Zapewnić rozsądne ujednolicenie umów o wymianie wzajemnej i opracować wersję do opcjonalnego wykorzystania, akceptowaną przez społeczność międzynarodową.
> .....
> 4.1.3 Opis projektu
> opracować umowę o wymianie wzajemnej (do wykorzystania w całości), która będzie rekomendowana na szczeblu międzynarodowym do opcjonalnego wykorzystania."

3. Niniejsza Propozycja zawiera Modelową Umowę o Wymianie Wzajemnej w Zakresie Międzynarodowego Komercyjnego Korzystania z Elektronicznej Wymiany Danych, przedstawioną w Załączniku A.

I. Wcześniejsze prace

4. W 1987 r., pracując wspólnie z Grupą Roboczą, Międzynarodowa Izba Handlowa [*ang.* ICC] opracowała i opublikowała Ujednolicone Reguły Postępowania Przy Wymianie Danych Handlowych z Wykorzystaniem Teletransmisji (Reguły UNCID; Publikacja ICC nr 452). Celem Reguł UNCID było uproszczenie wymiany danych handlowych

przekazywanych za pomocą teletransmisji przez określenie uznanych reguł postępowania między stronami prowadzącymi taką wymianę.

5. Publikacja Reguł UNCID potwierdziła znaczenie, jakie dla handlu międzynarodowego ma występowanie między partnerami handlowymi pewnych umów dotyczących korzystania z automatycznych technik przetwarzania danych.

6. Reguły UNCID otwarcie stanowiły, iż ich postanowienia, jeśli polegać na nich, muszą być włączone do konkretnych umów obowiązujących pomiędzy prowadzącymi wymianę partnerami handlowymi. W rezultacie organizacje narodowe, stowarzyszenia i agendy administracji publicznej opracowały wiele różnorodnych modelowych umów o wymianie wzajemnej.

7. Biorąc swój początek z różnych kultur i systemów prawnych, istniejące umowy modelowe częstokroć prezentowały różne zagadnienia lub różne sposoby podejścia do podobnych zagadnień. Zróżnicowanie umów o wymianie wzajemnej, choć być może umowy te zaspokajają krajowe lub lokalne wymogi handlowe, powoduje, że nie mają one wymiaru międzynarodowego, co jest wymogiem stawianym przez użytkowników EDI [*ang. elektroniczna wymiana danych*], którzy dokonują transgranicznej wymiany komunikatów.

8. Rozpoczęto wysiłki w celu opracowania bardziej ujednoliconych umów o wymianie wzajemnej, jak na przykład niedawne zalecenie Komisji Europejskiej, aby korzystać z Europejskiej Modelowej Umowy EDI. Opracowanie prawdziwie międzynarodowej modelowej umowy o wymianie wzajemnej zostało uznane za cel główny Programu Działania, o którym mowa w paragrafie 1 powyżej.

9. Niedawne prace Komisji Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego, zmierzające do opracowania modelowych zapisów ustawowych dotyczących użycia EDI w handlu międzynarodowym — które to prace zostaną przedstawione Komisji do zaopiniowania w lipcu 1995 r. — otwarcie przewiduje, iż w rzeczywistości partnerzy handlowi mogą na mocy porozumienia pragnąć zróżnicować skutek prawny takich zapisów ustawowych.

10. Również w pracach Grupy Roboczej nad zdefiniowaniem i zrozumieniem istoty międzynarodowej transakcji handlowej (jak odzwierciedla to raport HANDEL/WP.4/R.971 oraz inne odnośne dokumenty) podkreślono liczbę relacji handlowych, w których można

wykorzystać EDI, a co za tym idzie, liczbę sytuacji, w których umowy o wymianie wzajemnej mogą okazać się potrzebne.

II. Opracowanie Umowy Modelowej

11. Niniejsza propozycja została opracowana przy współpracy i zaangażowaniu Zespołu Sprawozdawców Prawnych zgodnie z Wewnętrzną Organizacją i Procedurami Operacyjnymi, ustanowionymi na potrzeby tej organizacji w raporcie HANDEL/WP.4/R.1071. Organizacje międzynarodowe takie, jak ICC i UNCITRAL były reprezentowane na posiedzeniach, w trakcie których opracowano i upowszechniono projekty Umowy Modelowej.

12. W trakcie przygotowywania Umowy Modelowej rozpatrzono ponad 20 różnych istniejących, a opracowanych wcześniej, wzorcowych umów o wymianie wzajemnej oraz zapewniono sobie ścisłą współpracę ekspertów technicznych związanych z pracami nad UN/EDIFACT.

13. W celu zapewnienia zgodności niniejszej Propozycji z poprzednimi pracami, zostały rozpatrzone wcześniejsze Propozycje Grupy Roboczej, jak również propozycje lub podobne inicjatywy innych organizacji międzynarodowych związanych z upraszczaniem i ujednolicaniem międzynarodowych procedur handlowych. Przedkładając niniejszą Propozycję do akceptacji, Sprawozdawcy Prawni wyrażają przekonanie, że jest ona zgodna z poprzednimi propozycjami w tym zakresie i że realizuje ich cele.

14. Udostępniając podmiotom gospodarczym aktywnym w handlu międzynarodowym modelową wersję umowy o wymianie wzajemnej — do wykorzystania w skali globalnej zgodnie ze standardami UN/EDIFACT — Grupa Robocza realizuje zadanie ujednolicenia, uproszczenia i racjonalizacji najbardziej zasadniczej procedury handlu międzynarodowego, jaką jest komunikowanie się partnerów handlowych. Chociaż zalecane, warunki modelowej umowy o wymianie wzajemnej nie są jednakże obowiązujące. Partnerzy handlowi zachowują swobodę zmiany warunków każdej umowy o wymianie wzajemnej, ku swojemu obopólnemu zadowoleniu, lub mogą też w ogóle nie zawierać umowy o wymianie wzajemnej.

III. Zakres

15. Niniejsza Propozycja propaguje użycie umów o wymianie wzajemnej między partnerami handlowymi, którzy w ramach międzynarodowych transakcji handlowych korzystają z Elektronicznej Wymiany Danych.

IV. Obszar zastosowań

16. Niniejsza Propozycja koncentruje się na partnerach handlowych, którzy w ramach międzynarodowych transakcji handlowych korzystają z Elektronicznej Wymiany Danych. Może być ona również istotna dla władz administracyjnych, włączając w to na przykład urzędy statystyczne, lub dla ciał zajmujących się ułatwianiem działalności handlowej, w ich wysiłkach zmierzających do racjonalizacji oraz ujednolicenia procedur i procesów informatycznych.

17. Chociaż stworzona na użytek umów dwustronnych między dwoma parterami handlowymi, Modelowa Umowa o Wymianie Wzajemnej, po dostosowaniu, może z łatwością być wykorzystywana w relacjach wielostronnych takich, jak stowarzyszenie czy też środowisko handlowe.

V. Zalecenia

18. Opierając się na powyższych przesłankach, Komisja Gospodarcza Organizacji Narodów Zjednoczonych ds. Europy zaleca, aby:

1. Międzynarodowa społeczność użytkowników EDI, włączając w to podmioty gospodarcze, które w ramach międzynarodowych transakcji handlowych decydują się na korzystanie z Elektronicznej Wymiany Danych, korzystała z umów o wymianie wzajemnej w celu podniesienia bezpieczeństwa prawnego swoich kontaktów handlowych oraz użytkowania EDI.

2. Modelowa Umowa o Wymianie Wzajemnej w Zakresie Międzynarodowego Komercyjnego Korzystania z Elektronicznej Wymiany Danych była aprobowana przy negocjowaniu i zawieraniu umów o wymianie wzajemnej.

3. Modelowa Umowa o Wymianie Wzajemnej w Zakresie Międzynarodowego Komercyjnego Korzystania z Elektronicznej Wymiany Danych, w formie przedstawionej w raporcie HANDEL/WP.4/R.1120, została wpisana do Części 3 Rejestru Wymiany Danych Handlowych Organizacji Narodów Zjednoczonych (UN/TDID) oraz stała się częścią zaleceń dotyczących UN/EDIFACT.

4. Kraje członkowskie Organizacji Narodów Zjednoczonych wzięły pod rozwagę warunki i postanowienia Modelowej Umowy o Wymianie Wzajemnej przy wprowadzaniu zmian w ustawodawstwie i przepisach tak, aby zmiany te były zgodne z

intencjami i praktykami handlowymi, które stanowią istotę Modelowej Umowy o Wymianie Wzajemnej.

5. Kraje członkowskie Organizacji Narodów Zjednoczonych mogłyby w znacznym stopniu przyczynić się do podwyższenia bezpieczeństwa prawnego przy korzystaniu z EDI poprzez propagowanie — za pomocą programów oświatowych, wysiłków edukacyjnych i innych pokrewnych działań — dostępności i użyteczności Modelowej Umowy o Wymianie Wzajemnej, jak i komercyjnych praktyk handlowych związanych z handlem międzynarodowym a zgodnych z wcześniejszymi zaleceniami.

6. Przy projektowaniu i realizacji zastosowań EDI do celów administracyjnych związanych z międzynarodowymi transakcjami handlowymi, instancje i organy administracyjne — choć mają własne konkretne wymagania, które należy wziąć pod rozwagę — powinny ocenić i uwzględnić coraz powszechniejsze komercyjne zastosowanie umów o wymianie wzajemnej, jak i warunki i praktyki handlowe zawarte w Modelowej Umowie o Wymianie Wzajemnej.

ZAŁĄCZNIK A

KOMISJA GOSPODARCZA
ORGANIZACJI NARODÓW ZJEDNOCZONYCH DS. EUROPY

MODELOWA UMOWA O WYMIANIE WZAJEMNEJ W ZAKRESIE MIĘDZYNARODOWEGO KOMERCYJNEGO KORZYSTANIA Z ELEKTRONICZNEJ WYMIANY DANYCH

SPIS TREŚCI

PRZEDMOWA

Modelowa Umowa o Wymianie Wzajemnej w Zakresie Międzynarodowego Komercyjnego Korzystania z Elektronicznej Wymiany Danych została opracowana jako część projektu w ramach Programu Działania dotyczącego Prawnych i Handlowych Aspektów Elektronicznej Wymiany Danych, przyjętego przez Grupę Roboczą ds. Upraszczania Międzynarodowych Procedur Handlowych Komisji Gospodarczej Organizacji Narodów Zjednoczonych ds. Europy ("WP.4") w 1991 r. Program ten przedstawiony jest w Dokumencie Organizacji Narodów Zjednoczonych Nr HANDEL/WP.4/r.697. Program kładzie nacisk na te zagadnienia prawne, które można łatwo zdefiniować i stawia sobie za cel opracowanie wytycznych dotyczących tych zagadnień prawnych oraz wskazanie właściwych rozwiązań w formie instrumentów i narzędzi prawnych lub zmian w praktykach handlowych.

Modelowa Umowa o Wymianie Wzajemnej jest rezultatem jednego z głównych projektów realizowanych w ramach Programu. Celem tego projektu jest zapewnienie właściwego ujednolicenia umów o wymianie wzajemnej używanych w handlu międzynarodowym oraz opracowanie wersji umowy do dobrowolnego wykorzystania i która będzie akceptowana w skali międzynarodowej. Na mocy procedur operacyjnych grupy WP.4, zaleca się, aby wszystkie podmioty prowadzące komercyjną działalność handlową i pragnące korzystać w handlu międzynarodowym z Elektronicznej Wymiany Danych wzięły pod uwagę Modelową Umowę o Wymianie Wzajemnej.

Modelowa Umowa o Wymianie Wzajemnej została przygotowana przez grupę ekspertów z zakresu prawa oraz pokrewnych dziedzin, posiadających wiedzę i doświadczenie w sferze EDI i handlu międzynarodowego. Eksperci ci, reprezentujący wiele krajów z całego świata, są regularnie zwoływani pod auspicjami grupy WP.4, za pośrednictwem Zespołu Sprawozdawców Prawnych, który został zorganizowany przez dwóch Sprawozdawców Prawnych wybranych przez członków grupy WP.4. Niniejsza praca, zrealizowana przy ścisłej współpracy innych zespołów ekspertów z dziedziny EDI, odzwierciedla interdyscyplinarne podejście do tematu, co jest nieodzowne w zakresie EDI. Bierze ona pod rozwagę także podobieństwa i różnice występujące między różnorodnymi systemami prawnymi.

[Marzec 1995]

WPROWADZENIE DO UMÓW O WYMIANIE WZAJEMNEJ

Czym jest umowa o wymianie wzajemnej?

Umowa o wymianie wzajemnej zawierana jest pomiędzy partnerami handlowymi starającymi się ustalić reguły, które zostaną przez nich przyjęte w zakresie Elektronicznej Wymiany Danych (EDI). Elektroniczna Wymiana Danych jest elektronicznym przekazywaniem z komputera do komputera transakcji handlowych i dyspozycji wykonawczych z wykorzystaniem uzgodnionego standardu w zakresie formatu danych dotyczących transakcji i komunikatów. Umowa precyzuje także funkcje i odpowiedzialność prawną poszczególnych partnerów handlowych w odniesieniu do transmisji, odbioru i przechowywania komunikatów elektronicznych. Ze względu na różnice występujące w handlowym wykorzystaniu EDI, omówienie tych zagadnień w sytuacji, gdy odnoszą się one do nowej sfery handlu, jaką jest obrót elektroniczny, zmniejsza niepewność prawną, jaka

mogłaby zrodzić się w wyniku elektronicznej wymiany handlowej i podnosi zakres pewności, z jaką technologia ta jest stosowana.

Dlaczego opracowuje się i korzysta z umów o wymianie wzajemnej?

EDI rozwija się gwałtownie jako skuteczne narzędzie handlowe w zakresie handlu międzynarodowego. Wykorzystanie EDI do celów gospodarczych i administracyjnych jest już praktyką powszechnie stosowaną w wielu ważnych gałęziach gospodarki w Europie, Ameryce Północnej, Australii i Nowej Zelandii oraz w Azji.

Coraz powszechniejsze wykorzystanie EDI w sposób fundamentalny zmienia międzynarodowe praktyki handlowe przez zastąpienie tradycyjnych dokumentów pisemnych odpowiednikami elektronicznymi. Zamiast wysyłania i otrzymywania oryginałów sporządzonych dokumentów wraz ze złożonymi na nich odręcznie podpisami, kontrahenci przekazują za pomocą środków elektronicznych usystematyzowane dane handlowe z jednego systemu komputerowego do drugiego, przy coraz powszechniejszym wykorzystaniu podpisów elektronicznych.

Jednakże występują poważne różnice co do zakresu, w jakim prawodawstwo krajowe i międzynarodowe akceptuje fakt, iż komunikat elektroniczny może realizować te same funkcje co dokument w formie pisemnej. Wiele konwencji i umów związanych z handlem międzynarodowym nie przewiduje możliwości wykorzystania EDI. Wynika to przede wszystkim z faktu, że EDI po prostu nie istniała w momencie, gdy owe konwencje i umowy międzynarodowe były przygotowywane, a konieczne poprawki jeszcze nie zostały wprowadzone. Również wiele krajowych systemów prawnych rodzi niepewność odnośnie prawnej ważności transakcji realizowanych w oparciu o EDI lub też jest niespójnych w zakresie traktowania przez nie nowych technologii. Ponadto niewiele sądów miało sposobność orzekania na temat ważności elektronicznych dokumentów, komunikatów lub podpisów.

Od początków zastosowania EDI tego typu umowy prawne były stosowane przez przedsiębiorstwa działające w różnych gałęziach gospodarki, w różnych regionach ekonomicznych czy też geograficznych oraz na różnych poziomach zaawansowania technologicznego.

Dlaczego przedsiębiorstwo powinno korzystać z umowy o wymianie wzajemnej?

Wobec braku jasnych przepisów i zasad prawnych regulujących to zagadnienie, umowa o wymianie wzajemnej udostępnia przedsiębiorstwu gotowy sposób formalnego ułożenia relacji z jego partnerami handlowymi w zakresie EDI.

Na przykład, Umowa Modelowa, jeśli realizowana jest w sposób właściwy, dąży do tego, aby komunikaty EDI miały wiążący skutek prawny niezależnie od różnych krajowych systemów prawnych. Cel ten realizowany jest przez odniesienie się do wszystkich podstawowych zagadnień prawnych, które muszą być uwzględnione zanim przedsiębiorstwo wykorzysta EDI do komunikowania się ze swoimi krajowymi czy też zagranicznymi partnerami handlowymi. A zatem, gdy przedsiębiorstwo podejmie już decyzję o wykorzystaniu EDI, będzie potrzebowało porozumienia ze swoimi partnerami handlowymi w zakresie przynajmniej następujących zagadnień, których priorytety będą różne w zależności od konkretnych potrzeb tego przedsiębiorstwa:

a) dobór komunikatów EDI, ich standardów oraz metod komunikacji;

b) odpowiedzialność za zagwarantowanie efektywnej obsługi i serwisu sprzętu, oprogramowania i usług;

c) procedury wprowadzania wszelkich zmian w systemie, które to zmiany mogłyby obniżyć zdolność partnerów handlowych do komunikowania się;

d) procedury i usługi w zakresie bezpieczeństwa;

e) sytuacje, w których komunikaty EDI wywołują skutek prawny;

f) funkcje i umowy z wszelkimi osobami trzecimi - usługodawcami;

g) procedury postępowania w przypadku pomyłek technicznych;

h) potrzeba (jeśli występuje) poufności;

i) odpowiedzialność prawna w przypadku jakiegokolwiek opóźnienia lub niedotrzymania uzgodnionych zobowiązań w zakresie komunikacji EDI;

j) przepisy prawa regulujące wymianę komunikatów EDI oraz uzgodnienia między umawiającymi się stronami;

k) metody rozwiązywania wszelkich możliwych sporów.

Umowa o wymianie wzajemnej między partnerami handlowymi jest porozumieniem całkowicie dobrowolnym. Jednakże, jak pokazuje całkiem obszerna lista powyżej, nim przedsiębiorstwo zacznie wykorzystywać EDI do komunikowania się z partnerami handlowymi, będzie musiało rozważyć wiele bardzo ważnych zagadnień. Umowa o wymianie wzajemnej stanowi usystematyzowaną formułę rozpatrywania i formalnego rozwiązania tych podstawowych problemów.

Brak dobrej i wiążącej umowy w zakresie reguł regulujących łączność EDI w przedsiębiorstwie stwarza ryzyko zbędnych i kosztownych sporów pomiędzy partnerami handlowymi, a w sytuacji skrajnej może doprowadzić nawet do postępowania sądowego.

Jakie modelowe umowy o wymianie wzajemnej istnieją?

Zarówno do wykorzystania regionalnego jak i krajowego opracowano dużą liczbę umów o wymianie wzajemnej. Obejmują one umowy o wymianie wzajemnej opublikowane przez krajowe organizacje EDI, profesjonalne stowarzyszenia prawników i agendy administracji publicznej. W chwili ukazania się niniejszej publikacji nie istnieje jednakże żaden inny światowy wzorzec oprócz Modelowej Umowy o Wymianie Wzajemnej.

W sytuacji braku istniejącej umowy modelowej w odniesieniu do międzynarodowych komercyjnych transakcji handlowych, istniało również przekonanie, że sprzeczności pomiędzy istniejącymi krajowymi lub regionalnymi umowami modelowymi ograniczały zastosowanie EDI w handlu międzynarodowym. Różne umowy modelowe, do których odwołał się Zespół Sprawozdawców Prawnych różniły się znacznie swoją obszernością, różniły się merytorycznie, a także pod względem treści. Modelowa Umowa o Wymianie Wzajemnej dąży do kompromisu i znalezienia wspólnego mianownika, w celu ułatwienia korzystania z EDI w handlu międzynarodowym.

Jak dalece Modelowa Umowa o Wymianie Wzajemnej różni się od innych umów modelowych?

Niniejsza Modelowa Umowa o Wymianie Wzajemnej jest szczególnie przydatna w handlu międzynarodowym. Została opracowana z uwzględnieniem różnic występujących między krajowymi systemami prawnymi i oferuje praktyczne sposoby przezwyciężania wszelkich trudności, jakie mogą z tego faktu wynikać. Umowa została pomyślana jako narzędzie wystarczająco elastyczne, aby sprostać wymaganiom tych wszystkich sektorów

gospodarki, jakie uczestniczą w handlu międzynarodowym. Być może użytkownicy uznają ją także za instrument przydatny przy opracowywaniu umów o wymianie wzajemnej w odniesieniu do czysto krajowej lub regionalnej działalności handlowej prowadzonej z wykorzystaniem EDI.

Jeśli przedsiębiorstwo zdecyduje się użyć wzoru umowy międzynarodowej przedstawionej w niniejszej Umowie o Wymianie Wzajemnej jako podstawy do określenia przepisów regulujących zastosowanie EDI w swoich relacjach z partnerami handlowymi, to może mieć ono pewność, że wybrało narzędzie, które:

- odnosi się do powszechnie przyjętych zagadnień prawnych, które powstają na gruncie komercyjnego wykorzystania EDI w handlu międzynarodowym;
- stanowi silny fundament prawny i praktyczny do podejmowania i rejestrowania niezbędnych decyzji handlowych.

MODELOWA UMOWA O WYMIANIE WZAJEMNEJ W ZAKRESIE MIĘDZYNARODOWEGO KOMERCYJNEGO KORZYSTANIA Z ELEKTRONICZNEJ WYMIANY DANYCH

Niniejsza publikacja Modelowej Umowy o Wymianie Wzajemnej składa się z trzech części:

MODELOWA UMOWA O WYMIANIE WZAJEMNEJ.

KOMENTARZ, KTÓRY ZAWIERA PEWNE WYJAŚNIENIA I DODATKOWE WYTYCZNE.

ARKUSZ KONTROLNY DO ZAŁĄCZNIKA TECHNICZNEGO, PODSUMOWUJĄCY WYMOGI W ZAKRESIE TREŚCI ZAŁĄCZNIKA TECHNICZNEGO, KTÓRY ZOSTAJE DOŁĄCZONY DO KAŻDEJ RZECZYWISTEJ UMOWY.

Modelowa Umowa o Wymianie Wzajemnej została opracowana do użytku w relacjach między prowadzącymi komercyjną wymianę partnerami handlowymi. Wykorzystanie w organach administracji lub urzędach lub w transakcjach z indywidualnym klientem, wymagać będzie stosownych zmian.

MODELOWA UMOWA O WYMIANIE WZAJEMNEJ

NINIEJSZA UMOWA O WYMIANIE WZAJEMNEJ ("Umowa") zostaje zawarta przez i pomiędzy {wstawić nazwy i adresy stron} (zwanych dalej "stronami") dnia _____ , 19___ r. Na mocy niniejszej umowy strony, wyrażając intencję podporządkowania się jej postanowieniom, niniejszym uzgadniają co następuje:

SEKCJA 1: ZAKRES I STRUKTURA

1.1 Zakres

Niniejsza Umowa reguluje wszelki elektroniczny transfer Komunikatów pomiędzy stronami. Za wyjątkiem przypadków jasno określonych, niniejsza Umowa nie reguluje żadnych innych relacji, umownych czy też nie, w kontekście których Komunikaty są przekazywane. Komunikat oznacza dane zorganizowane zgodnie ze Standardami UN/EDIFACT, jak określono to w Sekcji 2.

1.2 Załącznik Techniczny

Dołączony Załącznik Techniczny zawiera uzgodnione przez strony warunki techniczne w odniesieniu do określonych wymogów technicznych i proceduralnych. W przypadku wystąpienia sprzeczności między postanowieniami niniejszej Umowy a Załącznikiem Technicznym, obowiązują postanowienia niniejszej Umowy.

SEKCJA 2: KOMUNIKACJA I DZIAŁANIE

Strony będą przekazywały Komunikaty zgodnie z następującymi postanowieniami:

2.1 Standardy

"Standardy UN/EDIFACT" są standardami, które zostały ustanowione na potrzeby Elektronicznej Wymiany Danych (łącznie z odnośnymi zaleceniami), w formie zatwierdzonej i opublikowanej w Rejestrze Wymiany Danych Handlowych Organizacji Narodów Zjednoczonych (UN/TDID). Strony będą korzystały z tych wersji Standardów UN/EDIFACT, które określono w Załączniku Technicznym.

2.2 Działanie systemu

Każda ze stron będzie testować i zapewniać serwis w odniesieniu do własnego sprzętu, oprogramowania i usług koniecznych dla efektywnego i niezawodnego przekazywania i odbierania Komunikatów.

2.3 Zmiany w systemie

Żadna ze stron, bez uprzedniego doręczenia powiadomienia o planowanej zmianie, nie będzie wprowadzać w funkcjonowaniu systemu jakichkolwiek zmian, które obniżyłyby wzajemną zdolność stron do komunikowania się zgodnie z intencją niniejszej Umowy.

2.4 Komunikowanie się

Strony precyzyjnie określą w Załączniku Technicznym metody komunikowania się, włączając w to wymagania w zakresie telekomunikacji lub korzystania ze świadczeń usługodawców - osób trzecich.

2.5 Procedury i usługi w zakresie bezpieczeństwa

Każda ze stron wprowadzi i będzie realizować procedury i usługi w zakresie bezpieczeństwa, włączając w to wszystkie określone w Załączniku Technicznym, w celu ochrony

Komunikatów i ich rejestrów przed nieszczęśliwymi zdarzeniami lub niewłaściwym wykorzystaniem, włączając w to nieuprawniony dostęp, zmianę treści lub utratę.

2.6 Przechowywanie rejestrów

Strony będą zapisywać i przechowywać rejestry i Komunikaty przekazane na mocy niniejszej Umowy w sposób określony w Załączniku Technicznym.

SEKCJA 3: PRZETWARZANIE KOMUNIKATÓW

3.1 Odbiór

Każdy Komunikat przesłany zgodnie z niniejszą Umową będzie traktowany jako otrzymany w momencie, gdy stanie się on dostępny dla strony odbierającej w sposób określony w Załączniku Technicznym. Do momentu takiego odbioru, żaden przesłany Komunikat nie będzie rodził jakichkolwiek skutków prawnych, o ile stosowne prawo nie nadaje mocy prawnej takiemu Komunikatowi w momencie nadania, bez względu na to, czy został odebrany czy nie.

3.2 Potwierdzenie odbioru

3.2.1. O ile Załącznik Techniczny nie stanowi inaczej, odbiór Komunikatu nie musi być potwierdzony przez stronę odbierającą. Wymóg potwierdzenia odbioru w Załączniku Technicznym powinien zawierać metody i rodzaje potwierdzeń (włączając w to wszelkie Komunikaty lub procedury) oraz okresy czasu, jeśli występują, w których potwierdzenie odbioru musi zostać otrzymane.

3.2.2. Potwierdzenie odbioru będzie *prima facie* dowodem, że dany Komunikat został odebrany. Strona odbierająca Komunikat wymagający potwierdzenia odbioru nie będzie podejmować na podstawie tego Komunikatu żadnych czynności, do chwili wysłania potwierdzenia odbioru. Jeśli strona odbierająca nie jest w stanie wysłać potwierdzenia odbioru, strona ta nie będzie podejmować na podstawie tego Komunikatu żadnych czynności bez dodatkowych instrukcji ze strony nadawcy Komunikatu. Brak potwierdzenia odbioru Komunikatu przez stronę odbierającą nie pozbawia tego Komunikatu jego skutku prawnego, z wyjątkiem sytuacji, gdy tożsamość strony inicjującej nie może zostać zidentyfikowana na podstawie tego Komunikatu.

3.2.3. W przypadku, gdy strona inicjująca nie otrzymała, w odniesieniu do właściwie przesłanego Komunikatu, wymaganego potwierdzenia odbioru a żadne dodatkowe instrukcje nie zostały przekazane, strona inicjująca może unieważnić taki Komunikat przez powiadomienie o tym fakcie strony odbierającej.

3.3. Pomyłki Techniczne. Strona odbierająca musi powiadomić stronę inicjującą o okolicznościach, włączając w to pomyłki techniczne przy odbiorze transmisji, które uniemożliwiają dalsze przetwarzanie Komunikatu.

SEKCJA 4: WAŻNOŚĆ I WYKONALNOŚĆ

4.1 Ważność

Strony uzgadniają, iż ważne i wykonalne zobowiązania mogą powstać w drodze przekazywania Komunikatów zgodnie z niniejszą Umową. Strony kategorycznie zrzekają się wszelkich praw do kwestionowania ważności transakcji wyłącznie na podstawie faktu, iż komunikacja pomiędzy stronami odbyła się dzięki wykorzystaniu Elektronicznej Wymiany Danych.

4.2 Dowody

Bez względu na brak jakichkolwiek dokumentów w formie pisemnej i podpisów odręcznych, w zakresie dopuszczalnym przez prawo, rejestry Komunikatów przechowywane przez strony będą dopuszczalne i mogą być użyte jako dowód dotyczący informacji w nich zawartej.

4.3 Zawarcie kontraktu

Kontrakt zawarty z wykorzystaniem Elektronicznej Wymiany Danych w ramach niniejszej Umowy zostaje uznany za zawarty w momencie, gdy Komunikat przesłany jako przyjęcie oferty został odebrany zgodnie z postanowieniami Sekcji 3.1.

SEKCJA 5: WYMOGI W ZAKRESIE TREŚCI DANYCH

5.1 Status poufności

Żadna informacja zawarta w jakimkolwiek Komunikacie przekazanym na podstawie niniejszej Umowy nie będzie traktowana jako poufna, chyba że z mocy prawa lub przez zaznaczenie w Załączniku Technicznym lub w samym Komunikacie.

5.2 Zgodność z prawem

5.2.1. Każda ze stron powinna zagwarantować, iż treść każdego Komunikatu jest przesyłana, odbierana i przechowywana w zgodzie z wszystkimi obowiązującymi stronę wymogami prawa.

5.2.2. W przypadku, gdy odbiór lub przechowywanie jakiegokolwiek elementu Komunikatu stanowiłoby naruszenie właściwego prawa, odbiorca powinien niezwłocznie powiadomić o takiej niezgodności.

5.2.3. Tak długo, jak odbiorca pozostaje nieświadomy niezgodności prawnej Komunikatu, jego prawa i obowiązki w ramach niniejszej Umowy nie ulegają zmianie.

5.2.4. Po powiadomieniu nadawcy o niezgodności prawnej, odbiorca nie będzie w żadnym stopniu zobowiązany do odpowiedzi na jakiekolwiek dalsze, niezgodny z prawem Komunikaty. Po otrzymaniu powiadomienia nadawca zobowiązany jest do powstrzymania się od przekazywania jakichkolwiek dalszych, niezgodnych z prawem Komunikatów.

SEKCJA 6: ODPOWIEDZIALNOŚĆ

6.1. Siła wyższa

Żadna ze stron nie ponosi odpowiedzialności za jakiekolwiek opóźnienie lub innego rodzaju niewywiązanie się ze swoich zobowiązań wynikających z niniejszej Umowy, gdy takie opóźnienie lub niewywiązanie się spowodowane jest przez jakiekolwiek zdarzenie pozostające poza kontrolą tej strony, a którego to zdarzenia (a) nie można było racjonalnie przewidzieć w momencie podpisania niniejszej Umowy lub (b) skutków którego nie można było uniknąć lub przezwyciężyć.

6.2. Wyłączenie odszkodowania

Żadna ze stron nie jest zobowiązana do zapłaty odszkodowania za jakiekolwiek szkody specjalne, pośrednie, wtórne lub też z nawiązką, a wynikające z jakiegokolwiek naruszenia niniejszej Umowy.

6.3. Odpowiedzialność usługodawców

6.3.1. Strona korzystająca z usług osoby trzeciej w zakresie przekazywania lub przetwarzania Komunikatów jest odpowiedzialna w ramach niniejszej Umowy za wszelkie działania, niewywiązanie się lub zaniedbanie takiego usługodawcy w zakresie świadczenia rzeczonych usług.

6.3.2. Każda ze stron polecająca drugiej stronie skorzystanie z usług konkretnego usługodawcy, osoby trzeciej, jest odpowiedzialna za wszelkie działania, niewywiązanie się lub zaniedbanie takiego usługodawcy.

SEKCJA 7: POSTANOWIENIA OGÓLNE

7.1. Prawo umowy
Niniejsza Umowa jest regulowana prawem krajowym _____ . W przypadku sprzeczności prawnej między prawem regulującym transakcję a prawem regulującym niniejszą Umowę, obowiązują postanowienia prawa regulującego niniejszą Umowę.

7.2. Rozdzielność postanowień Umowy
W przypadku, gdyby którekolwiek z postanowień niniejszej Umowy okazało się z jakiegokolwiek powodu nieważne lub niewykonalne, to wszystkie pozostałe postanowienia Umowy zachowują w pełni swoją moc.

7.3. Wypowiedzenie
Każda ze stron może wypowiedzieć niniejszą Umowę za nie krótszym niż [30] dni uprzednim pisemnym wypowiedzeniem. Wypowiedzenie nie wpływa na wymianę komunikatów przed datą wypowiedzenia, ani też na realizację związanych z tym transakcji. Bez względu na wypowiedzenie, postanowienia Sekcji 2.5, 2.6, 4, 5.1, 6, 7.1 i 7.5 niezmiennie zachowują swoją moc i pozostają wiążące dla stron.

7.4. Całość Umowy
Niniejsza Umowa, wraz z Załącznikiem Technicznym, stanowi całość porozumienia stron w przedmiocie niniejszej Umowy i wchodzi w życie w momencie podpisania przez strony. Strony lub osoba upoważniona przez stronę do złożenia podpisu w jej imieniu może wprowadzać poprawki do Załącznika Technicznego. Każda ze stron dostarczy drugiej pisemny i podpisany protokół na temat każdej uzgodnionej poprawki. Każda poprawka

wchodzi w życie po wymianie pisemnych i podpisanych protokołów. Załącznik Techniczny i wszystkie poprawki będące wtedy w mocy stanowią porozumienie pomiędzy stronami.

7.5. Tytuły i podtytuły akapitów

Tytuły i podtytuły akapitów niniejszej Umowy stanowią część punktu lub podpunktu, w którym się znajdują.

7.6. Powiadomienia

Za wyjątkiem potwierdzeń i powiadomień, o których mowa w Sekcji 3, każde powiadomienie, które jest wymagane na podstawie niniejszej Umowy lub na podstawie Załącznika Technicznego uznaje się za właściwie doręczone, jeśli zostało ono doręczone stronie przeciwnej w formie pisemnej i podpisane przez osobę upoważnioną do tego przez stronę doręczającą takie powiadomienie lub jego ekwiwalent elektroniczny, który może być zarejestrowany. Każde powiadomienie ma skutek z dniem następnym po dniu jego doręczenia na wyżej wymieniony adres strony przeciwnej.

7.7. Rozstrzyganie sporów

Alternatywa nr 1: Klauzula arbitrażowa

Wszelkie spory powstające na gruncie niniejszej Umowy lub w związku z nią, włączając w to wszelkie kwestie dotyczące jej zawarcia, ważności lub wypowiedzenia, będą przekazywane do ostatecznego rozstrzygnięcia w drodze arbitrażu prowadzonego przez jedną {lub trzy} osobę(~y), zgodnie wybraną(~e) przez strony, a w przypadku braku porozumienia, wyznaczoną(~e) przez _____ w zgodzie i na mocy reguł procedury _____ .

Alternatywa nr 2: Właściwość sądu

Wszelkie spory powstające na gruncie niniejszej Umowy lub w związku z nią będą przekazywane sądom _____ , których właściwość będzie wyłączna.

Strony podpisały niniejszą Umowę z datą umieszczoną na jej początku.

Nazwa Strony:

Upoważniony Pracownik:

Podpis:

Nazwa Strony:

Upoważniony Pracownik:

Podpis:

KOMENTARZ DO MODELOWEJ UMOWY O WYMIANIE WZAJEMNEJ

Niniejszy Komentarz jest drugą częścią propozycji Organizacji Narodów Zjednoczonych dotyczącej Modelowej Umowy o Wymianie Wzajemnej w Zakresie Międzynarodowego Komercyjnego Korzystania z Elektronicznej Wymiany Danych ("Umowa Modelowa"). Zakłada się, że Komentarz będzie wykorzystywany wraz z Umową Modelową przy opracowywaniu rzeczywistych umów handlowych. Komentarz zawiera objaśnienia poszczególnych sekcji Umowy Modelowej i wytyczne dotyczące sposobu opracowywania rzeczywistych umów. Terminy pisane w Komentarzu wielką literą zostały użyte w takim samym znaczeniu w Umowie Modelowej.

I. Prezentacja ogólna

Umowa o Wymianie Wzajemnej składa się z siedmiu sekcji:

Sekcja 1. Zakres i struktura
Sekcja 2. Komunikacja i działanie
Sekcja 3. Przetwarzanie Komunikatów
Sekcja 4. Ważność i wykonalność
Sekcja 5. Wymogi w zakresie treści danych
Sekcja 6. Odpowiedzialność
Sekcja 7. Postanowienia ogólne

Ponadto istnieje potrzeba uzupełnienia Umowy o Załącznik Techniczny, który musi być do niej dołączony i jest traktowany jako integralna część Umowy. Po Komentarzu następuje Arkusz Kontrolny do Załącznika Technicznego, który można wykorzystać przy opracowywaniu Załącznika Technicznego w ramach relacji między partnerami handlowymi.

Umowa Modelowa zawiera jasne i jednoznaczne stwierdzenie, iż strony wyrażają wolę związania się tą Umową. Podkreśla to pragnienie partnerów handlowych do działania w ramach, a nie poza granicami prawa w odniesieniu do korzystania przez nich z Elektronicznej Wymiany Danych. Celem Umowy jest stworzenie silnych ram prawnych dających gwarancję, że komunikaty EDI będą miały prawnie wiążący skutek, z uwzględnieniem mogących mieć tu zastosowanie praw lub regulacji krajowych (porównaj Sekcja 7.1).

Choć opracowana do użytku w relacjach między dwoma prowadzącymi wymianę handlową partnerami, Umowa Modelowa może z łatwością zostać zaadaptowana do użytku wielostronnego w relacjach między wieloma prowadzącymi wymianę handlową partnerami,

lub w sytuacjach, w których społeczność handlowa lub też stowarzyszenie użytkowników EDI podejmuje decyzję lub zachęca do korzystania z tej samej umowy o wymianie wzajemnej. Umowa Modelowa może być zaadaptowana także do tych celów, ze stosownymi zmianami, które określą sposób, w jaki Umowa będzie wiążąca dla wielu stron.

II. Indywidualne sekcje

Sekcja 1. ZAKRES I STRUKTURA

Sekcja 1.1 Zakres

Umowa ustanawia określone zasady regulujące formy elektronicznego komunikowania się stron, które przesyłają komunikaty EDI zgodnie z formułami i standardami UN/EDIFACT ("Komunikaty"). Sekcja 2.1 (oraz Komentarz) stanowi dalsze omówienie tego aspektu Umowy. Umowa nie ma zastosowania do innych form elektronicznego komunikowania się takich, jak transmisja faksowa, czy też do form elektronicznego przesyłania tekstów (takich, jak poczta elektroniczna), które nie są usystematyzowanymi i ujednoliconymi komunikatami.

Należy podkreślić fakt, iż Umowa nie określa zasad regulujących transakcje handlowe, na użytek których może być zastosowana EDI, ponieważ transakcje te opierają się na swoich własnych, mających tu zastosowanie, przepisach prawa, na przykład: umowy sprzedaży, umowy o przewóz, umowy ubezpieczeniowe, uzgodnienia w zakresie magazynowania i inne podobne relacje.

Sekcja 1.2 Załącznik Techniczny

Załącznik Techniczny stanowi integralną część porozumienia zawartego pomiędzy partnerami handlowymi (porównaj Sekcja 7.4); jego warunki są prawnie wiążące. Załącznik Techniczny opisuje szczegółowe procedury techniczne, które zostaną wykorzystane przez strony przy przesyłaniu przez nie komunikatów EDI. Umowa o Wymianie Wzajemnej przewiduje, że pewne zagadnienia zostaną omówione w Załączniku Technicznym; zagadnienia te wymienione są w Technicznym Arkuszu Kontrolnym na końcu niniejszego Komentarza. W zależności od konkretnych potrzeb partnerów handlowych może pojawić się potrzeba omówienia dodatkowych zagadnień; zaleca się, aby w odniesieniu do tych zagadnień partnerzy handlowi skonsultowali się z właściwymi doradcami technicznymi.

Chociaż Umowa o Wymianie Wzajemnej i Załącznik Techniczny stanowią całość porozumienia między stronami, zaleca się, aby personel techniczny i radcy prawni mieli wzajemnie świadomość swoich potrzeb. Sekcja 1.2 Umowy zawiera zasadę, iż w przypadku wystąpienia sprzeczności między Umową a Załącznikiem Technicznym, będą obowiązywały postanowienia Umowy.

Sekcja 2 KOMUNIKACJA I DZIAŁANIE

Sekcja ta przedstawia zasady regulujące łączność pomiędzy partnerami handlowymi i wymagane metody działania, które każdy z partnerów musi zastosować przy nadawaniu i odbiorze Komunikatów. Dzięki takiemu postępowaniu, konieczne uzgodnienia zawierane między stronami mają prawnie wiążący skutek. Może wystąpić potrzeba zawarcia dodatkowych umów z innymi stronami (takimi, jak usługodawcy - osoby trzecie; porównaj Sekcja 2.4). Użytkowników zachęca się do zawarcia z tymi stronami wiążących umów.

Sekcja 2.1 Standardy

Mając na względzie jej międzynarodowy zasięg, Modelową Umowę o Wymianie Wzajemnej opracowano tak, aby korzystać z niej w oparciu o standardy UN/EDIFACT i zalecenia wypracowane w obrębie Komisji Gospodarczej Organizacji Narodów Zjednoczonych ds. Europy, a zatwierdzone do międzynarodowego użytku przez Międzynarodową Organizację Normalizacji (ISO). Standardy te obejmują zalecenia dotyczące formatu komunikatów, składni, rejestrów kodów, elementów i segmentów danych. Zawarte są w Rejestrze Wymiany Danych Handlowych Organizacji Narodów Zjednoczonych (UN/TDID), o którym mowa w Umowie. Techniczny Arkusz Kontrolny również wymienia określone usługi w zakresie bezpieczeństwa, dla których także istnieją standardy.

Umowa Modelowa jest jedną z propozycji zawartych w UN/TDID. Zaleca się ze wszech miar, aby użytkownicy w związku z wykorzystaniem przez nich Umowy Modelowej zapoznali się z UN/TDID oraz innymi odnośnymi publikacjami Organizacji Narodów Zjednoczonych. Lista wybranych publikacji (wraz z informacją, jak je otrzymać) zawarta jest na końcu niniejszego Komentarza.

Sekcja 2.2 Działanie systemu

Zgodnie z dominującymi praktykami handlowymi, Sekcja 2.2 obarcza każdego z partnerów handlowych indywidualnie odpowiedzialnością za testowanie i zapewnienie serwisu w odniesieniu do własnego systemu jak i kosztami z tym związanymi. Za porozumieniem strony mogą rozliczyć swoje koszty własne w inny sposób. Umowa nakłada na strony obowiązek zagwarantowania, iż będą one w stanie komunikować się w sposób zarówno efektywny jak i niezawodny.

Sekcja 2.3 Zmiany w systemie

Wiele zmian w systemie operacyjnym może obniżyć pożądaną przez strony zdolność do przesyłania informacji z jednego końca systemu do drugiego, nawet jeśli zmiany nie dotyczą bezpośrednio programu EDI lub plików. We wszystkich sytuacjach, gdy jest to praktycznie możliwe do zrealizowania, zachęca się strony do współpracy z partnerami handlowymi w celu zapobieżenia przerwom w łączności. Celem tej Sekcji jest nałożenie na partnerów handlowych wymogu powiadamiania o wszelkich proponowanych zmianach w wersjach wybranych standardów, które mają być zastosowane.

Sekcja 7.6 Umowy precyzuje sposób, w jaki powiadomienie o zmianach proponowanych w ramach niniejszej Sekcji 2.3 powinno być doręczone przez partnerów handlowych. Okres czasu przed wprowadzeniem proponowanej zmiany, w którym powiadomienie musi zostać doręczone nie jest sprecyzowany; zaleca się, aby partnerzy handlowi przewidzieli przed wprowadzeniem jakichkolwiek istotnych zmian konieczność stosownego dialogu, testów i weryfikacji w gronie ekspertów technicznych.

Sekcja 2.4 Komunikowanie się

Praktyki handlowe związane z EDI wymagają, aby strony określiły i uzgodniły metody, za pomocą których przekazywane będą Komunikaty. Metody te mogą się różnić; Komunikaty przekazuje się (zarówno nadaje jak i odbiera) używając środków telekomunikacji, poprzez dostarczanie taśm magnetycznych lub dyskietek, albo też wykorzystując wydruki. Przez umowne sprecyzowanie tych wymogów Sekcja 2.4 gwarantuje kompatybilność poszczególnych działań partnerów handlowych. Aspekty techniczne, które być może wymagają sprecyzowania, wymienione są w Technicznym Arkuszu Kontrolnym na końcu niniejszego Komentarza.

Zaleca się, aby partnerzy handlowi sprecyzowali w Załączniku Technicznym nie tylko wymagania w zakresie łączności z jednego końca systemu do drugiego, ale uwzględnili także inne relacje umowne, za pomocą których można realizować działania w zakresie EDI. Także Sekcja 6.3 omawia takie relacje.

Sekcja 2.5 Procedury i usługi w zakresie bezpieczeństwa

Stworzenie i zachowanie efektywnie bezpiecznego środowiska pracy w związku z wykorzystaniem EDI jest ważnym celem handlowym. Ponadto zarządzanie procedurami i usługami w zakresie bezpieczeństwa może być decydującym czynnikiem przy określaniu prawnego sposobu postępowania z rejestrami Komunikatów oraz określaniu ich prawnej ważności.

Partnerzy handlowi powinni dążyć do osiągnięcia najdogodniejszej formy zabezpieczenia całego kanału łączności, z jednego końca do drugiego, biorąc pod uwagę charakter wiadomości, ich relatywne zaawansowanie, koszty, dostępne środki i zmieniającą się technologię. Możliwe jest zastosowanie procedur i usług, które potwierdzają autentyczność przesyłanych i odbieranych Komunikatów oraz usprawniają stałą kontrolę, jaką strony sprawują nad spójnością wzajemnej łączności. Załącznik Techniczny określa, w sposób zwięzły, dostępne alternatywne formy usług z zakresu zabezpieczenia łączności między partnerami handlowymi oraz czynniki, jakie należy wziąć pod uwagę przy wprowadzaniu wewnętrznych procedur zabezpieczających.

Sekcja 2.6 Przechowywanie rejestrów

W celu zagwarantowania ważności i wykonalności transakcji zawartych przy użyciu EDI, Sekcja 2.6 zobowiązuje partnerów handlowych do zapisywania i przechowywania (a) przekazanych Komunikatów (zarówno nadanych jak i odebranych) i (b) rejestrów odnoszących się do tych Komunikatów. Rejestry te mogą obejmować przebiegi lub raporty dotyczące połączeń jak i bazy danych zawierające wypisy z pewnych fragmentów Komunikatów.

Wymagania dotyczące przechowywania rejestrów, które mogą być określone w Załączniku Technicznym, powinny być opracowane na podstawie wymogów handlowych i prawnych, w ramach których każda ze stron prowadzi swoją działalność. Celem jest określenie niezbędnych wymogów, które każdemu z partnerów handlowych dadzą

maksymalną pewność, iż w razie potrzeby zarówno wymagane jak i pożądane rejestry są dostępne. Prawa i regulacje krajowe dotyczące łatwości odczytania, trwałości i spójności rejestrów elektronicznych mogą różnić się między sobą znacznie.

Nie wskazuje się żadnych konkretnych wymogów czasowych ani też formatów przechowywania danych, jednakże zaleca się partnerom handlowym szczegółowe określenie tych zagadnień tak, aby w przypadku jakichkolwiek nieporozumień lub sporów w przyszłości można było stosowne rejestry odczytać w celu analizy. Poza tym Umowa nie nakłada żadnych ograniczeń w zakresie procedur wewnętrznych stosowanych przez strony w celu spełnienia wymogów Sekcji 2.6.

Sekcja 3. PRZETWARZANIE KOMUNIKATÓW

Sekcja 3.1 Odbiór

W oparciu o różne krajowe i międzynarodowe teksty i instrumenty prawne, skutek prawny komunikatu może wystąpić albo w momencie jego przesłania, albo w momencie jego odbioru, lub też gdy istniały realne warunki, w których powinien on zostać odebrany. Umowa udostępnia formułę określającą, kiedy przekazywane Komunikaty należy uznać za odebrane oraz kiedy wywołują one skutek prawny. Formuła ta jest istotna dla zrozumienia rezultatów niektórych komunikatów.

W kategoriach konkretnych, na podstawie Sekcji 3.1 Umowy, Komunikat nie będzie wywoływał skutku prawnego do chwili, gdy stanie się on dostępny dla strony odbierającej w sposób określony w Załączniku Technicznym. Pozwala to stronom określić, na jakim etapie procesu komunikacji Komunikat jest odbierany, czy to w skrytce elektronicznej, w logowej książce transakcji, w konkretnym urządzeniu lub odebrany przez konkretne osoby lub pracowników przedsiębiorstwa. Nie ma wymogu, aby Komunikat został faktycznie otwarty lub przejrzany; musi on być jedynie dostępny.

Umowa rozważa jeden ważny wyjątek: na mocy pewnych krajowych przepisów handlowych lub administracyjnych nadanie komunikatu, czy to w formie elektronicznej czy też nie, wywołuje określony skutek prawny, bez względu na to, czy komunikat faktycznie został odebrany czy też nie przez zamierzonego odbiorcę. Na przykład nabywca wysyłając reklamację wadliwego towaru zachowuje swoje prawa nawet jeśli sprzedawca nie otrzyma tego komunikatu.

Sekcja 3.2 Potwierdzenie odbioru

Formuły UN/EDIFACT przewidują, że zarówno w celu kontroli jak i zachowania bezpieczeństwa, partnerzy handlowi mogą uznać za pożądane, aby odbiór każdego Komunikatu był potwierdzany przez stronę odbierającą. W tym celu dostępne są konkretne Komunikaty. Komunikaty te mogą służyć do potwierdzania zarówno faktu odbioru jak i stwierdzenia, że w składni Komunikatu nie wystąpiły żadne błędy. Decyzja, czy konkretny typ Komunikatu jest odpowiedni do celów potwierdzania odbioru pozostaje całkowicie w gestii partnerów handlowych; partnerzy handlowi mogą dojść do wniosku, że nie występuje potrzeba potwierdzania odbioru każdego przesłanego Komunikatu. Przy podejmowaniu takich decyzji bierze się często pod uwagę koszt przekazywania potwierdzeń.

Sekcja 3.2.1 nakłada na strony obowiązek określenia w Załączniku Technicznym, kiedy odbiór Komunikatu powinien być potwierdzony. Ponieważ strona przekazująca potwierdzenie powinna mieć sposobność stwierdzenia, czy Komunikat został rzeczywiście odebrany, Załącznik Techniczny powinien być opracowany z uwzględnieniem dwóch sytuacji: (a) kiedy potwierdzenie będzie wymagane w normalnym trybie oraz (b) kiedy wymóg potwierdzenia jest zawarty w konkretnym Komunikacie, który został przekazany. Jak mówi o tym Sekcja 3.2.1, zagadnienia, jakie należy tu omówić obejmują metody i rodzaje potwierdzeń oraz okresy czasu, jeśli występują, w których potwierdzenie odbioru musi zostać otrzymane.

Sekcja 3.2.2 dopuszcza potwierdzenie odbioru jako *prima facie* dowód na to, że odnośny Komunikat został odebrany. Na podstawie tej reguły możliwe byłoby przedstawienie dowodu przeciwnego. Partnerom handlowym zwraca się uwagę na fakt, że w świetle określonych lokalnych przepisów dowodowych ich wysiłki zmierzające do kontroli dopuszczalności określonych dowodów w postępowaniu procesowym mogą zostać odrzucone.

W sytuacji, gdy wymagane jest potwierdzenie odbioru, Sekcja 3.2.2 definiuje również dodatkowy zakres odpowiedzialności. Po pierwsze, strona odbierająca nie będzie podejmować na podstawie danego Komunikatu żadnych czynności, do chwili wysłania potwierdzenia odbioru. Jeśli potwierdzenie odbioru nie może zostać wysłane, to strona odbierająca albo stosownie powiadomi o tym nadawcę tego Komunikatu, lub też poprosi o dalsze instrukcje. Do chwili otrzymania dalszych instrukcji ze strony inicjującej kontakt, strona odbierająca nie będzie podejmować zgodnie z Sekcją 3.2.2 żadnych czynności na podstawie tego Komunikatu. Zatem w większości sytuacji strony pozostają w pozycji neutralnej, aż do

momentu porozumienia się. Instrukcje mogą być przekazane telefonicznie, faksem lub w formie dostarczonych dokumentów pisemnych.

Po drugie, w odniesieniu do strony inicjującej, która oczekuje na wymagane potwierdzenie odbioru, w przypadku braku takiego potwierdzenia i nieprzekazaniu dodatkowych instrukcji, strona inicjująca może unieważnić Komunikat w drodze powiadomienia. Powiadomienie takie musi odpowiadać wymogom Sekcji 7.6. Uprawnienie takie występuje wyłącznie w przypadku Komunikatu, który na wstępie został "właściwie przesłany".

Ponieważ określone rodzaje Komunikatów mogą rodzić niekorzystny dla strony odbierającej skutek prawny (na przykład reklamacja wadliwego towaru przesłana sprzedającemu), Sekcja 3.2.2 zabrania stronie odbierającej pozbawiać Komunikat, po odebraniu, jego skutku prawnego przez nieprzesłanie wymaganego potwierdzenia odbioru.

Na podstawie Sekcji 3.2.3 strona odbierająca może nie wysłać wymaganego potwierdzenia odbioru wyłącznie w sytuacji, w której tożsamość docelowego odbiorcy nie może być określona na podstawie oryginalnego Komunikatu. W celu określenia tejże tożsamości powinny zostać sprawdzone wszystkie komponenty Komunikatu, ale nie jest wymagana żadna dodatkowa staranność.

Sekcja 3.3 Pomyłki Techniczne

W przypadku wystąpienia okoliczności uniemożliwiających dalsze przetwarzanie Komunikatu, Sekcja 3.3 nakłada na stronę odbierającą obowiązek powiadomienia strony inicjującej. Okoliczności takie mogą dotyczyć złego funkcjonowania systemu, ale obejmują także pomyłki techniczne w odebranej transmisji. W takiej sytuacji obowiązek powiadomienia strony inicjującej występuje nawet w przypadku Komunikatów, względem których nie wymaga się potwierdzenia odbioru.

WAŻNOŚĆ I WYKONALNOŚĆ

Sekcja 4 stanowi, iż intencją partnerów handlowych podpisujących Umowę jest aby wynikiem przekazywanych komunikatów EDI były ważne i wykonalne zobowiązania. Sekcja omawia zasadnicze aspekty prawne korzystania z EDI w handlu międzynarodowym.

Sekcja 4.1 Ważność

Pewne prawa krajowe mogą zezwalać partnerowi handlowemu na kwestionowanie ważności określonych komunikatów na gruncie wymogu zachowania formy pisemnej lub też dokumentu podpisanego. Sekcja 4.1 Umowy wyjaśnia, iż ważność transakcji nie może być podważana przez żadną ze stron ze względu na fakt, iż była ona oparta w swojej istocie na EDI. To postanowienie nie zawsze może być wykonalne w ramach niektórych systemów prawnych; kwestia ta może wpływać na wybór prawodawstwa krajowego regulującego postanowienia Umowy w ramach Sekcji 7.1.

Mając na uwadze fakt, iż rezultatem wykorzystania EDI jest wyeliminowanie odręcznych podpisów, zaleca się, aby strony dokonały oceny procedur i usług w zakresie bezpieczeństwa, które mogą być wybrane i zastosowane w relacjach między partnerami handlowymi. Chociaż podpisy elektroniczne mogą być przyjęte w relacjach między stronami, a także sprecyzowane w Załączniku Technicznym, to nie można zagwarantować jednak, że wszystkie usługi w zakresie podpisów elektronicznych będą spełniać te same funkcje (włączając w to funkcje prawne), co tradycyjne podpisy używane w podobnych sytuacjach.

Sekcja 4.2 Dowody

Sekcja 4.2 wyraża intencję stron, aby rejestry Komunikatów zachowywane przez strony były dopuszczalne i mogły być użyte jako dowód. Umowa przyznaje jednakże, iż prawa krajowe mogą różnić się pod względem stopnia, w jakim strony mogą określać na potrzeby postępowania procesowego dopuszczalność określonych rodzajów dowodów.

Sekcja 4.3 Zawarcie Kontraktu

Sekcja 4.3 definiuje kiedy kontrakt, który ma zostać zawarty z wykorzystaniem EDI zostaje uznany za zawarty. Określenie momentu zawarcia jest często istotne z prawnego punktu widzenia. Chociaż zostały już ogólnie zdefiniowane zasady kontraktów zawieranych drogą pocztową lub telefonicznie, to nadal istnieją niejasności w odniesieniu do kontraktów zawieranych przy użyciu EDI. Zasada wprowadzona przez Umowę zapewnia partnerom handlowym gwarancję przewidywalności i prognozowania.

Na podstawie Sekcji 4.3, oraz zgodnie z Sekcją 3.1, kontrakt zostaje zawarty, gdy zostaje odebrany Komunikat przesłany jako przyjęcie oferty. Ta "zasada odbioru" jest zgodna

z postanowieniami różnych stosowanych krajowych i regionalnych umów modelowych oraz z dominującymi praktykami handlowymi w zakresie EDI.

Sekcja 5. WYMOGI W ZAKRESIE TREŚCI DANYCH

Sekcja 5.1 Status poufności

Wymiana informacji w ramach transakcji handlowych wymaga często przekazywania poufnych danych związanych z działalnością gospodarczą prowadzoną przez partnerów handlowych. Leżące u podstaw tego umowy zazwyczaj definiują obowiązki stron w odniesieniu do sposobu postępowania z tymi danymi. Stosowne prawa krajowe mogą także określać pewne obowiązki w zakresie poufnego traktowania informacji. Zaleca się, aby strony upewniły się, iż ich sposób postępowania w odniesieniu do poufności informacji w formie elektronicznej jest równorzędny tej samej informacji przekazywanej za pomocą innych mediów.

Na podstawie tej Sekcji treść Komunikatów nie będzie traktowana jako poufna, o ile nie zostaną one oznaczone inaczej. Partnerzy handlowi mogą określić poufny charakter informacji zawartych w Komunikatach za pomocą Załącznika Technicznego lub w treści danego Komunikatu.

Sekcja 5.2 Zgodność z prawem

Sekcja ta dostarcza stronom wskazówek na temat sposobu, w jaki strony powinny prowadzić swoją działalność, aby zagwarantować jej zgodność z prawami krajowymi, które mogą definiować lub ograniczać treść Komunikatów. Ponadto niektóre przepisy (takie, jak przepisy o ochronie danych) ograniczają przekazywanie określonych informacji za granicę.

Sekcja 5.2.1 zobowiązuje każdą ze stron do zapewnienia zgodności treści Komunikatu ze wszystkimi wymogami prawnymi odnoszącymi się do danej strony. Termin "przechowywanie" odnosi się do przechowywania danych zawartych w jakimkolwiek Komunikacie, a nie do sposobu, w jaki Komunikaty mogą być przechowywane.

Sekcja ta nie nakłada na partnera handlowego obowiązku zapewnienia zgodności swoich Komunikatów z prawami obowiązującymi drugiego partnera. Jednakże pozostałe podpunkty Sekcji przedstawiają w zarysie sposób, w jaki strony będą postępować, jeśliby

Komunikat nadany przez jednego z partnerów handlowych, w sytuacji odbioru lub przechowywania, zmuszał drugiego do naruszenia właściwego prawa.

Wymagane jest powiadomienie (zgodnie z postanowieniami Sekcji 7.6), a następnie strona inicjująca musi powstrzymać się od powtórzenia postępowania, które związane jest z tym naruszeniem prawa. Przykładem może być przesłanie komunikatu zawierającego dane osobiste z kraju, w którym nie obowiązują prawa o ochronie danych do kraju, gdzie takie prawa obowiązują.

Sekcja 6. ODPOWIEDZIALNOŚĆ

Sekcja 6.1 Siła wyższa

Sekcja ta wzmacnia wzajemne dążenie stron do nadania ich elektronicznej wymianie komunikatów konsekwencji prawnych przez usunięcie ryzyka nieoczekiwanej odpowiedzialności, jaka mogłaby wystąpić przy prowadzeniu tej działalności. Sekcja 6.1 posługuje się językiem zwyczajowo używanym w wielu umowach handlowych, który pozwala stronom na uniknięcie odpowiedzialności w sytuacji, gdy opóźnienie lub niedotrzymanie warunków umowy spowodowane jest określonymi zdarzeniami poza indywidualną kontrolą partnerów.

Oczywiście strony mogą bardziej szczegółowo określić zdarzenia, które będą traktowane przez nie jako "siła wyższa", poza kontrolą danej strony. Gdyby wystąpiły określone zdarzenia, takie jak klęska żywiołowa, które można przewidzieć, to nadal nie występuje odpowiedzialność stron, o ile konsekwencji takiego pozostającego poza kontrolą zdarzenia nie można uniknąć lub przezwyciężyć.

Sekcja 6.2 Wyłączenie odszkodowania

Sekcja ta stanowi, iż wzajemną intencją stron jest, aby korzystanie przez nich z EDI na mocy niniejszej Umowy nie narażało ich na odpowiedzialność za wymienione rodzaje szkód. Różne krajowe konstrukcje prawne mogą dawać partnerom handlowym tytuł do odszkodowania (włączając, gdzie ma to zastosowanie, odszkodowania specjalne, pośrednie, wtórne lub też z nawiązką) w przypadku, gdy zostaje naruszone zobowiązanie umowne. Odszkodowania tego rodzaju są często przyznawane w celu wynagrodzenia utraconych zysków lub też jako sankcja prawna za szczególnie nieodpowiednie postępowanie.

Sekcja nie reguluje kwestii, czy obowiązek zapłaty określonego rodzaju odszkodowania może zostać nałożony na mocy warunków i postanowień innych zobowiązań umownych zawartych pomiędzy stronami. Pewne prawa krajowe mogą ograniczać możliwości egzekwowania postanowień tej Sekcji.

Sekcja 6.3 Odpowiedzialność usługodawców

Wiele przedsiębiorstw stosujących EDI korzysta także z usług usługodawców - osób trzecich (często określanych jako sieć z wartością dodaną[2]), którzy wspomagają realizację koniecznych funkcji w zakresie łączności oraz funkcji z tym związanych (na przykład prowadzenie skrytki elektronicznej, do której mogą być przesyłane Komunikaty lub też wyniesione systemy przechowywania rejestrów dotyczących Komunikatów).

Decyzja którego usługodawcę - osobę trzecią zaangażować oraz warunki umowy pomiędzy partnerem handlowym a jego usługodawcą - osobą trzecią pozostają poza kontrolą drugiego z partnerów handlowych; stosownie zatem, Sekcja 6.3.1 obarcza partnera handlowego odpowiedzialnością za działania, niewywiązanie się lub zaniedbanie swojego usługodawcy. (Sekcja 6.3.1 ma zastosowanie zarówno w przypadku, gdy partnerzy handlowi angażują różnych usługodawców - osoby trzecie a także, gdy dobrowolnie decydują się wykorzystać tego samego usługodawcę.)

W niektórych przypadkach jeden z partnerów handlowych będzie wymagał od swojego partnera handlowego skorzystania z usług konkretnego usługodawcy - osoby trzeciej; w takiej sytuacji Sekcja 6.3.2 przenosi odpowiedzialność za postępowanie usługodawcy na tego z partnerów handlowych, który wydał takie polecenie.

Sekcja 7. POSTANOWIENIA OGÓLNE

Sekcja 7 zawiera postanowienia często występujące w wielu rodzajach umów handlowych. Postanowienia te nie stanowią zamkniętej listy postanowień ogólnych, a zwyczaje i praktyki w konkretnej dziedzinie gospodarki lub regionie mogą zawierać inne podobne postanowienia ogólne.

Sekcja 7.1 Prawo Umowy

Wobec braku stosownych ustaw i przepisów regulujących wykorzystanie EDI, Umowa została przygotowana tak, aby dać stronom maksymalną gwarancję ważności i wykonalności przesyłanych przez nich komunikatów EDI. Dąży się do tego, aby cel ten był możliwy do osiągnięcia w ramach różnorodnych systemów prawnych. Zaleca się, aby partnerzy handlowi określili prawa krajowe, które będą regulowały postanowienia Umowy. Na ich decyzję mogą mieć wpływ różnice w prawodawstwie krajowym w odniesieniu do zakresu poufności operacji komputerowych, ochrony danych, transgranicznego przekazywania danych oraz podobnych zagadnień. Jednakże, w ramach większości systemów prawnych, wybrane prawo musi być związane w pewien sposób ze stronami Umowy.

Ponieważ w dążeniu do rozwiązania sporów powstających na gruncie transakcji opartych na wykorzystywaniu EDI w ramach tej Umowy może wystąpić sprzeczność między określonymi zasadami prawnymi, Umowa precyzuje, jak takie konflikty należy rozwiązywać.

Odwołanie się do praw krajowych może w sposób niewłaściwy określać pewne umowy lub przepisy regionalne, które strony mogą chcieć zastosować w Umowie. W takim przypadku zaleca się, aby strony dodały właściwe sformułowania.

Sekcja 7.2 Rozdzielność postanowień Umowy

Sekcja 7.2 wzmacnia dążenie partnerów handlowych do nadania swoim zobowiązaniom pełnej moc prawnej. Ponieważ z jakiejś przyczyny prawnej jedna lub więcej część Umowy mogą zostać uznane za nieważne lub niewykonalne, Sekcja ta gwarantuje, że w takich okolicznościach cały kontrakt nie zostanie unieważniony.

Sekcja 7.3 Wypowiedzenie

Umowa reguluje wyłącznie sytuacje, w których między stronami przesyłane są Komunikaty; nie wymaga ona korzystania z EDI przez cały czas lub przy przekazywaniu wszystkich informacji handlowych. Sekcja 7.3 daje partnerom handlowym gwarancję wolnej woli zawierania umów, zezwalając każdemu z partnerów handlowych na zakończenie w każdej chwili okresu obowiązywania Umowy. Stronie, która nie wypowiada Umowy zapewnia się odpowiedni okres czasu na zorganizowanie alternatywnych procedur w zakresie łączności. Trzydziestodniowy okres jest odzwierciedleniem dominującej praktyki handlowej,

jednakże może on zostać odpowiednio dostosowany na podstawie porozumienia stron. Bez względu na sformułowania Sekcji 7.6, wymagane powiadomienie musi zostać doręczone na piśmie.

Wypowiedzenie nie zezwala partnerom handlowym na uniknięcie wiążącego skutku prawnego określonych sekcji, a zwłaszcza Sekcji 2.5 (Procedury i usługi w zakresie bezpieczeństwa), 2.6 (Przechowywanie rejestrów), 4 (Ważność i wykonalność), 5.1 (Status poufności), 6 (Odpowiedzialność) i 7.1 (Prawo Umowy).

Sekcja 7.4 Całość Umowy

Sekcja ta stanowi, iż Załącznik Techniczny jest integralną część Umowy. Oczywiście w przypadku sporu określone prawa krajowe zezwalają, aby przy interpretowaniu postanowień Umowy były brane pod uwagę także inne aspekty stosunków między stronami.

Ponadto Sekcja 7.4 podkreśla fakt, iż poprawki muszą być sporządzone w formie pisemnej i podpisane; komunikat elektroniczny nie jest wystarczający. Ponieważ poprawki do Załącznika Technicznego będą najprawdopodobniej omawiane przez osoby posiadające wiedzę techniczną, strony mogą udzielić takiej osobie pełnomocnictwa do podpisania tych poprawek w ich imieniu.

Sekcja 7.5 Tytuły i Podtytuły Akapitów

Sekcja ta przytacza zwyczajową zasadę interpretacyjną dotyczącą sposobu, w jaki Umowa ma być odczytywana, umożliwiając tym samym wzięcie pod rozwagę pełnej treści Umowy. Strony mogą także, jeśli uznają to za stosowne, wyłączyć tytuły akapitów jako część tekstu Umowy.

Sekcja 7.6 Powiadomienia

Sekcja 7.6 daje partnerom handlowym swobodę użycia elektronicznych ekwiwalentów dokumentów pisemnych jako wymaganych powiadomień, pod warunkiem, że można sporządzić rejestr równoważny wymaganemu, podpisanemu dokumentowi w formie pisemnej. Istnieją określone rozwiązania technologiczne, które umożliwiają osiągnięcie takiego celu.

Jednakże wiele krajowych systemów prawnych nie uznaje w jasny sposób komunikatów elektronicznych jako "dokumentów pisemnych". Partnerzy handlowi powinni zachować ostrożność przy korzystaniu z elektronicznych powiadomień. Zaleca się także, aby na bieżąco śledzili nowe rozwiązania w stosownym prawodawstwie.

Strony powinny pamiętać, że postanowienia Sekcji 7.6 nie dotyczą przekazywania komunikatów w ramach Sekcji 3.2, Potwierdzenie Odbioru.

Sekcja 7.7 Rozstrzyganie sporów

Ponieważ podmioty, które dążą do zastosowania elektronicznego przesyłania komunikatów są prawdopodobnie przyciągane przez korzyści wynikające z prędkości i efektywności, jakie oferuje ta technologia, istnieje prawdopodobieństwo, że podmioty te będą również preferować podobną metodę rozstrzygania sporów, tj. arbitraż (Alternatywa nr 1). Alternatywa ta wymaga podjęcia przez strony dodatkowych decyzji w odniesieniu do procedur, jakie mają być zastosowane: miejsca, gdzie procedura ta będzie realizowana, zespołu arbitrów, metody ich doboru oraz odpowiednich zasad regulujących to postępowanie.

W przypadku podmiotów preferujących bardziej tradycyjne forum rozstrzygania sporów, Alternatywa nr 2 pozwala stronom określić sąd właściwy do rozstrzygania wszelkich możliwych sporów. Ponieważ w odniesieniu do tego zagadnienia zdecydowanie ceni się poczucie pewności, Umowa przewiduje wyłączną właściwość sądu.

Ponadto pragnieniem partnerów handlowych może być także określenie sposobów wykorzystania alternatywnych instrumentów rozstrzygania sporów, które powstają na różnych rynkach i w różnych sektorach gospodarki.

ARKUSZ KONTROLNY DO ZAŁĄCZNIKA TECHNICZNEGO

Poniższy arkusz kontrolny zostaje zaprezentowany jako część Modelowej Umowy o Wymianie Wzajemnej w celu pokazania listy zagadnień, w odniesieniu do których zaleca się, aby strony Umowy o Wymianie Wzajemnej dokonały szczegółowych ustaleń i wypracowały dane techniczne.

Lista ta nie ma stanowić pełnego wyliczenia wszelkich możliwych zagadnień, które mogą zostać omówione w Załączniku Technicznym. Uwzględnione zagadnienia wynikają bezpośrednio z odniesień do Załącznika Technicznego w Modelowej Umowie o Wymianie Wzajemnej. Lista zagadnień może zostać uzupełniona zgodnie z wymaganiami partnerów handlowych na takim poziomie szczegółowości, jaki uznają oni za konieczny.

Usilnie zaleca się, aby użytkownicy rozważyli i omówili także inne zagadnienia, które uznają za istotne dla zapewnienia pełnego zrozumienia między partnerami handlowymi w zakresie wymogów technicznych i proceduralnych związanych z realizacją EDI. Jak wspomniano o tym w Sekcji 1.2 Modelowej Umowy o Wymianie Wzajemnej:

"Dołączony Załącznik Techniczny przedstawia uzgodnione przez strony warunki techniczne w odniesieniu do określonych wymogów technicznych i proceduralnych."

Ze względu na wygodę użycia poniższy arkusz kontrolny prezentuje treść odnośnych sekcji Modelowej Umowy o Wymianie Wzajemnej:

Sekcja 2. Komunikacja i działanie
2.1 Standardy

"Strony będą korzystały z tych wersji Standardów UN/EDIFACT, które określono w Załączniku Technicznym."

Strony powinny uzgodnić wersję standardów UN/EDIFACT, jaką zamierzają stosować. Strony mogą także sprecyzować sposób, w jaki będą oceniać pod kątem zastosowania nowo opublikowane wersje standardów UN/EDIFACT.

Strony powinny także określić w kategoriach praktycznych niezbędne warunki i szczegóły techniczne. Zagadnienia, jakie powinny zostać rozważone obejmują

identyfikację katalogów, listy kodowe, wytyczne na temat realizacji komunikatów oraz inne zagadnienia bezpośrednio związane ze zdefiniowanymi standardami i ich właściwymi wersjami.

2.2 Działanie systemu

"Każda ze stron będzie testować i zapewniać serwis w odniesieniu do własnego sprzętu, oprogramowania i usług koniecznych dla efektywnego i niezawodnego przekazywania i odbierania Komunikatów."

Strony powinny opisać metody i procedury testowania pracy swoich systemów, efektywności i niezawodności procesu wzajemnej wymiany komunikatów, terminy, w jakich testy powinny być przeprowadzane oraz pożądane wyniki, jakie muszą być uzyskane. Strony powinny wprowadzić metodę jasnego informowania o gotowości swoich systemów EDI do przekazywania i odbierania Komunikatów.

2.4 Komunikowanie się

"Strony precyzyjnie określą w Załączniku Technicznym metody komunikowania się, włączając w to wymagania w zakresie telekomunikacji lub korzystania ze świadczeń usługodawców - osób trzecich."

W odniesieniu do metody komunikowania się szczegóły i warunki techniczne powinny opisywać:

- wybraną metodę(~y) komunikowania się;
- właściwe protokoły komunikacyjne, które będą stosowane przez strony w uzupełnieniu standardów UN/EDIFACT (takie jak X.25 lub X.400, itp.);
- w przypadkach koniecznych, szczegółową informację dotyczącą usługodawcy (~ów) - osoby (~ób) trzeciej (~ch), ze świadczeń którego (~ych) będzie się korzystać, włączając w to właściwy adres i informację kontaktową oraz inne szczegóły.

Strony mogą także zastanowić się nad określeniem procedur w sytuacjach krytycznych, w celu odzyskania Komunikatów w przypadku ich utraty lub awarii albo w celu zapewnienia

alternatywnej drogi transmisji oraz procedur na wypadek, gdyby zawiodła wybrana metoda komunikowania się.

2.5 Procedury i usługi w zakresie bezpieczeństwa

"Każda ze stron wprowadzi i będzie realizować procedury i usługi w zakresie bezpieczeństwa, włączając w to wszystkie określone w Załączniku Technicznym, w celu ochrony Komunikatów i ich rejestrów przed nieszczęśliwymi zdarzeniami lub niewłaściwym wykorzystaniem, włączając w to nieuprawniony dostęp, zmianę treści lub utratę."

Strony mogą zdecydować się na szczegółowe określenie procedur i usług w zakresie bezpieczeństwa, które uznają za konieczne do wprowadzenia w związku ze stosowaniem przez siebie EDI. Istnieją różne środki podwyższania niezawodności transmisji EDI między partnerami handlowymi. Celem zasadniczym jest efektywne i bezbłędne przesłanie i odbiór oraz przetworzenie możliwie największej liczby komunikatów bez podwyższania kosztów do nieuzasadnionego poziomu.

Wybór i zastosowanie środków ochrony/bezpieczeństwa jest oparte zazwyczaj na ocenie zagrożeń i co równie ważne, implikacji prawnych. Rezultatem tego może być wprowadzenie różnorodnych środków bezpieczeństwa, z których wszystkie będą niezależne od struktury komunikatu wg. UN/EDIFACT, ale mimo to mogą przyczynić się do wytworzenia poczucia pewności prawnej opartej o dostępne rejestry.

Partnerzy handlowi stosujący UN/EDIFACT mogą wybierać spośród różnych procedur i usług w zakresie bezpieczeństwa, z których kilka dostępnych jest w ramach UN/EDIFACT, a inne są ogólnie dostępne.

Usługi w zakresie bezpieczeństwa w ramach UN/EDIFACT. W celu sprostania wymogom prawnym lub skutecznej ochrony przed rozpoznanymi zagrożeniami, partnerzy handlowi mogą wybrać usługi w zakresie bezpieczeństwa, które w części składają się z usług w zakresie bezpieczeństwa dostępnych w ramach UN/EDIFACT, a wymienionych poniżej. Każda z tych usług wymaga użycia technik kryptograficznych. Stad każdy komunikat (który jest niczym innym jak sekwencją cyfr) przesyłany z jednego komputera do drugiego może być zabezpieczany przez obliczanie cyfrowych funkcji matematycznych opartych na tym komunikacie przed i po transmisji. Daje to instrument do wykrywania wszelkich

niezamierzonych zmian nie tylko w czasie przesyłania, ale także w czasie przechowywania na obu końcach systemu, realizując w ten sposób pożądaną usługę w zakresie bezpieczeństwa.

Dokumenty UN/EDIFACT wymienione w ramach listy umieszczonej na końcu Technicznego Arkusza Kontrolnego obejmują konkretne materiały objaśniające usługi w zakresie bezpieczeństwa oraz podstawowe techniki zarządzania nimi, wymienione szczegółowo poniżej. Użytkownik poszukujący informacji powinien zapoznać się z tymi materiałami.

Integralność treści komunikatu chroni przed wszelkiego rodzaju modyfikacją danych zawartych w komunikacie. Można to narzędzie rozbudować dalej, aż do osiągnięcia integralności sekwencji komunikatów, która ustanawia kolejność, w jakiej pojawiają się komunikaty. Integralność komunikatów sama w sobie nie jest zazwyczaj możliwa do osiągnięcia, o ile nie jest zastosowany jakiś klucz do generowania tak zwanego Kodu Prawdziwości Komunikatu [*ang.* MAC][3]. Jest to unikalny kryptograficzny identyfikator komunikatu tworzony za pomocą tajnego klucza. Zazwyczaj, o ile nie zastosowano specjalnie zabezpieczonego sprzętu, każdy posiadacz tego tajnego klucza może generować wartości MAC.

Jeśli istnieje dodatkowa potrzeba rozróżnienia między nadawcą a odbiorcą komunikatu (np. ze względów prawnych), właściwą usługą w zakresie bezpieczeństwa, jaką należy tu zastosować jest brak możliwości wyparcia się autorstwa przez nadawcę[4], co wymaga dodania znaczników czasu, a następnie wyliczenia cyfrowych sygnatur w oparciu o algorytmy kluczy jawnych.

Zatem brak możliwości wyparcia się autorstwa przez nadawcę implikuje potwierdzenie prawdziwości, co z kolei implikuje integralność komunikatu.

Podobnie, jak w przypadku braku możliwości wyparcia się autorstwa przez nadawcę, odbiorca może odesłać komunikat opatrzony cyfrową sygnaturą, co jest równoznaczne z brakiem możliwości wyparcia się autorstwa przez odbiorcę[5]. Inny charakter ma poufność tej usługi; zabezpiecza ona przed ujawnieniem treści komunikatu w czasie transmisji w sieci.

Środki bezpieczeństwa UN/EDIFACT dotyczą ochrony wyłącznie komunikatów EDIFACT, a nie bezpieczeństwa wewnętrznego związanego z aplikacjami użytkownika końcowego, gdzie generowane i przetwarzane są komunikaty. Podsumowując, korzystanie ze

środków bezpieczeństwa w UN/EDIFACT wymaga użycia technik kryptograficznych, które z kolei wymagają użycia kluczy kryptograficznych. Zatem korzystanie ze środków bezpieczeństwa w UN/EDIFACT implikuje sprawowanie zarządu nad kluczami.

W odniesieniu do środków bezpieczeństwa klucze (które w rzeczywistości są wielkimi liczbami) muszą pod każdym względem być traktowane ostrożnie. Algorytmy są częścią ogólnie dostępnej wiedzy i zapewniają pożądany stopień bezpieczeństwa wyłącznie, jeśli używa się ich w połączeniu z kluczami. Użytkownicy mogą posiadać wspólny klucz, który stosowany jest w celach kryptograficznych, lub też każdy z nich może posiadać parę wzajemnie pasujących do siebie kluczy (jeden poufny i jeden jawny). Cechą wspólną wszystkich systemów jest wymóg dystrybucji kluczy w bezpieczny sposób. Można tego dokonać albo na zasadach dwustronnych, albo przy udziale osoby trzeciej. Takiej osobie trzeciej powierza się realizację określonych procedur związanych z rejestracją, wydawaniem świadectw i dystrybucją kluczy. Takie osoby trzecie są często nazywane Powierniczymi Osobami Trzecimi [ang. TTP][6]. W każdej sytuacji muszą pomiędzy zaangażowanymi stronami istnieć uzgodnione zasady i procedury zarządzania kluczami.

Dodatkowe procedury i usługi w zakresie bezpieczeństwa. W celu pełnego zabezpieczenia się przed różnorodnymi formami ryzyka związanego z elektroniczną wymianą danych, strony mogą rozważyć — w odniesieniu do pewnych, przedstawionych poniżej, form ryzyka — wprowadzenie niektórych, przedstawionych poniżej, procedur i usług, które są niezależne od struktur UN/EDIFACT:

- użycie dodatkowych kodów identyfikujących, unikalnych kodów sekwencyjnych lub podobnych niekodowanych schematów śledzących i etykietujących;

- zatrudnienie usługodawców - osób trzecich, wnoszących wartość dodaną, w celu prowadzenia logowych ksiąg transakcji lub też podobnego archiwizowania i weryfikowania transakcji;

- użycie chronionych form automatycznego przechowywania danych w lokalnych stacjach roboczych w ramach sieci komputerowej przedsiębiorstwa;

- nadzorowanie dostępności i sprawności urządzeń łączności.

2.6 Przechowywanie rejestrów

"Strony będą zapisywać i przechowywać rejestry i Komunikaty przekazane na mocy niniejszej Umowy w sposób określony w Załączniku Technicznym."

Istotne szczegóły i warunki techniczne dotyczące zapisywania i przechowywania rejestrów oraz Komunikatów mogą obejmować:

- zakres rejestrów, które będą przechowywane
- format (~y), w jakim (~ch) będzie realizowane przechowywanie
- okresy czasu, w jakich rejestry będą przechowywane
- media, jakie będą stosowane do zapisu i przechowywania
- prawa dostępu do rejestrów, jakich trzeba będzie udzielić
- sposób, w jaki będzie realizowane przechowywanie (włączając w to testowanie, warunki środowiskowe, itp.)
- wymagania w zakresie integralności i niezmienności rejestrów
- zasady dotyczące dostępności rejestrów.

Zachęca się strony do rozważenia, przy okazji rozpatrywania niniejszego zagadnienia, szczegółów określonych przy omawianiu Sekcji 2.5, Procedury i usługi w zakresie bezpieczeństwa.

Sekcja 3: Przetwarzanie Komunikatów

3.1 Odbiór

"Każdy Komunikat przesłany zgodnie z niniejszą Umową będzie traktowany jako otrzymany w momencie, gdy stanie się on dostępny dla strony odbierającej w sposób określony w Załączniku Technicznym."

Określenie formy dostępu może obejmować:

- dostęp za pośrednictwem usługodawcy działającego w imieniu odbiorcy
- dostęp odbiorcy do Komunikatu, który jest przechowywany przez usługodawcę (np. w skrytce elektronicznej)
- dostęp za pośrednictwem własnego systemu komputerowego odbiorcy.

3.2.1 Potwierdzenie odbioru

"O ile Załącznik Techniczny nie stanowi inaczej, odbiór Komunikatu nie musi być potwierdzony przez stronę odbierającą. Wymóg potwierdzenia odbioru w Załączniku Technicznym powinien zawierać metody i rodzaje potwierdzeń (włączając w to wszelkie Komunikaty lub procedury) oraz okresy czasu, jeśli występują, w których potwierdzenie odbioru musi zostać otrzymane."

Strony mogą ustalić, kiedy potwierdzenie odbioru będzie wymagane w więcej niż jednej formie. Komunikaty, które będą musiały być potwierdzane mogą zostać określone za pomocą typu komunikatu (na przykład przez użycie nazw Komunikatów UN/EDIFACT) lub przez sprecyzowanie okoliczności, w których przesłane Komunikaty wymagają potwierdzenia odbioru. Strony mogą ustalić, że potwierdzenie odbioru jest wymagane, gdy stosowna prośba zostaje zawarta w Komunikacie, który został przesłany.

W przypadkach, gdy potwierdzenie odbioru będzie wymagane, strony powinny także określić szczegóły dotyczące sposobu, w jaki to potwierdzenie ma być przekazane, włączając w to:

- metodę potwierdzenia odbioru (zwrotne przesłanie Komunikatu; przesłanie innego Komunikatu takiego, jak Komunikat CONTROL; użycie innych mediów takich, jak transmisja faksowa)
- okresy czasu, w których potwierdzenie odbioru musi zostać otrzymane
- istotne procedury i usługi, które będą zastosowane w zakresie bezpieczeństwa (takie, jak Komunikat AUTACK).

Sekcja 5: Wymogi w zakresie treści danych

5.1 Status poufności

"Żadna informacja zawarta w jakimkolwiek Komunikacie przekazanym na podstawie niniejszej Umowy nie będzie traktowana jako poufna, chyba że z mocy prawa lub przez zaznaczenie w Załączniku Technicznym lub w samym Komunikacie."

Strony mogą określić w Załączniku Technicznym, że szczególne rodzaje Komunikatów (np. PAXLST, używany do przekazywania list pasażerów) lub konkretne informacje zawarte w Komunikatach (takie, jak cenniki lub dane osobowe) będą traktowane jako poufne.

Ponadto strony mogą określić szczegóły dotyczące sposobu, w jaki — wewnątrz Komunikatu — strona nadająca może zażądać poufności tego Komunikatu lub konkretnej informacji zawartej w tym Komunikacie.

W każdym przypadku, gdy wymagana jest poufność, zachęca się strony, aby zagwarantowały, iż Załącznik Techniczny lub stosowne umowy handlowe precyzują wzajemne zobowiązania stron w odniesieniu do sposobu, w jaki poufność ma być zachowana.

Sekcja 7: Postanowienia ogólne

7.6 Powiadomienia

"Za wyjątkiem potwierdzeń i powiadomień, o których mowa w Sekcji 3, każde powiadomienie, które jest wymagane na podstawie niniejszej Umowy lub na podstawie Załącznika Technicznego uznaje się za właściwie doręczone, jeśli zostało ono doręczone stronie przeciwnej w formie pisemnej i podpisane przez osobę upoważnioną do tego przez stronę doręczającą takie powiadomienie lub jego ekwiwalent elektroniczny, który może być zarejestrowany. Każde powiadomienie ma skutek z dniem następnym po dniu jego doręczenia na wyżej wymieniony adres strony przeciwnej."

W uzupełnieniu powiadomień, które mogą okazać się potrzebne na podstawie uprzednich sekcji Załącznika Technicznego, strony mogą sprecyzować także inne okoliczności, w których powiadomienia powinny być doręczane w związku z korzystaniem przez strony z Elektronicznej Wymiany Danych. Na przykład Sekcja 2.3 nakłada obowiązek powiadamiania o zmianach w funkcjonowaniu systemu; strony mogą określić w Załączniku Technicznym wszelkie specjalne wymogi w zakresie takiego powiadomienia.

---

[1] Nazwy poszczególnych ciał ONZ zostały oparte na terminologii użytej przez E. J. Osmańczyka w *Encyklopedii ONZ i Stosunków Międzynarodowych*, "Wiedza Powszechna" Warszawa 1982 [K.J.P.]

[2] ang. *value-added network*

[3] ang. *Message Authentication Code*

[4] ang. *non-repudiation of origin*

[5] ang. *non-repudiation of receipt*

[6] ang. *Trusted Third Parties*

Załącznik 2.

Wzór umowy EDI proponowany przez Komisję Europejską

Wzór umowy EDI proponowany przez Komisję Europejską

Rekomendacja Komisji Europejskiej z dnia 19 października 1994 roku dotycząca prawnych aspektów wymiany danych informatycznych o nr 94/820/CE (opublikowana: "Journal officiel des Communautés européennes" nr L 338/98 z 28.12.1994 r.)

Niniejsza umowa zostaje zawarta pomiędzy:

.....

a

.....

Artykuł 1 Przedmiot i zakres zastosowania

1.1. Niniejszy wzór umowy dotyczący EDI, zwany następnie "umową", określa zakres i warunki prawne, które mają zastosowanie do transakcji dokonywanych pomiędzy partnerami na drodze informatycznej wymiany danych (EDI).

1.2. Umowa składa się z postanowień prawnych, a uzupełnieniem jej jest aneks techniczny.

1.3. Za wyjątkiem postanowień przeciwnych zawartych pomiędzy stronami niniejszej umowy, jej postanowienia nie regulują zobowiązań kontraktowych, wynikających z transakcji dokonywanych pomiędzy nimi.

Artykuł 2 Definicje

2.1. Użytym w niniejszej umowie terminom nadano następujące znaczenie:

2.2. EDI
Wymiana danych informatycznych jest elektronicznym transferem danych handlowych i administracyjnych, w postaci zlecenia EDI, którego struktura odpowiada przyjętej normie, i który odbywa się z jednego do drugiego komputera.

2.3. Przesyłka EDI
Przesyłka EDI jest to zespół segmentów, ustrukturyzowanych według przyjętej normy, zbudowany w formie pozwalającej na odczytanie za pomocą komputera i mogący zostać automatycznie przetworzony do jednoznacznej postaci.

2.4. UN/EDIFACT
Według definicji Organizacji Narodów Zjednoczonych - Komisji ekonomicznej dla Europy, reguły ONZ odnoszące się do wymiany danych informatycznych dla administracji, handlu i transportu (UN/EDIFACT), składają się z zespołu norm, zbiorów i dyrektyw dotyczących elektronicznej wymiany ustrukturyzowanych danych, w szczególności tych dotyczących handlu produktami i usługami. Wymiana ta odbywa się pomiędzy niezależnymi systemami informatycznymi, uznanymi na szczeblu międzynarodowym.

2.5. Potwierdzenie odbioru
Potwierdzenie odbioru przesyłki EDI - jest procedurą poprzez którą, składnia i semantyka przesyłki są weryfikowane w czasie jej odbioru, a potwierdzenie odbioru jest przesyłane zwrotnie przez odbiorcę przesyłki.

Artykuł 3 Prawomocność i kształt umowy

3.1. Strony umowy, podporządkowując się jej treści, zobowiązują się nie kwestionować wartości prawnej kontraktu zawartego zgodnie z regułami i warunkami niniejszej umowy, w drodze EDI.

3.2. Każda strona umowy zobowiązuje się do zapewnienia, że zawartość wysłanej lub otrzymanej przesyłki EDI nie będzie sprzeczna z ustawodawstwem obowiązującym w ich państwach, według którego zawartość przesyłki mogłaby być zastrzeżona oraz do przedsięwzięcia wszelkich niezbędnych środków w celu niezwłocznego poinformowania drugiej strony o takiej sprzeczności.

3.3. Momentem i miejscem zawarcia kontraktu w drodze EDI są czas i miejsce akceptacji oferty, otrzymanej przez system informatyczny oferenta.

Artykuł 4 Dopuszczenie do przyjęcia i wartość dowodowa przesyłki EDI

4.1. W przypadkach, w których ustawodawstwo krajowe stron umowy na to zezwala, zobowiązują się one poprzez niniejszą umowę uznawać, w przypadku sporu, że zarejestrowane przesyłki EDI, które są przechowywane zgodnie z postanowieniami niniejszej umowy będą dopuszczone w postępowaniu przed sądem i będą dowodem tego co jest w nich zawarte, jeżeli nie zostanie przedstawiony dowód przeciwny.

Artykuł 5 Przetworzenie i potwierdzenie odbioru przesyłki EDI

5.1. Przesyłki są przetwarzane niezwłocznie po ich otrzymaniu w każdym przypadku w terminach podanych w aneksie technicznym.

5.2. Potwierdzenie odbioru nie jest wymagane, za wyjątkiem przypadków kiedy druga strona tego żąda.
Potwierdzenie odbioru może zostać zażądane na mocy postanowień szczegółowych zawartych w aneksie technicznym lub w drodze bezpośredniego żądania osoby wysyłającej, zawartego w przesyłce EDI.

5.3. W przypadku gdy potwierdzenie odbioru jest wymagane, odbierający przesyłkę EDI musi upewnić się, że potwierdzenie odbioru zostało wysłane w terminie....(np. jednego) dni roboczych, licząc od momentu otrzymania przesyłki, w którym miało miejsce potwierdzenie odbioru, chyba że inny termin był przewidziany w aneksie technicznym.
Dzień roboczy oznacza każdy inny dzień niż sobota, niedziela i wszystkie inne dni ustawowo wolne od pracy w miejscu odbioru przesyłki.
Przesyłka zaopatrzona w żądanie potwierdzenia odbioru nie może być wykonana przez odbiorcę przed wysłaniem potwierdzenia odbioru.

5.4. Jeżeli wysyłający nie otrzymał potwierdzenia odbioru przesyłki w przewidzianym terminie, ma on prawo, pod warunkiem powiadomienia odbiorcy, uważać ją za niebyłą i nieważną wobec upływu przewidzianego dla potwierdzenia terminu lub ma on prawo uruchomić procedurę w celu odzyskania przesyłki, przewidzianą w aneksie technicznym dla efektywnego zabezpieczenia otrzymania potwierdzenia odbioru.
Jeżeli procedura odzyskania nie powiedzie się w oznaczonym terminie, przesyłka EDI jest definitywnie uważana za niebyłą i nieważną wobec upływu przewidzianego terminu, pod warunkiem jednak, że odbiorca zostanie o tym powiadomiony.

Artykuł 6 Bezpieczeństwo przesyłki EDI

6.1. Strony umowy zobowiązują się do wprowadzenia i zachowywania procedur i środków mających na celu zapewnienie ochrony przesyłek EDI i zapobieganie ryzyku ich modyfikacji, opóźnienia, zniszczenia i utraty oraz dostępu do nich osób niepowołanych.

6.2. Procedury i środki bezpieczeństwa obejmują sprawdzenie oryginalności, sprawdzenie integralności, środki zapobiegające odrzuceniu przesyłki i zapewniające jej poufność.
Procedury i środki bezpieczeństwa odnoszące się do sprawdzenia oryginalności i integralności przesyłki pozwalają na identyfikację osoby wysyłającej oraz na zapewnienie, że otrzymana przesyłka EDI jest kompletna i nie została sfałszowana. Te procedury i środki są obligatoryjne dla wszystkich przesyłek EDI. Jeżeli jest to niezbędne, podstawowe procedury i środki bezpieczeństwa mogą zostać bezpośrednio wyszczególnione w aneksie technicznym.

6.3. Jeżeli procedury i środki bezpieczeństwa doprowadzą do odrzucenia przesyłki EDI lub do wykrycia błędu w przesyłce, odbiorca musi o tym zawiadomić w przewidzianym terminie wysyłającego.
Odbiorca przesyłki EDI , która nie została przyjęta lub która zawiera błąd nie może odmówić jej przyjęcia bez autoryzacji wysyłającego. W przypadku gdy wiadomość nie przyjęta lub zawierająca błąd zostaje ponownie przesłana przez wysyłającego, przesyłka musi zawierać jasne wytłumaczenie, o co w niej chodzi.

Artykuł 7 Poufność i ochrona danych o charakterze osobistym

7.1. Strony umowy muszą zapewnić, że przesyłki zawierające informacje poufne, wyszczególnione jako takie przez wysyłającego lub, które są poufne na podstawie zawartej pomiędzy nimi umowy, pozostają poufne i nie są rozpowszechniane lub przesyłane do innych nieupoważnionych osób , ani też używane w innych celach aniżeli tych, które zostały ustalone przez strony.
W przypadku gdy przesyłka podlega autoryzacji, dalsze przesłanie zawartych w niej informacji jest podporządkowane takiemu samemu stopniowi poufności.

7.2. Przesyłki EDI uchodzą za nie zawierające informacji poufnych w przypadku gdy informacje są własnością powszechną.

7.3. Strony umowy mogą ustalić posługiwanie się specjalnymi środkami ochrony dla pewnych przesyłek, w tym metodą ich szyfrowania, w przypadku gdy prawo danego państwa taką formę przesyłek uznaje.

7.4. Jeżeli przesyłki EDI zawierające dane o charakterze osobistym zostały wysłane lub otrzymane w kraju gdzie nie obowiązuje żadna ustawa chroniąca dane, to wówczas aż do czasu dostosowania danego ustawodawstwa do norm Wspólnoty, każda strona umowy zobowiązuje się przestrzegać, jako normę minimalną dyspozycje konwencji Rady Europejskiej dotyczącej ochrony jednostki przy automatycznym przetwarzaniu danych o charakterze osobistym[1].

Artykuł 8 Rejestracja i przechowywanie przesyłek EDI

8.1. Każda strona umowy musi przechowywać wszystkie przesyłki EDI wymienione pomiędzy stronami w trakcie transakcji handlowej w komplecie oraz w porządku chronologicznym. W czasie przechowywania tych przesyłek strony zachowują wszystkie środki bezpieczeństwa gwarantujące niezmienność przesyłki, uwzględniając terminy ich przechowywania oraz inne przepisy legislacyjne państwa,

[1] Konwencja nr 108 Rady Europy z 28 stycznia 1981 r.

którego podmiotem jest dana strona umowy. Jednakże minimalny okres przechowywania wynosi ..... (np. trzy lata), licząc od sfinalizowania transakcji.

8.2. Z zastrzeżeniem przepisów o przeciwnej treści w ustawodawstwie państwa strony umowy, przesyłki EDI muszą być przechowywane w formie nadanej im przez wysyłającego i w formie w jakiej otrzymał je odbierający.

8.3. Strony umowy muszą zapewnić, że przesyłki EDI przechowywane w pamięci elektronicznej lub informatycznej, są łatwo dostępne i mogą być odtworzone w formie czytelnej dla człowieka oraz w razie potrzeby wydrukowane. Wszystkie materiały niezbędne do tych operacji muszą być przechowywane (dostępne).

Artykuł 9 Szczegóły dotyczące funkcjonowania EDI

9.1. Strony umowy zobowiązują się zastosować i utrzymywać materiały niezbędne do funkcjonowania EDI, odpowiednio do postanowień niniejszej umowy, przez co rozumie się następujące uzgodnienia:

9.2. Wyposażenie
Strony umowy muszą zaopatrzyć się i zapewnić odpowiednie urządzenia, oprogramowanie i obsługę niezbędną do przesyłania, otrzymywania, tłumaczenia, rejestrowania i przechowywania przesyłek EDI.

9.3. Środki komunikacji
Strony umowy muszą uzgodnić środki, których będą używały do komunikowania się, przez co należy rozumieć protokoły telekomunikacyjne oraz wybór podmiotu, który będzie zajmował się obsługą (świadczył usługi serwisowe).

9.4. Normy stosowane do przesyłek EDI
Wszystkie przesyłki EDI będą przesyłane zgodnie z normami, rekomendacjami i procedurami UN/EDIFACT[2], zatwierdzonymi przez Komisję Ekonomiczną Narodów Zjednoczonych Europy (CEE/NU-WP 4) i zgodnymi z normami europejskimi.

9.5. Kody
Listy kodów elementów danych, do których odnoszą się przesyłki EDI muszą zawierać w sobie listy kodów uaktualnionych UN/EDIFACT, listy kodów międzynarodowych utworzonych zgodnie z międzynarodowymi normami ISO, jak również listy kodów CEE/NU lub listy które były oficjalnie opublikowane.
Jeżeli takie listy kodów nie są dostępne, należy wówczas dać pierwszeństwo listom kodów opublikowanych, uaktualnionych i gwarantujących zgodność (współpracę) z innymi systemami kodowania.

Artykuł 10 Właściwości i wymagania techniczne

Aneks techniczny musi określać właściwości i wymagania stanu technicznego, organizacyjnego i proceduralnego niezbędne do funkcjonowania EDI, zgodnie z postanowieniami niniejszej umowy, w szczególności dotyczące:

- wymagań dotyczących działania EDI przedstawionych w art. 9, przez co należy rozumieć urządzenia niezbędne do funkcjonowania EDI, środki komunikacji, normy mające zastosowanie do przesyłek EDI oraz kody,

---

[2] Reguły składniowe UN/EDIFACT ISO 9735 EN 29735, TDEED UN/EDIFACT ISO 7372-EN 27372. L'UNTDID (repertorium wymiany danych handlowych ONZ) zawiera również: zasady przewodnie dotyczące wykorzystania składni, wykaz elementów danych, listę kodów, wykaz elementów danych złożonych, wykaz standardowych segmentów, wykaz UNSM i zasady UNCID.

- przyjęcia i potwierdzenia odbioru przesyłek EDI,
- bezpieczeństwa przesyłek EDI,
- rejestrowania i przechowywania przesyłek EDI,
- terminów,
- procedur mających zastosowanie do działań próbnych i sprawdzających pozwalających ustalić i kontrolować zgodność stanu faktycznego z ustalonymi właściwościami i wymaganiami technicznymi.

Artykuł 11 Odpowiedzialność

11.1. Żadna ze stron umowy nie jest odpowiedzialna za szkody specjalne, pośrednie oraz drugorzędne (uboczne) wynikające z niewykonania postanowień niniejszej umowy.

11.2. Żadna ze stron umowy nie jest odpowiedzialna za straty lub szkody doznane przez drugą stronę z powodu opóźnienia lub zwłoki w wykonaniu któregoś z postanowień niniejszej umowy, w przypadku kiedy to opóźnienie lub zwłoka nastąpiły z przyczyn niezależnych od woli strony i które nie mogły być przez stronę racjonalnie przewidziane w chwili podpisania umowy, lub których konsekwencji nie można było uniknąć lub opanować.

11.3. Jeżeli strona angażuje pośrednika (usługodawcę) do świadczenia takich usług jak przesyłanie, rejestrowanie lub przetwarzanie przesyłki EDI, strona ta jest odpowiedzialna za szkody wynikające bezpośrednio z działań, opóźnień lub zaniechania dokonanego przez tego pośrednika w trakcie wykonywania przez niego w/wym. usług.

11.4. Jeżeli jedna strona umowy domaga się aby druga strona skorzystała z pośrednika przy przesyłaniu, rejestrowaniu lub przetwarzaniu przesyłki EDI, strona ta jest wówczas odpowiedzialna względem tej strony, od której się tego domagała, za szkody wynikające bezpośrednio z działań, opóźnień lub zaniechania dokonanych przez tego pośrednika w trakcie wykonywania przez niego w/wym. usług.

Artykuł 12 Rozstrzyganie sporów

Możliwość 1[3]

Klauzula wyboru sądu polubownego

Wszystkie spory wynikające z tej umowy lub których przedmiotem jest niniejsza umowa, przez co należy rozumieć wszystkie kwestie dotyczące jej istnienia, ważności lub jej wygaśnięcia, są poddane do rozstrzygnięcia sądowi polubownemu, składającemu się z jednej (lub trzech) osoby wybranej zgodnie przez strony umowy, a w przypadku braku wspólnego porozumienia w kwestii wyboru tej osoby, będzie ona desygnowana przez .....[4], odpowiednio do postanowień proceduralnych .....[5] .

---

[3] Strony muszą dokonać wyboru pomiędzy możliwością 1 "wybór sądu polubownego", a możliwością 2 "wyznaczającą właściwość".

[4] Podmiot wyposażony przez strony we władzę mianowania arbitra; część do wypełnienia przez strony.

[5] Wybór procedury arbitrażowej; do wypełnienia przez strony.

Możliwość 2

Klauzula oznaczająca właściwość

Wszystkie spory wynikające z niniejszej umowy lub których przedmiotem jest ta umowa, są poddane do rozstrzygnięcia przez sądy .....[6], które mają kompetencję wyłączną do rozpoznania sprawy.

Artykuł 13 Prawo umowy

Bez przedkładania ponad inne danego prawa narodowego, które mogłoby zostać zastosowane w stosunkach pomiędzy stronami, w tym co dotyczy rejestracji, przechowywania przesyłek EDI lub ich poufności i ochrony danych o charakterze osobistym, umowa podlega ustawodawstwu .....[23].

Artykuł 14 Moc obowiązywania, zmiany umowy, wygaśnięcie umowy, niezależność postanowień

14.1. Moc obowiązywania
Umowa niniejsza wchodzi w życie z datą jej podpisania przez strony.

14.2. Zmiany umowy
W każdym przypadku, postanowienia uzupełniające umowę lub zastępujące niektóre postanowienia niniejszej umowy, które zostały uznane przez strony, są traktowane jako część integralna umowy, licząc od daty podpisania tej modyfikacji.

14.3. Wygaśnięcie umowy
Każda ze stron może odstąpić od niniejszej umowy poprzez uprzednie zawiadomienie w terminie co najmniej ..... (np. jednego) miesiąca, przy czym zawiadomienie musi mieć formę listu poleconego lub musi zostać zakomunikowane drugiej stronie w każdy inny sposób przez strony uzgodniony. Transakcje dokonane po tym terminie będą rozważane po ustaniu niniejszej umowy.
Wygaśnięcie niniejszej umowy, bez względu na przyczynę nie będzie skutkowało powstaniem uprawnień ani zobowiązań dla stron wynikających z artykułów 4, 6, 7 i 8.

14.4. Niezależność postanowień
Unieważnienie całego lub części któregoś z artykułów niniejszej umowy pozostaje bez wpływu na ważność pozostałych artykułów tej umowy.

---

[6] "Państwo"; do wypełnienia przez strony.

Załącznik 3.

Ustawa o podpisie cyfrowym stanu Utah. Tytył 46, Rozdział 3 (1996)

Zasady ogólne. Kodeks postępowania administracyjnego stanu Utah. R154-10

USTAWA O PODPISIE CYFROWYM STANU UTAH
TYTUŁ 46 KODEKSU STANU UTAH, ROZDZIAŁ 3 (1996)

Część 1. Skrót tytułu, interpretacja i definicje.

Abstrakt : Ta część definiuje terminy i stanowi wytyczne interpretacji Ustawy. Określa ona również rolę Wydziału.

101. Skrót tytułu

Rozdział ten będzie znany i przytaczany jako Ustawa o podpisie cyfrowym.

102. Cele i konstrukcja

Rozdział ten został opracowany zgodnie z tym co jest rozsądne w handlu w tych okolicznościach i aby spełniać następujące cele :
1. ułatwić handel poprzez wiarygodne komunikaty elektroniczne;
2. maksymalnie ograniczyć fałszerstwo cyfrowych podpisów i oszustwo w handlu przy zastosowaniu elektroniki;
3. wdrażać prawnie ogólny import odpowiednich standardów takich jak X.509 Międzynarodowego Związku Telekomunikacji (International Telecommunication Union) (dawniej International Telegraph and Telephone Consultative Committee lub CCITT);
4. ustalić we współpracy z licznymi stanami jednolite wymogi dotyczące autoryzacji i wiarygodności komunikatów elektronicznych.

103. Definicje

Dla celów tego rozdziału i o ile kontekst nie wskazuje inaczej :
1. "Akceptować certyfikat" oznacza alternatywnie :
    1. aprobować certyfikat znając jego zawartość , lub będąc o niej poinformowanym
    2. składać podanie o certyfikat do licencjonowanego Organu Certyfikującego nie anulując ani nie odwołując tego podania poprzez skierowanie zawiadomienia o anulowaniu lub odwołaniu do Organu Certyfikującego i uzyskując podpisane pisemne potwierdzenie od tego Organu Certyfikującego jeśli organ ten następnie wyda certyfikat zgodnie z podaniem.
2. "Asymetryczny kryptosystem" oznacza algorytm lub serię algorytmów , które zapewnią bezpieczną parę kluczy.
3. "Certyfikat" oznacza zapis komputerowy, który :
    1. identyfikuje Organ Certyfikujący który go wydał ;
    2. określa lub identyfikuje osobę, której dotyczy ;
    3. zawiera klucz publiczny podpisującego; oraz
    4. jest cyfrowo podpisywany przez Organ Certyfikujący;
4. "Organ Certyfikujący" oznacza osobę , która wydaje certyfikat.
5. "Jawne akta dotyczące Organu Certyfikującego" oznaczają bezpośrednio i publicznie dostępny zapis, który dotyczy licencjonowanego Organu Certyfikującego i który jest przechowywany w Wydziale Urzędu. Jawne akta dotyczące Organu Certyfikującego mają zawartość według przepisu Wydziału Urzędu zgodnego z ustępem 202 Kodeksu R154-10.
6. "Wymogi certyfikacji" oznaczają oświadczenie dotyczące wymogów jakimi ogólnie kieruje się organ nadający certyfikaty lub nadający konkretny certyfikat.

7. "Certyfikować" oznacza wydawać oświadczenie w odniesieniu do certyfikatu na podstawie zdolności do oceny i z obowiązkiem zaznajomienia się ze wszystkimi zaistniałymi faktami.
8. "Potwierdzać" oznacza uzyskiwać pewność poprzez stosowne badanie.
9. "Odpowiadać" oznacza ,w odniesieniu do kluczy , należeć do tej samej pary kluczy.
10. "Podpis cyfrowy" oznacza przetworzenie komunikatu za pośrednictwem asymetrycznego kryptosystemu w ten sposób , że osoba posiadająca wyjściowy komunikat i publiczny klucz podpisującego może dokładnie ustalić :
    1. czy przetworzenie zostało dokonane przy użyciu klucza prywatnego, który odpowiada kluczowi publicznemu podpisującego; oraz
    2. czy komunikat został zmieniony od czasu dokonania przetworzenia.
11. "Wydział Urzędu" oznacza Wydział Handlu Stanu Utah, Wydział Podmiotów Prawnych i Kodeksu Handlowego.
12. "Sfałszować podpis cyfrowy" oznacza alternatywnie :
    1. złożyć podpis cyfrowy bez upoważnienia legalnego posiadacza klucza prywatnego; lub
    2. złożyć podpis cyfrowy sprawdzalny poprzez certyfikat podający za osobę podpisującą kogoś kto nie istnieje, lub też nie posiada klucza prywatnego odpowiadającego kluczowi publicznemu określonemu na certyfikacie.
13. "Posiadać klucz prywatny" oznacza być w stanie wykorzystać klucz prywatny.
14. "Włączać poprzez odnośniki" oznacza czynić jeden komunikat częścią innego komunikatu poprzez oznaczenie komunikatu do włączenia i wyrażając zamiar jego włączenia.
15. "Wydać certyfikat" oznacza czynności Organu Certyfikującego związane z tworzeniem certyfikatu i powiadomieniem osoby podpisującej określonej w certyfikacie.
16. "Para kluczy" oznacza klucz prywatny i odpowiadający mu klucz publiczny w asymetrycznym kryptosystemie, klucze mające tego rodzaju właściwość, że klucz publiczny może sprawdzić podpis cyfrowy utworzony przez klucz prywatny.
17. "Licencjonowany Organ Certyfikujący" oznacza Organ Certyfikujący , któremu Wydział Urzędu wydał licencję posiadającą ważność.
18. "Komunikat" oznacza cyfrowe przedstawienie informacji.
19. "Powiadomić" oznacza przekazać pewien fakt innej osobie w sposób jak najbardziej wierny w danych okolicznościach w celu udzielenia informacji innej osobie.
20. "Personel operacyjny" oznacza jedną lub więcej osób fizycznych występujących jako Organ Certyfikujący lub jego przedstawiciel, lub mających stosunek pracy z Organem Certyfikującym lub w ramach kontraktu z nim i które :
    1. mają stanowiska kierownicze i są odpowiedzialne za wytyczanie linii działania działając na rzecz Organu Certyfikującego; lub
    2. mają obowiązki bezpośrednio związane z wydawaniem certyfikatów, tworzeniem kluczy prywatnych lub administracją urządzeń obliczeniowych Organu Certyfikującego.
21. "Osoba" oznacza osobę fizyczną lub jakąkolwiek organizację zdolną do podpisywania dokumentów, z mocą prawną lub fizycznie składającą podpis.
22. "Klucz prywatny" oznacza klucz z pary kluczy używany do tworzenia podpisu cyfrowego.
23. "Klucz publiczny" oznacza klucz z pary kluczy używany do sprawdzania podpisu cyfrowego.
24. "Publikować" oznacza wprowadzać do rejestru.
25. "Ograniczone prawo do zapłaty" oznacza odszkodowania od licencjonowanego Organu Certyfikującego zasądzone za pośrednictwem sądu właściwego dla Organu Certyfikującego w postępowaniu cywilnym o złamanie postanowień tego rozdziału.
26. "Odbiorca" oznacza osobę , która otrzymuje lub ma podpis cyfrowy i pragnie na nim polegać.

27. "Uznany rejestr" oznacza rejestr uznany przez Wydział Urzędu zgodnie z ustępem 501 tego rozdziału.
28. "Zalecany limit zaufania" oznacza limit kwotowy zalecany jako wiarygodny dla certyfikatu zgodnie z ustępem 309 (1).
29. "Rejestr" oznacza system przechowywania i wyszukiwania certyfikatów i innych danych związanych z podpisami cyfrowymi.
30. "Anulować certyfikat" oznacza spowodować utratę ważności certyfikatu na stałe od określonej daty. Anulowanie jest zrealizowane poprzez zapis lub wpis do zbioru anulowanych certyfikatów i nie oznacza, że anulowany certyfikat jest zniszczony lub stał się nieczytelny.
31. "Legalnie posiadać klucz prywatny" oznacza być w stanie używać klucz prywatny:
    1. który nie będzie nikomu ujawniany przez posiadacza lub przedstawicieli posiadacza łamiąc tym postanowienie ustępu 305 (1); oraz
    2. który nie został uzyskany przez posiadacza poprzez kradzież, oszustwo, podsłuch lub inne nielegalne sposoby.
32. "Podpisujący" oznacza osobę, która :
    1. jest określona na certyfikacie;
    2. akceptuje certyfikat; oraz
    3. posiada prywatny klucz, który odpowiada kluczowi publicznemu określonemu w tym certyfikacie.
33. "Odpowiednia gwarancja" oznacza albo rewers gwarancyjny sporządzony przez gwaranta mającego pozwolenie Wydziału Ubezpieczeń Stanu Utah do prowadzenia działalności w tym stanie lub też nieodwołalną akredytywę wystawioną przez instytucję finansową mającą pozwolenie Wydziału Instytucji Finansowych Stanu Utah na prowadzenie działalności w tym stanie, który rewers spełnia wszystkie z następujących wymogów :
    1. jest płatny wobec Wydziału Urzędu na rzecz osób posiadających ograniczone prawa do zapłaty od licencjonowanego Organu Certyfikującego określonego jako główny dłużnik rewersu lub płatnik akredytywy;
    2. jest wystawiony na kwotę określoną przepisem Wydziału Urzędu zgodnie z ustępem 201 Kodeksu R154-10;
    3. stwierdza, że jest wystawiony do celów zgodnych z tym rozdziałem;
    4. określa okres ważności rozciągający się przynajmniej na okres licencji wydawanej organowi wydającemu certyfikat; oraz
    5. sporządzony jest w formie przepisanej lub zaakceptowanej zgodnie z przepisem Wydziału Urzędu.

Odpowiednia gwarancja może również przewidywać, że całkowite roczne zobowiązanie gwarancyjne wobec osób wysuwających roszczenia oparte na niej nie może przekraczać nominalnej kwoty gwarancyjnej.
34. "Zawiesić certyfikat" oznacza spowodowanie tymczasowego unieważnienia certyfikatu na określony okres w przyszłości.
35. " Datownik" oznacza alternatywnie :
    1. załączenie do komunikatu, podpisu cyfrowego lub certyfikatu adnotacji z podpisem cyfrowym podającej przynajmniej datę, czas, i tożsamość osoby załączającej adnotację,
    2. adnotację w ten sposób załączoną.
36. "Certyfikat transakcyjny" oznacza ważny certyfikat obejmujący poprzez odnośniki jeden lub więcej cyfrowych podpisów.

37. "Wiarygodny system" oznacza sprzęt komputerowy i oprogramowanie :
    1. które w rozsądnym zakresie są zabezpieczone przed zewnętrznym lub niewłaściwym użyciem;

2. które zapewniają dostateczną dostępność, pewne i poprawne funkcjonowanie; oraz
3. które są racjonalnie dobrane do wykonania swoich przewidzianych funkcji.

38. "Ważny certyfikat" oznacza certyfikat :
1. który został wydany przez Organ Certyfikujący;
2. który został zaakceptowany przez wskazanego w nim podpisującego;
3. który nie został anulowany lub zawieszony; oraz
4. którego ważność nie wygasła;

pod warunkiem, że certyfikat transakcyjny jest ważnym certyfikatem tylko w odniesieniu do podpisu cyfrowego włączonego do niego poprzez odnośnik.

39. "Weryfikować podpis cyfrowy" oznacza w odniesieniu do danego podpisu cyfrowego, komunikatu, oraz klucza publicznego, ustalanie dokładnie , że :
1. podpis cyfrowy został utworzony poprzez klucz prywatny odpowiadający kluczowi publicznemu, oraz
2. komunikat nie został zmieniony od czasu utworzenia podpisu cyfrowego.

104. Rola Wydziału Urzędu.

Organ Certyfikujący

Wydział Urzędu będzie stanowić Organ Certyfikujący i może wydać , zawiesić, i anulować certyfikaty w sposób przewidziany dla licencjonowanych Organów Certyfikujących. Część 3 dotyczy Wydziału Urzędu w odniesieniu do certyfikatów , które wydaje.

Baza danych jawnych akt organu certyfikującego

Wydział Urzędu będzie zajmować się publicznie dostępną bazą danych zawierającą jawne akta organu certyfikującego dla każdego licencjonowanego organu certyfikującego. Wydział Urzędu opublikuje zawartość bazy danych w przynajmniej jednym uznanym rejestrze.

Wymogi

Wydział Urzędu zapewni zgodność wymogów z tym rozdziałem i realizacją swoich założeń w celu :
1. zawiadywania licencjonowanymi organami certyfikującymi , ich działalnością i zakończeniem działalności Organu Certyfikującego;
2. wyznaczenia odpowiedniej kwoty gwarancji w odniesieniu od :
    1. zakresu zobowiązania jakie odpowiednia gwarancja nakłada na licencjonowane Organy Certyfikujące; oraz
    2. zapewnienia odpowiedzialności finansowej jaką przyjmuje wobec osób, które zawierzają certyfikatom wydawanym przez licencjonowane Organy Certyfikujące;
3. sprawdzenia oprogramowania używanego przy tworzeniu podpisów cyfrowych oraz opublikowania raportów dotyczących oprogramowania;
4. określenia racjonalnych wymogów formy certyfikatów wydawanych przez licencjonowane Organy Certyfikujące zgodnie z ogólnie przyjętymi normami dla certyfikatów z podpisami cyfrowymi;

5. określenia racjonalnych wymogów dotyczących przechowywania akt przez licencjonowane Organy Certyfikujące;
6. określenia racjonalnych wymogów co do treści, formy i źródeł informacji w jawnych aktach Organu Certyfikującego, aktualność oraz wymiar czasowy tych informacji oraz inne czynności i linia działania jakie dotyczą jawnych akt Organu Certyfikującego;
7. określenia formy oświadczenia dotyczącego wymogów certyfikacji;
8. w inny sposób nadania skuteczności i realizowania tej Ustawy o Podpisie Cyfrowym.

Część 2. Licencjonowanie i wymogi wobec Organów Certyfikujących.

Streszczenie : Część ta pozwala Wydziałowi Urzędu na udzielanie licencji i narzucanie wymogów na organy certyfikujące w celu zapewnienia podstawowego poziomu jakości ich usług, które są istotne dla wiarygodności podpisów cyfrowych.

201. Licencja i kwalifikacje organów certyfikujących.

Kwalifikacje

Aby otrzymać i zachować licencję organ certyfikujący powinien :

1. być podpisującym w certyfikacie opublikowanym w uznanym rejestrze;
2. zatrudniać w personelu operacyjnym osoby, które nie zostały skazane w okresie ostatnich piętnastu lat za przestępstwa związane z oszustwem lub fałszywym zeznaniem;
3. zatrudniać jako personel operacyjny osoby , które wykazały wiedzę i biegłość w wykonywaniu wymogów tego rozdziału;
4. składać w Wydziale Urzędu odpowiednią gwarancję , chyba , że organem certyfikującym jest Gubernator, agenda rządu stanowego, główny prokurator, Rada Sądu Stanu Utah, lub okręg, i pod warunkiem , że każdy z powyżej wymienionych działa poprzez swoich przedstawicieli upoważnionych przepisami lub aktem prawnym do spełniania funkcji organu certyfikującego; a ten stan lub dana jednostka występują jako podpisujący wszystkich certyfikatów wydanych przez taki organ certyfikujący;
5. posiadać prawo do posługiwania się takim godnym zaufania systemem, zawierającym pewne środki kontroli wykorzystania klucza prywatnego;
6. przedstawiać Wydziałowi Urzędu dowód posiadania kapitału obrotowego w dostatecznej wysokości, zgodnie z przepisami Wydziału Urzędu, który umożliwi petentowi prowadzenie działalności gospodarczej jako organ certyfikujący.
7. prowadzić biuro w tym stanie lub ustanowi zarejestrowanego pełnomocnika dla obsługi procesu certyfikacyjnego w tym stanie;
8. spełniać wszystkie dalsze wymogi licencyjne ustalone przepisem Wydziału Urzędu.

Wydawanie licencji

Wydział Urzędu wyda licencję organowi certyfikującemu, który :
1. posiada kwalifikacje zgodne z podustępem (1) tego ustępu;

2. wniesie na piśmie podanie o licencję, oraz
3. pokryje opłatę ustaloną przepisem Wydziału Urzędu.

Ograniczone licencje

Wydział Urzędu może klasyfikować licencje według określonych ograniczeń, takich jak maksymalna liczba zaległych certyfikatów, łączna maksymalna wartość zaleconych limitów zaufania w certyfikatach wydawanych przez organ certyfikujący lub ograniczenie wydawania certyfikatu w ramach tylko pojedynczej firmy lub instytucji, i Wydział Urzędu może wydawać ograniczone licencje według limitów każdej kategorii. Organ certyfikujący będzie występować jako nielicencjonowany organ certyfikujący wydając certyfikat przekraczający ograniczenia licencyjne organu certyfikującego.

Zawieszenie lub anulowanie licencji

Wydział Urzędu może anulować lub zawiesić licencję organu certyfikującego za niezastosowanie się do postanowień tego rozdziału lub nie zachowując kwalifikacji zgodnie z podustępem (1) tego ustępu, zgodnie z postępowaniem sądowym przepisanymi przez Ustawę o Postępowaniu Administracyjnym, tytuł 63, rozdział 46b.

Uznanie innych licencji

Wydział Urzędu może w zasadzie uznać licencję lub upoważnienie organów certyfikujących nadane przez inne agendy rządowe, pod warunkiem, że te wymogi uzyskania licencji lub upoważnienia są w przeważającej mierze podobne do wymogów tego stanu. Jeśli w ten sposób uznana jest licencja nadana przez inne agendy rządowe:

1. część 4 tego rozdziału , odnosząca się do założeń i skutków prawnych, dotyczy certyfikatów wydanych przez organy certyfikujące licencjonowane lub upoważnione przez tę agendę rządową w taki sam sposób jak dotyczy innych licencjonowanych organów certyfikujących tego stanu; oraz
2. ograniczenia odpowiedzialności z ustępu 309 dotyczą organów certyfikujących licencjonowanych lub upoważnionych przez tę agendę rządową w ten sposób jak dotyczą licencjonowanych organów certyfikujących tego stanu.

Skutek braku licencjonowania

O ile strony nie uzgodnią inaczej w kontrakcie zawartym między sobą , wymogi dotyczące licencjonowania nie mają wpływu na skuteczność, możliwości egzekucji, czy ważność jakiegokolwiek podpisu cyfrowego, z tym wyjątkiem, że część 4 tego rozdziału nie będzie się stosować do podpisu cyfrowego , który nie może być weryfikowany poprzez certyfikat wydany przez licencjonowany organ certyfikujący. Ponadto, ograniczenia odpowiedzialności ustępu 309 nie dotyczą nielicencjonowanych organów certyfikujących.

202. Audyt działalności

Audyt rocznej działalności

Biegły księgowy, który posiada znajomość ochrony komputerowej lub poświadczony specjalista w dziedzinie ochrony komputerowej dokona badania działalności każdego organu

certyfikującego przynajmniej raz na rok w celu sprawdzenia zgodności z postanowieniami tego rozdziału . Wydział Urzędu może swoimi przepisami bardziej szczegółowo określić kwalifikacje biegłych księgowych.

Klasyfikacja i ogłoszenie wyników

W oparciu o informacje zebrane w trakcie badania, audytor dokona klasyfikacji zgodności przestrzeganej przez licencjonowany organ certyfikujący w sposób następujący :

1. Pełna zgodność : wszystko wskazuje na to, że organ certyfikujący spełnia wymogi ustawowe i regulacyjne.
2. Zasadnicza zgodność : organ certyfikujący ogólnie przestrzega wymogów ustawowych i regulacyjnych; jednakże w badanym materiale wykryto jeden lub więcej przykładów niezgodności lub sytuacji gdzie nie można wykazać zgodności lecz które najprawdopodobniej pozostają bez konsekwencji.
3. Częściowa zgodność : organ certyfikujący przestrzega pewne ustawowe i regulacyjne wymogi lecz stwierdzono , że nie spełnił lub nie był w stanie wykazać dopełnienia jednego lub więcej ważnych zabiegów zabezpieczających.
4. Niezgodność : organ certyfikujący spełnił kilka lub nie dopełnił żadnego z ustawowych i regulacyjnych wymogów , nie posiada odpowiedniej dokumentacji dla wykazania zgodności z więcej niż kilkoma wymogami lub odmawia poddania się badaniu.

Wydział Urzędu ogłosi w jawnych aktach organu certyfikującego, jakie posiada dla organu certyfikującego datę badania i wynikającą z tego klasyfikację organu certyfikującego.

Zwolnienie z wymogu badania wyników działalności

Wydział Urzędu może zwolnić licencjonowany organ certyfikujący z wymogu podustępu (1) tego ustępu jeśli :

1. organ certyfikujący mający być przedmiotem zwolnienia wniesie na piśmie wniosek o zwolnienie;
2. ostatnie badanie wyników działalności organu certyfikującego jeśli takie miało miejsce wykazało pełną lub zasadniczą zgodność; oraz
3. organ certyfikujący oświadcza pod przysięgą lub przez oficjalne zapewnienie , że jedno lub więcej z następujących stwierdzeń jest prawdziwe w odniesieniu do organu certyfikującego:
    1. organ certyfikujący wydał mniej niż sześć certyfikatów w okresie ostatniego roku i że ogólna wartość zalecanych limitów zaufania wszystkich takich certyfikatów nie wynosi więcej niż 10000 dolarów;
    2. łączna ważność wszystkich certyfikatów wydanych przez organ certyfikujący w ciągu ostatniego roku wynosi mniej niż trzydzieści dni a całość zalecanych limitów zaufania wszystkich takich certyfikatów nie wynosi więcej niż 10000 dolarów.
    3. zalecany limit zaufania wszystkich niezałatwionych certyfikatów i wydanych przez organ certyfikujących wynosi ogółem mniej niż 1000 dolarów.

    Jeśli oświadczenie organu certyfikującego zgodnie z tym podparagrafem fałszywie przedstawi pewien istotny fakt, będzie to uznane za niespełnienie przez ten organ certyfikujący wymogu badania działalności zawartego w tym ustępie.

Jeśli licencjonowany organ certyfikujący jest zwolniony w myśl tego podustępu, Wydział Urzędu ogłosi w jawnych aktach organu certyfikującego jakie prowadzi dla tego organu

certyfikującego oświadczenie stwierdzające, że organ certyfikujący jest zwolniony z wymogu badania.

203. Egzekwowanie wymogów stawianych licencjonowanym organom certyfikującym

Nadzorująca działalność Wydziału Urzędu

Wydział Urzędu może kontrolować czynności licencjonowanego organu certyfikującego, które są istotne pod względem zgodności z postanowieniami tego rozdziału
i wydać nakazy organowi certyfikującemu w celu kontynuacji badania i zabezpieczenia zgodności z tym rozdziałem.

Ograniczenie, zawieszenie lub anulowanie licencji

Wydział może ograniczyć licencję organu certyfikującemu jak przewiduje ustęp 201 za niewykonywanie nakazów Wydziału Urzędu, lub może zawiesić czy anulować licencję organu certyfikującego jak przewiduje ustęp 201.

Kary grzywny

Każdy kto świadomie lub umyślnie łamie postanowienia tego rozdziału lub przepis czy nakaz Wydziału Urzędu podlega karze grzywny w kwocie nie wyższej niż 5.000 dolarów za wykroczenie lub w wysokości 90% zalecanego limitu zaufania danego certyfikatu w zależności od tego co stanowi mniejszą wartość.

Koszt nadzoru

Wydział Urzędu może nakazać organowi certyfikującemu, który złamał postanowienia tego rozdziału, pokryć koszty poniesione przez ten Wydział Urzędu w postępowaniu sądowo administracyjnym związanym z tym nakazem i jego egzekucją.

Postępowanie administracyjne

Wydział Urzędu może korzystać ze swoich uprawnień w myśl tego ustępu zgodnie z procedurą postępowania administracyjnego przepisanego ustawą o postępowaniu administracyjnym , tytuł 63, rozdział 46b, a licencjonowany organ certyfikujący może uzyskać orzeczenie sądowe dotyczące działań Wydziału Urzędu tak jak to przewiduje ustawa o postępowaniu administracyjnym. Wydział Urzędu może także ubiegać się o zwolnienie od obowiązku egzekwowania spełnienia jednego z jego nakazów i może pobierać wszelkie kwoty należne zgodnie z tym ustępem w trybie przewidzianym prawem cywilnym dla egzekwowania nakazów w ustawie o postępowaniu administracyjnym , tytuł 63, rozdział 46b.

204. Zakaz prowadzenia przez organ certyfikujący działań stwarzających ryzyko

Wykluczenie ryzyka nieuzasadnionego handlowo

Żaden z organów certyfikujących, z lub bez licencji, nie będzie prowadził działalności gospodarczej stwarzającej ryzyko strat dla osób podpisujących organu certyfikującego , dla osób polegających na certyfikatach wydanych przez organ certyfikujący, lub dla rejestru.

Publikacja biuletynów ostrzegawczych

Wydział Urzędu może publikować w jednym lub więcej znanych rejestrach krótkie informacje dla osób podpisujących, osób polegających na podpisach cyfrowych, i/lub dla rejestrów o wszelkich działaniach organu certyfikującego , licencjonowanego lub nielicencjonowanego , które stwarzają ryzyko zakazane przez podustęp (1) tego ustępu. Organ certyfikujący wymieniony w informacji , któremu zarzuca się stwarzanie lub przyczynianie się do takiego ryzyka może zaprotestować przeciwko publikacji informacji zgłaszając krótką pisemną obronę. Po otrzymaniu takiego protestu , Wydział Urzędu opublikuje pisemną obronę razem z informacją Wydziału Urzędu i niezwłocznie przekaże protestującemu organowi certyfikującemu zawiadomienie oraz możliwość przesłuchania. Po przesłuchaniu, Wydział Urzędu wycofa informację jeśli jej opublikowanie nie było uzasadnione w myśl tego ustępu, anuluje ją jeśli jej opublikowanie już nie jest uzasadnione, lub będzie ją podtrzymywać lub poprawi ją jeśli pozostanie ona uzasadniona, lub też podejmie dalsze kroki prawne w celu wyeliminowania czy też zmniejszenia ryzyka zakazanego poprzez ten podustęp 1 tego ustępu. Wydział Urzędu ogłosi swoją decyzję w jednym lub więcej uznanych rejestrów.

Nakazy

W sposób przewidziany przez ustawę o postępowaniu administracyjnym , tytuł 63, rozdział 46b, Wydział Urzędu może wydać nakazy lub inne środki cywilno prawne w celu powstrzymania lub ograniczenia organu certyfikującego przed łamaniem postanowień tego ustępu niezależnie od tego czy organ certyfikujący posiada licencję. Ten ustęp nie uprawnia do działania innej osoby jak Wydziału Urzędu.

Część 3 . Obowiązki organów certyfikujących i podpisujących

Streszczenie : Ta część zawiera wymogi działalności licencjonowanego organu certyfikującego, a szczególnie wymogi dotyczące wydawania, zawieszania i anulowania certyfikatów, zapisów, które przypisują parę kluczy podpisu cyfrowego osobie , korporacji lub podmiotowi gospodarczemu określonych przez organ certyfikujący. Ta część również zakazuje przedstawiania nieprawdy w certyfikatach i wymaga aby podpisujący zachowywał poufność klucza prywatnego. Ponadto, ogranicza ona odpowiedzialność organu certyfikującego do zalecanego limitu zaufania określonego w danym certyfikacie.

301. Ogólne wymogi dla organów certyfikujących

Wiarygodne systemy

Licencjonowany organ certyfikujący lub podpisujący będą jedynie używać wiarygodnego systemu :

1. w celu wydania, zawieszenia lub anulowania certyfikatu;
2. w celu publikacji lub zawiadomienia o wydaniu, zawieszeniu lub anulowaniu certyfikatu;
3. do tworzenia prywatnego klucza.

Udostępnienie informacji

Licencjonowany organ certyfikujący będzie ujawniał wszelkie istotne wymogi dotyczące działalności certyfikacyjnej i wszelkie fakty istotne dla wiarygodności certyfikatu , który wydaje lub swojej zdolności do świadczenia usług. Organ certyfikujący może żądać podpisanego, pisemnego i w uzasadnionym zakresie szczegółowego wniosku od określonej osoby oraz zapłaty w rozsądnym wymiarze, jako warunków poprzedzających ujawnienie wymagane w tym ustępie.

302. Wydanie certyfikatu

Warunki wstępne dla wydania certyfikatu

Licencjonowany organ certyfikujący może wydać certyfikat podpisującemu jedynie po spełnieniu wszystkich następujących warunków :

1. organ certyfikujący otrzymał wniosek o wydanie podpisany przez przyszłego podpisującego;
2. organ certyfikujący potwierdził , że :
    1. przyszły podpisujący jest osobą, która będzie wymieniona w wydawanym certyfikacie;
    2. jeśli przyszły podpisujący działa poprzez jednego lub więcej pełnomocników, podpisujący odpowiednio upoważnił pełnomocnika lub pełnomocników do sprawowania pieczy nad prywatnym kluczem podpisującego oraz żądać wydania certyfikatu podającego odpowiedni klucz publiczny;
    3. informacja w wydawanym certyfikacie jest dokładna;
    4. przyszły podpisujący ma prawo do posiadania prywatnego klucza odpowiadającego kluczowi publicznemu, który będzie podany w certyfikacie;
    5. przyszły podpisujący posiada klucz prywatny pozwalający na tworzenie podpisu cyfrowego;
    6. klucz publiczny podany w certyfikacie może być użyty do weryfikacji podpisu cyfrowego złożonego poprzez klucz prywatny posiadany przez przyszłego podpisującego.

Ani organ certyfikujący ani podpisujący czy też obydwaj nie mogą zrezygnować lub odrzucić wymogów tego podustępu.

Publikacja wydanego i akceptowanego certyfikatu

Jeśli podpisujący zaakceptuje wydany certyfikat , organ certyfikujący opublikuje podpisaną kopię certyfikatu w uznanym rejestrze, według uzgodnienia między organem certyfikującym i podpisującym wymienionymi w certyfikacie, o ile kontrakt między organem certyfikującym i podpisującym nie przewiduje inaczej. Jeśli podpisujący nie zaakceptuje certyfikatu , licencjonowany organ certyfikujący nie opublikuje go lub też wycofa publikację jeśli certyfikat został już opublikowany.

Dopuszczenie bardziej rygorystycznych wymogów

Nic w tym ustępie nie powstrzymuje licencjonowanego organu certyfikującego przed stosowaniem norm, wymogów certyfikowania, planów zabezpieczeń lub kontraktowych wymogów , które byłyby bardziej rygorystyczne niż te zawarte w tym rozdziale a jednocześnie zgodne z nimi.

Zawieszenie lub anulowanie przez organ certyfikujący z powodu błędu

Po wydaniu certyfikatu, licencjonowany organ certyfikujący powinien natychmiast go anulować po stwierdzeniu , że nie został wydany zgodnie z tym ustępem. Licencjonowany organ certyfikujący może także zawiesić wydany przez siebie certyfikat w rozsądnym wymiarze czasowym na okres nie dłuższy niż 48 godzin jaki jest potrzebny do zbadania podstaw anulowania zgodnie z tym podustępem. Organ certyfikujący powiadomi podpisującego jak najszybciej jest to możliwe o anulowaniu lub zawieszeniu zgodnie z tym podustępem.

Zawieszenie lub anulowanie poprzez nakaz

Wydział Urzędu może nakazać licencjonowanemu organowi certyfikującemu zawieszenie lub anulowanie certyfikatu wydanego przez ten organ certyfikujący jeśli po przekazaniu wymaganego zawiadomienia i po umożliwieniu organowi certyfikującemu i podpisującemu przesłuchania zgodnie z Ustawą o Postępowaniu Administracyjnym, tytuł 63, rozdział 46b, Wydział Urzędu ustali, że :

1. certyfikat został wystawiony bez zasadniczej zgodności z tym ustępem;
2. niezgodność stwarza znaczne ryzyko dla osób , które polegają na certyfikacie,

Po stwierdzeniu , że nagła sytuacja wymaga natychmiastowego działania i zgodnie z ustawą o postępowaniu administracyjnym Wydział Urzędu może samemu zawiesić certyfikat na okres nie dłuższy niż 48 godzin.

303. Gwarancje i zobowiązania organu certyfikującego przy wydawaniu certyfikatu

Gwarancje dla podpisującego

Wydając certyfikat licencjonowany organ certyfikujący gwarantuje podpisującemu wymienionemu na certyfikacie , że :

1. certyfikat nie zawiera żadnej informacji , o której organ certyfikujący wie że jest fałszywa;
2. certyfikat spełnia wszystkie istotne wymogi tego rozdziału;

3. organ certyfikujący nie przekroczył żadnych ograniczeń swojej licencji wydając certyfikat.

Organ certyfikujący nie będzie zrzekać się lub ograniczać gwarancji tego podustępu.

Podjęcie zobowiązań wobec podpisującego

O ile podpisujący i organ certyfikujący nie uzgodnią inaczej, organ certyfikujący wydając certyfikat, składa podpisującemu obietnicę że :

1. podejmie niezwłoczne działanie w celu zawieszenia lub anulowania certyfikatu zgodnie z ustępem 306 lub 307 poniżej ;
2. zawiadamiać podpisującego w rozsądnym terminie o faktach znanych organowi certyfikującemu które mogą znacznie wpłynąć na ważność lub wiarygodność certyfikatu, który już został wydany.

Oświadczenie po wydaniu certyfikatu

Wydając certyfikat licencjonowany organ certyfikujący zaświadcza wszystkim, którzy w rozsądnym zakresie polegają na informacji zawartej w certyfikacie, że :

1. cała informacja zawarta w certyfikacie i przedstawiona jako informacja potwierdzona przez organ certyfikujący jest dokładna;
2. cała informacja która się wydaje istotna dla wiarygodności certyfikatu, jest podana lub włączona przez odnośnik do certyfikatu;
3. podpisujący zaakceptował certyfikat;
4. licencjonowany organ certyfikujący spełnił wszystkie obowiązujące przepisy prawa tego stanu odnoszące się do wydania certyfikatu.

Oświadczenie przy publikacji

Publikując certyfikat, licencjonowany organ certyfikujący zaświadcza wobec rejestru w którym certyfikat jest publikowany i wobec wszystkich, którzy w rozsądnym zakresie polegają na informacji zawartej w certyfikacie , że organ certyfikujący dokonał wydania certyfikatu podpisującemu.

304. Przedstawianie danych i obowiązki przy akceptacji certyfikatu

Sugerowane twierdzenia podpisującego

Przyjmując certyfikat wydany przez licencjonowany organ certyfikujący, podpisujący wymieniony w certyfikacie zaświadcza wobec wszystkich , którzy w rozsądnym zakresie polegają na informacji zawartej w certyfikacie, że :

1. podpisujący legalnie posiada klucz prywatny odpowiadający kluczowi publicznemu wymienionemu w certyfikacie;
2. wszystkie twierdzenia podpisującego skierowane do organu certyfikującego i istotne dla informacji zawartych w certyfikacie są prawdziwe;

3. wszelkie istotne stwierdzenia podpisującego skierowane do organu certyfikującego lub dokonane w certyfikacie i nie potwierdzone przez organ certyfikujący przy wydawaniu certyfikatu są prawdziwe.

Przedstawienie danych poprzez pełnomocnika lub domniemanego pełnomocnika podpisującego

Wnosząc w imieniu zleceniodawcy o wydanie certyfikatu podającego zleceniodawcę jako podpisującego osoba składająca prośbę prawnie zaświadcza wszystkim , którzy w rozsądnym zakresie polegają na informacji zawartej w certyfikacie , że wnioskodawca :

1. posiada wszelkie uprawnienia jakie prawnie są wymagane do ubiegania się o certyfikat podający zleceniodawcę jako podpisującego;
2. posiada uprawnienie do składania cyfrowego podpisu w imieniu zleceniodawcy, a jeśli to uprawnienie jest pewien sposób ograniczone, istnieją stosowne zabezpieczenia przed podpisem cyfrowym przekraczającym uprawnienia tej osoby.

Ograniczenie zrzeczenia się lub zwolnienia z odpowiedzialności materialnej

Nikt nie może zrzec się lub poprzez kontrakt ograniczyć zakres stosowania tego ustępu, ani też uzyskać zwolnienia od odpowiedzialności materialnej za związane z nim skutki jeśli zrzeczenie się, ograniczenie lub zwolnienie od odpowiedzialności materialnej spowoduje ograniczenie odpowiedzialności za fałszywe przedstawienie danych wobec osób, które w rozsądnym zakresie polegają na certyfikacie.

Zwolnienie organu certyfikującego od odpowiedzialności materialnej przez podpisującego

Poprzez zaakceptowanie certyfikatu, podpisujący zwalnia wydający certyfikat organ certyfikujący od odpowiedzialności materialnej za straty czy szkody spowodowane wydaniem lub publikacją certyfikatu w wypadku :

1. fałszywego przedstawienia istotnego faktu przez podpisującego;
2. nieujawnienia przez podpisującego istotnego faktu;

jeśli przedstawienie faktu lub nieujawnienie miało na celu oszukanie organu certyfikującego lub osoby polegającej na certyfikacie, lub też zaszło z powodu zaniedbania. Jeśli organ certyfikujący wydał certyfikat na prośbę jednego lub dwóch pełnomocników podpisującego , pełnomocnik lub pełnomocnicy osobiście zobowiązują się zwolnić organ certyfikujący od odpowiedzialności materialnej zgodnie z tym podustępem, jak gdyby byli akceptującymi w ich prawach. Zwolnienia przewidzianego w tym podustępie nie można się zrzec lub poprzez kontrakt ograniczyć jego zakresu; jednakże kontrakt może zawierać logicznie powiązane dodatkowe warunki dotyczące zabezpieczenia przed odpowiedzialnością materialną.

Fałszywe oświadczenia

Uzyskując informację o podpisującym, istotną przy wydawaniu certyfikatu , organ certyfikujący może żądać aby podpisujący poświadczył dokładność stosownej informacji pod przysięgą lub oficjalnym zapewnieniem prawdy pod odpowiedzialnością karną za składanie fałszywych oświadczeń pod przysięgą.

305. Kontrola prywatnego klucza

Obowiązek podpisującego do bezpiecznego przechowywania klucza

Akceptując certyfikat wydany przez licencjonowany organ certyfikujący , podpisujący określony w tym certyfikacie podejmuje obowiązek sprawowania w rozsądnym zakresie kontroli nad kluczem prywatnym i zapobiegania ujawnieniu klucza osobie nieuprawnionej do tworzenia podpisu cyfrowego.

Prywatny klucz jest własnością podpisującego

Prywatny klucz jest osobistą własnością podpisującego , który go legalnie posiada.

Organ certyfikujący pełni rolę powiernika jeśli posiada klucz prywatny podpisującego

Jeśli organ certyfikujący posiada klucz prywatny odpowiadający kluczowi publicznemu wymienionemu w certyfikacie, który wydał, organ certyfikujący posiada klucz prywatny jako powiernik podpisującego wymienionego w certyfikacie, i może używać tego klucza tylko za uprzednią pisemną aprobatą podpisującego, chyba że podpisujący umyślnie udziela klucz organowi certyfikującemu i celowo pozwala organowi certyfikującemu na posiadanie klucza prywatnego na innych warunkach.

306. Zawieszenie certyfikatu

Zawieszenie certyfikatu przez organ certyfikujący

O ile nie zostanie to inaczej uzgodnione przez organ certyfikujący i podpisującego, licencjonowany organ certyfikujący , który wydał certyfikat nie będący certyfikatem transakcyjnym , zawiesza certyfikat na okres nie przekraczający 48 godzin :

1. na wniosek osoby określającej się jako podpisujący wymieniony na certyfikacie lub jako osoba , której wiadomo o naruszeniu bezpieczeństwa prywatnego klucza podpisującego, taka jak pełnomocnik, współpracownik, pracownik, lub członek najbliższej rodziny podpisującego;
2. nakazem Wydziału Urzędu zgodnie z powyższym podustępem 302(5).

Organ certyfikujący nie musi potwierdzać tożsamości lub upoważnienia osoby żądającej zawieszenia.

Zawieszenie przez Wydział Urzędu, urzędnika sądowego lub okręgowego

O ile certyfikat nie przewiduje inaczej lub certyfikat nie jest certyfikatem transakcyjnym , Wydział Urzędu, urzędnik sądu lub urzędnik okręgowy może zawiesić certyfikat wydany przez licencjonowany organ certyfikujący na okres 48 godzin jeśli :

1. osoba określająca siebie jako podpisujący wymieniony na certyfikacie lub jako osoba taka jak agent, współpracownik, pracownik, lub członek najbliższej rodziny podpisującego żąda zawieszenia;
2. wnioskodawca twierdzi , że organ certyfikujący , który wydał certyfikat nie jest osiągalny.

Wydział Urzędu, urzędnik sądu lub urzędnik okręgowy może żądać aby osoba wnosząca o zawieszenie przedstawiła dowody łącznie z oświadczeniem pod przysięgą lub oficjalnym zapewnieniem dotyczącym jego lub jej tożsamości, upoważnieniem, i/lub nieosiągalności wydającego certyfikat organu certyfikującego i może odmówić zawieszenia certyfikatu według swojego uznania. Wydział Urzędu i/lub organy wymiaru sprawiedliwości mogą wszcząć badanie dotyczące zawieszenia przez Wydział Urzędu lub urzędników sądowych lub okręgowych rozpatrując ewentualne wykroczenie przez osoby wnoszące o zawieszenie.

Zawiadomienie

Natychmiast po zawieszeniu certyfikatu przez licencjonowany organ certyfikujący , licencjonowany organ certyfikujący opublikuje podpisane zawiadomienie o zawieszeniu w rejestrze określonym w certyfikacie dla celów publikacji zawiadomienia o zawieszeniu. Jeśli w ten sposób są określone jeden lub więcej rejestrów to licencjonowany organ certyfikujący opublikuje podpisane zawiadomienie o zawieszeniu we wszystkich takich rejestrach. Jeśli w taki sposób określony rejestr już nie istnieje lub odmawia przyjęcie publikacji, lub też rejestr tego rodzaju nie jest uznawany zgodnie z ustępem 501 z tego rozdziału to licencjonowany organ certyfikujący także opublikuje zawiadomienie w uznawanym rejestrze. Jeśli certyfikat jest zawieszony przez Wydział Urzędu lub urzędnika sądowego czy też okręgowego, Wydział Urzędu lub urzędnik wydadzą zawiadomienie według wymogów tego podustępu dla licencjonowanego organu certyfikującego, pod warunkiem że osoba żądająca zawieszenia pokryje z góry opłatę wymaganą przez rejestr dla publikacji zawiadomienia o zawieszeniu.

Zakończenie żądanego zawieszenia

Organ certyfikujący zakończy zawieszenie wszczęte na żądanie tylko :

1. jeśli podpisujący wymieniony na zawieszonym certyfikacie żąda zakończenia zawieszenia, organ certyfikujący potwierdził , że osoba wnosząca o zawieszenie jest podpisującym lub pełnomocnikiem podpisującego upoważnionym do zakończenia zawieszenia;
2. kiedy organ certyfikujący odkryje i potwierdzi , że wniosek o zawieszenie został złożony bez upoważnienia podpisującego, pod warunkiem, że ten podustęp nie wymaga aby organ certyfikujący potwierdzał wniosek o zawieszenie.

Alternatywy procedur umownych

Umowa między podpisującym a licencjonowanym organem certyfikującym może ograniczyć lub uniemożliwić żądane zawieszenie przez organ certyfikujący, lub może przewidzieć inne postanowienie dla zakończenia wnoszonego zawieszenia. Jeśli jednak kontrakt ogranicza lub uniemożliwia zawieszenie przez Wydział Urzędu, lub urzędnika sądowego czy też urzędnika okręgowego kiedy wydający certyfikat organ certyfikujący nie jest osiągalny, ograniczenie lub uniemożliwienie będzie skuteczne tylko jedynie jeśli zawiadomienie o tym będzie opublikowane w tym certyfikacie.

Zakaz fałszywego lub nieupoważnionego wniosku o zawieszenie

Nikt nie może świadomie lub umyślnie fałszywie przedstawiać organowi certyfikującemu swojej tożsamości lub upoważnienia wnosząc o zawieszenie certyfikatu. Złamanie postanowienia tego podustępu stanowi wykroczenie klasy B.

Skutek zawieszenia

Podpisujący jest zwolniony z obowiązku bezpiecznego przechowywania klucza prywatnego zgodnie z ustępem 305 (1) w okresie zawieszenia certyfikatu.

307. Anulowanie certyfikatu

Anulowanie na żądanie

Licencjonowany organ certyfikujący anuluje certyfikat , który wydał lecz który nie jest certyfikatem transakcyjnym po :

1. otrzymaniu wniosku o anulowanie przez podpisującego wymienionego na certyfikacie;
2. potwierdzeniu , że osoba wnosząca o anulowanie jest tym podpisującym, lub jest agentem tego podpisującego z upoważnieniem do wnoszenia o anulowanie.

Czas wprowadzenia żądanego anulowania

Licencjonowany organ certyfikujący potwierdzi wniosek o anulowanie i anuluje certyfikat w ciągu jednego dnia roboczego po otrzymaniu zarówno pisemnego wniosku podpisującego jak i dowód w rozsądnej mierze wystarczający dla potwierdzenia tożsamości i upoważnienia osoby wnoszącej o zawieszenie.

Anulowanie w wypadku śmierci podpisującego

Licencjonowany organ certyfikujący anuluje certyfikat , który wydał :

1. po otrzymaniu poświadczonego odpisu aktu zgonu podpisującego, lub innego dowodu śmierci podpisującego;
2. po przedstawieniu dokumentów powodujących rozwiązanie się podpisującego lub po potwierdzeniu przez inne dowody, że podpisujący został rozwiązany lub też przestał istnieć.

Anulowanie niepewnych certyfikatów bez żądania

Licencjonowany organ certyfikujący może anulować jeden lub więcej certyfikatów , które wydał jeśli certyfikaty są lub stają się niepewne niezależnie od tego czy podpisujący zgadza się na anulowanie i pomimo jakiegokolwiek przeciwnego postanowienia w kontrakcie pomiędzy podpisującym i organem certyfikującym.

Zawiadomienie

Natychmiast po anulowaniu certyfikatu przez licencjonowany organ certyfikujący, licencjonowany organ certyfikujący opublikuje podpisane zawiadomienie o anulowaniu w rejestrze określonym w certyfikacie dla publikacji zawiadomień o anulowaniu. Jeśli jeden lub więcej rejestrów jest w ten sposób określonych to licencjonowany organ certyfikujący opublikuje podpisane zawiadomienie o anulowaniu we wszystkich takich rejestrach. Jeśli jeden z tak określonych rejestrów nie istnieje już lub odmawia przyjęcia publikacji, lub jeśli taki rejestr nie jest uznawany zgodnie z ustępem 501 tego rozdziału , to licencjonowany organ certyfikujący także opublikuje zawiadomienie w uznawanym rejestrze.

Wpływ wniosku o anulowanie na podpisującego

Podpisujący przestaje zaświadczać jak przewidziano w powyższym ustępie 304 i nie ma dalszego obowiązku zachowania bezpieczeństwa prywatnego klucza jak wymaga ustęp 305 w odniesieniu do certyfikatu , o którego anulowanie wnosił podpisujący, co następuje gdy :

1. zawiadomienie o anulowaniu jest opublikowane jak tego wymaga podustęp (5) tego ustępu; lub
2. dwa dni robocze po tym jak podpisujący wnosi na piśmie o anulowanie, dostarcza wydającemu certyfikat organowi certyfikującemu informację w rozsądnej mierze dostateczną dla potwierdzenia wniosku oraz pokryje opłatę wymaganą kontraktem,

zależnie od tego , które z nich nastąpi pierwsze.

Wpływ powiadomienia na organ certyfikujący

Po powiadomieniu jak wymaga podustęp (5) tego ustępu, licencjonowany organ certyfikujący jest uwolniony od swoich gwarancji związanych z wydaniem anulowanych certyfikatów i przestaje zaświadczać jak przewidują podustępy 303 (2) oraz 303 (3) w odniesieniu do anulowanych certyfikatów.

308. Wygaśnięcie certyfikatu

Ogólny wymóg

Certyfikat musi podawać datę z jaką wygasa, co nastąpi nie później niż trzy lata po jego wydaniu o ile certyfikat nie określa dłuższego okresu ważności.

Skutek

Gdy upływa ważność certyfikatu, podpisujący i organ certyfikujący przestają zaświadczać jak przewiduje to ten rozdział i organ certyfikujący jest zwolniony z swoich obowiązków wynikających z wydania wygasłego certyfikatu.

309. Zalecany limit zaufania i odpowiedzialności

Znaczenie zalecanego limitu zaufania

Określając zalecany limit zaufania w certyfikacie , wydający go organ certyfikujący oraz akceptująca osoba podpisująca zalecają , żeby polegano na certyfikacie tylko w takim zakresie, żeby całkowita kwota narażana na ryzyko nie przewyższała zalecanego limitu zaufania.

Limit odpowiedzialności dla licencjonowanych organów certyfikujących

O ile licencjonowany organ certyfikujący nie zrzeknie się zastosowania tego podustępu, licencjonowany organ certyfikujący :

1. nie będzie odpowiedzialny za wszelkie straty wynikające z zawierzenia fałszywemu lub sfałszowanemu podpisowi cyfrowemu podpisującego jeśli w związku z fałszywym lub sfałszowanym podpisem cyfrowym organ certyfikujący spełnił wszelkie istotne wymogi tego rozdziału;
2. nie będzie odpowiedzialny powyżej kwoty określonej w certyfikacie jako zalecany limit zaufania w razie :
    1. straty spowodowanej zawierzeniem niewłaściwemu przedstawieniu w certyfikacie faktu, który licencjonowany organ certyfikujący ma potwierdzić;
    2. niewypełnienia postanowień ustępu 302 w trakcie wydawania certyfikatu ;
3. będzie odpowiedzialny tylko za bezpośrednie kompensowanie straty we wszystkich postępowaniach mających pokryć straty wynikające z zawierzenia certyfikatowi. Bezpośrednie kompensaty nie obejmują :
    1. kompensat nałożonych karnie lub nawiązki ;
    2. kompensat za stracone zyski, oszczędności lub możliwości;
    3. kompensaty za spowodowany ból czy cierpienie.

310. Wypłata na podstawie odpowiedniej gwarancji

Prawo skarżącego do wypłaty

Pomimo jakichkolwiek przeciwnych postanowień w odpowiedniej gwarancji :

1. jeśli stosowna gwarancja jest rewersem gwarancyjnym to od rewersu można odzyskać pełną kwotę z ograniczonego prawa do zapłaty od głównego dłużnika określonego na rewersie lub jeśli jest więcej niż jedno takie ograniczone prawo do zapłaty w czasie okresu ważności rewersu, udział proporcjonalny, do maksymalnej wielkości całej odpowiedzialności gwaranta równej kwocie rewersu;
2. jeśli stosowna gwarancja jest akredytywą, od wydającej finansowej instytucji można odzyskać pełną kwotę ograniczonego prawa do zapłaty obciążającej osobę podaną w akredytywie lub jeżeli jest więcej niż jedno takie ograniczone prawo do zapłaty w okresie ważności akredytywy, udział proporcjonalny, do maksymalnej wysokości całkowitej odpowiedzialności wystawcy równej wysokości kredytu.

Skarżący może stopniowo odzyskać pieniądze na podstawie tej samej stosownej gwarancji pod warunkiem , że całkowita odpowiedzialność ze stosownej gwarancji wobec wszystkich

osób mających ograniczone prawo do zapłaty w okresie gwarancyjnym nie przekroczy kwoty stosownej gwarancji.

Honoraria prawnika

Oprócz odzyskanej kwoty z ograniczonego prawa zapłaty , skarżący może odzyskać na podstawie gwarancji , aż do wyczerpania jej, honoraria prawnika, w rozsądnym wymiarze i koszty sądowe poniesione przez skarżącego dochodzącego swych roszczeń pod warunkiem , że całkowita wysokość odpowiedzialności ze stosownej gwarancji wobec wszystkich osób mających ograniczone prawo zapłaty lub odzyskujących honoraria prawników w tym okresie nie przekroczy kwoty stosownej gwarancji.

Procedura dochodzenia roszczeń

Aby uzyskać ograniczone prawo zapłaty wobec gwaranta lub wystawcy stosownej gwarancji , skarżący :

1. wniesie pisemne powiadomienie o roszczeniu do Wydziału Urzędu podając swoje nazwisko, adres skarżącego, żądaną kwotę oraz podstawy do ograniczonego prawa wypłaty oraz wszelkie inne informacje wymagane przepisami Wydziału Urzędu;
2. dołączy do powiadomienia poświadczony odpis orzeczenia na którym opiera się ograniczone prawo do wypłaty.

Uzyskanie ograniczonego prawa do wypłaty z sumy stosownej gwarancji jest zależne od wypełnienia w zasadniczej mierze warunków tego podustępu.

Termin wnoszenia roszczeń

Uzyskanie ograniczonego prawa do wypłaty z sumy stosownej gwarancji będzie na zawsze uniemożliwione o ile roszczenie nie zostanie wniesione zgodnie z wymogami powyższego podustępu (3) w okresie dwóch trzech lat po naruszeniu rozdziału, który stanowi podstawę roszczenia.

Część 4. Moc prawna podpisu cyfrowego

Streszczenie : Ta część stwierdza, że podpis cyfrowy ma w zasadzie te same prawne konsekwencje co podpis odręczny na papierze.

401. Spełnienie wymogów podpisu

Ogólnie

Kiedy przepis prawa wymaga podpisu lub przewiduje pewne prawne konsekwencje w razie gdy nie ma podpisu to wymóg taki jest spełniany za pośrednictwem podpisu cyfrowego, jeśli :

1. ten podpis cyfrowy jest weryfikowany poprzez odniesienie do klucza publicznego podawanego przez ważny certyfikat wydany przez licencjonowany organ certyfikujący;

2. ten podpis cyfrowy został złożony przez podpisującego w celu podpisania komunikatu;
3. odbiorca nie wie lub nie został powiadomiony , że podpisujący albo :
    1. złamał swoje zobowiązanie jako podpisujący; lub
    2. nie posiada legalnie prywatnego klucza zastosowanego do złożenia podpisu.

Inne podpisy

Jednakże, rozdział niniejszy nie uniemożliwia użycie jakiegokolwiek symbolu z taką samą ważnością jak podpis zgodne z innym obowiązującym prawem takim jak Jednolity kodeks handlowy stanu Utah ustęp 70A-1-201(39).

Komisja podatkowa

Ten ustęp nie ogranicza uprawnienia Stanowej Komisji Podatkowej do ustalania formy deklaracji podatkowych lub innych dokumentów wnoszonych do Stanowej Komisji Podatkowej.

402. Niepewne podpisy cyfrowe

O ile nie zostanie inaczej przewidziane prawem lub kontraktem, odbiorca podpisu cyfrowego przyjmuje ryzyko , że podpis cyfrowy jest sfałszowany, jeśli zaufanie do podpisu cyfrowego nie jest rozsądne w danych okolicznościach. Jeśli odbiorca zdecyduje się nie polegać na podpisie cyfrowym zgodnie z tym ustępem niezwłocznie powiadomi podpisującego o swojej decyzji żeby nie polegać na podpisie cyfrowym i o podstawach tej decyzji.

403. Dokument podpisany cyfrowo ma formę pisemną

Komunikat jest ważny , egzekwowany, i skuteczny tak jak gdyby był napisany na papierze jeśli :

1. zawiera podpis cyfrowy obejmujący jego całość ; oraz
2. jest weryfikowany poprzez klucz publiczny podany na certyfikacie, który :
    1. został wydany przez licencjonowany organ certyfikujący; oraz
    2. był ważny w czasie kiedy tworzono podpis cyfrowy.

Rozdział ten jednak nie wyklucza uznania jakiegokolwiek komunikatu, dokumentu, czy też zapisu za wykonany w formie pisemnej czy też na piśmie zgodnie z innym obowiązującym prawem.

404. Oryginały podpisywane cyfrowo

Kopia cyfrowo podpisanego komunikatu jest skuteczna, ważna i egzekwowana tak jak oryginał komunikatu, o ile nie jest wiadome , że podpisujący wskazał, że wybrane wystąpienie cyfrowo podpisanego komunikatu jest jedynym oryginałem, a w takim przypadku tylko ten stanowi ważny, skuteczny i egzekwowany komunikat.

405. Certyfikat jako akt uznania

O ile prawo czy kontrakt nie przewidują inaczej , certyfikat wydany przez licencjonowany organ certyfikujący jest uznaniem podpisu cyfrowego weryfikowanego poprzez klucz publiczny wymieniony na certyfikacie, niezależnie od tego czy słowa uznania pojawiają się przy podpisie cyfrowym i czy podpisujący fizycznie stawił się przed organem certyfikującym kiedy wykonano podpis cyfrowy, jeśli podpis cyfrowy :

1. może być weryfikowany przez ten certyfikat; oraz
2. złożono go kiedy certyfikat był ważny.

406. Założenia przy rozstrzyganiu sporów

Rozstrzygając spór dotyczący podpisu cyfrowego, sąd tego stanu zakłada , że :

1. Certyfikat podpisany cyfrowo przez licencjonowany organ certyfikujący albo :
    1. opublikowany w uznanym rejestrze; lub
    2. udostępniony przez wydający organ certyfikujący lub też przez podpisującego określonego na certyfikacie

jest wydany przez organ certyfikujący , który podpisał go cyfrowo i jest zaakceptowany przez podpisującego jaki został w nim określony.
2. Informacja podana we ważnym certyfikacie i potwierdzona przez licencjonowany organ certyfikujący, który wydaje certyfikat jest dokładna.
3. Jeśli podpis cyfrowy jest weryfikowany kluczem publicznym podanym w ważnym certyfikacie wydanym przez licencjonowany organ certyfikujący :
    1. ten podpis cyfrowy jest podpisem cyfrowym podpisującego określonego przez ten certyfikat;
    2. ten podpis cyfrowy został złożony przez tego podpisującego z zamiarem podpisania komunikatu; oraz
    3. odbiorca tego podpisu cyfrowego nie wie , lub nie został powiadomiony że podpisujący :
        1. złamał swoje zobowiązanie jako podpisujący, lub
        2. nie posiada legalnie prywatnego klucza używanego do składania podpisu cyfrowego.
4. Podpis cyfrowy został utworzony zanim on został opatrzony datownikiem przez osobę niezaangażowaną używającą wiarygodnego systemu.

Część 5. Rejestry

Streszczenie: Ta część pozwala Wydziałowi Urzędu na uznanie rejestru na żądanie. Ogranicza to odpowiedzialność rejestrów do ich funkcji sprawozdawczej, oraz wyklucza odpowiedzialność jaka mogłaby być zakładana w związku z dokładnością certyfikatów i innej informacji zamieszczonej przez innych w rejestrze.

501. Uznanie rejestrów

Warunki uznania

Wydział Urzędu uzna jeden lub więcej rejestrów , po stwierdzeniu , że rejestr , który ma być uznany :

1. działa pod kierunkiem licencjonowanego organu certyfikującego;
2. obejmuje bazę danych zawierającą :
    1. certyfikaty publikowane w rejestrze;
    2. zawiadomienia o zawieszonych lub anulowanych certyfikatach publikowane przez licencjonowane organy certyfikujące lub inne osoby zawieszające lub anulujące certyfikaty;
    3. jawne akta organu certyfikującego dla licencjonowanych organów certyfikujących;
    4. wszystkie nakazy lub zalecenia publikowane przez Wydziału Urzędu o charakterze regulującym organy certyfikujące; oraz
    5. wszelkie inne informacje według wymogu Wydziału Urzędu.
3. działa poprzez system wiarygodny;
4. nie zawiera znaczącej ilości informacji o której Wydziału Urzędu wie że jest lub prawdopodobnie jest nieprawdziwa, niedokładna lub niepewna;
5. zawiera certyfikaty publikowane przez organy certyfikujące , które muszą przestrzegać wymogów działalności , które Wydział Urzędu uznaje za zasadniczo podobne lub bardziej rygorystyczne dla organu certyfikującego w stosunku do wymogów tego stanu;
6. prowadzi archiwum certyfikatów , które zostały zawieszone lub anulowane , lub też które wygasły w ciągu przynajmniej ostatnich trzech lat; oraz
7. przestrzega innych uzasadnionych wymogów ustanowionych przepisem Wydziału Urzędu.

Procedura uznania

Rejestr może zwrócić się do Wydziału Urzędu o uznanie wnosząc pisemną prośbę oraz dostarczając dowodu na to , żeby Wydziału Urzędu uznał , że są spełnione warunki uznania. Wydział Urzędu ustali czy udzielić lub odmówić zgody w trybie przewidzianym dla orzekania przez Ustawę o Postępowaniu Administracyjnym, tytuł 63, rozdział 46 b.

Cofnięcie uznania

Rejestr może cofnąć swoje uznanie poprzez trzydziestodniowe wypowiedzenie wniesione do Wydziału Urzędu. Poza tym, Wydział Urzędu może cofnąć uznanie rejestru :

1. po upływie terminu ważności określonego przez Wydział Urzędu przy udzielaniu uznania; lub
2. zgodnie z orzecznictwem zaleconym przez Ustawę o Postępowaniu Administracyjnym, tytuł 63, rozdział 46b, jeśli stwierdza , że rejestr już nie spełnia warunków uznania wymienionych w tym ustępie lub w wymogach Wydziału Urzędu.

502. Odpowiedzialność rejestrów

Publikacja ogłoszenia o zawieszeniu lub anulowaniu

Pomimo zrzeczenia się przez rejestr lub kontraktu przewidującego inaczej między rejestrem, organem certyfikującym , lub podpisującym, rejestr będzie odpowiedzialny za straty poniesione przez osobę ,które w rozsądnym zakresie polegała na podpisie cyfrowym weryfikowanym poprzez klucz publiczny podany w zawieszonym lub anulowanym certyfikacie, jeśli strata była poniesiona po więcej niż jednym dniu roboczym od odbioru przez rejestr wniosku o zamieszczenie ogłoszenia o zawieszeniu lub anulowaniu, a rejestr nie opublikował tego ogłoszenia kiedy dana osoba zawierzyła podpisowi cyfrowemu.

Ograniczenie odpowiedzialności

O ile nie nastąpi zrzeczenie, uznany rejestr lub właściciel czy też operator uznanego rejestru :

1. nie będzie odpowiedzialny za niedopełnienie zapisu ogłoszenia o zawieszeniu lub anulowaniu, o ile rejestr nie otrzyma zgłoszenia publikacji oraz nie upłynie jeden dzień roboczy od otrzymania zgłoszenia;
2. nie będzie odpowiedzialny zgodnie z podustępem (1) tego ustępu powyżej kwoty określonej w certyfikacie jako zalecany limit zaufania;
3. będzie odpowiedzialny zgodnie z podustępem (1) tego ustępu tylko za bezpośrednie wyrównawcze odszkodowanie, które nie będzie obejmować:
    1. karnego odszkodowania i nawiązki;
    2. odszkodowania za stracone zyski, oszczędności lub możliwości; lub
    3. odszkodowanie za ból lub cierpienie;
4. nie będzie odpowiedzialny za niewłaściwe przedstawienie faktów w certyfikacie opublikowanym przez licencjonowany organ certyfikujący;
5. nie będzie odpowiedzialny za dokładne zapisanie lub złożenie informacji , którą urzędnik okręgowy lub sądowy , lub Wydział Urzędu opublikował zgodnie z tym co wymaga lub na co zezwala się w tym rozdziale, łącznie z informacją o zawieszeniu lub anulowaniu certyfikatu;
6. nie będzie odpowiedzialny za złożenie informacji dotyczącej organu certyfikującego, certyfikatu, lub podpisującego jeśli taka informacja jest opublikowana zgodnie z tym co wymaga lub na co zezwala ten rozdział lub przepis Wydziału Urzędu, lub jest opublikowane na zlecenie Wydziału Urzędu wykonującego swoje funkcje licencjonowania i regulacji zgodnie z tym rozdziałem.

Proponowane poprawki do kodeksu karnego stanu Utah
Tytuł 76 (1996) załączony do kodeksu stanu Utah

Proponuje się następujące poprawki aby żeby kodeks karny stanu Utah mógł odpowiednio traktować oszustwo oraz fałszerstwo w działalności gospodarczej posługującej się telekomunikacją.

Ogólne Definicje

Podustęp 76-1-601 (12) jest poprawiony i przedstawia się w całości następująco:

(12) "Forma pisemna" obejmuje pismo odręczne, maszynowe, druk, przechowywanie elektroniczne lub przesyłanie lub też inny sposób zapisu informacji lub utrwalania jej w takiej formie żeby można ją było zachować.

Definicje zakazu fałszerstwa

Podustęp 76-6-501 (2) jest poprawiony i przedstawia się w całości następująco:

(2) Jak używano w tym ustępie, "forma pisemna" obejmuje druk, przechowywanie elektroniczne lub przesyłanie lub też inny sposób zapisu cennej informacji , w tym takie formy jak :
(a) czek, żeton, znaczek, pieczęć, karta kredytowa, odznaka, znak handlowy, pieniądze oraz każdy inny symbol wartości, prawa , przywileju lub identyfikacji;
(b) papier wartościowy, znaczek skarbowy, lub każdy inny dokument lub pismo wystawione przez rząd lub jego agendę;
(c) papier wartościowy , akcja, obligacja, weksel lub każdy inny dokument czy pismo przedstawiające udział lub roszczenie do majątku, lub też udział pieniężny czy też roszczenie w stosunku do osoby lub przedsiębiorstwa.

ZASADY OGÓLNE

KODEKS POSTĘPOWANIA ADMINISTRACYJNEGO STANU UTAH.

R154-10

101. Definicje

Definicje pochodzące z Ustawy o podpisie cyfrowym

W dokumencie tym zostały włączone poprzez odnośniki definicje pochodzące z Ustawy o podpisie cyfrowym.

Definicje pojęć:

1. "*Unikalna nazwa*" oznacza daną jednoznacznie identyfikującą osobę, do której ta nazwa należy
2. "*ISO*" oznacza Organizację Standartów Międzynarodowych
3. "*pierwotny wykaz przepisów wykonawczych dotyczących certyfikacji*" oznacza taki wykaz przepisów wykonawczych, który zawiera odnośniki do pozostałych istotnych wykazów;
4. "*Ustawa Stanu Utah*" oznacza Ustawę o podpisie cyfrowym Stanu Utah w wersji aktualnej

NADZÓR ORGANU CERTYFIKUJĄCEGO

201. Odpowiednia gwarancja

Odpowiedni poziom zaufania jest kwotowo równy lub wyższy niż większa z poniższych kwot:

1. 100 % najwyższego zalecanego poziomu zaufania certyfikatu, wydanego przez Organ Certyfikujący na okres ważności licencji tegoż Organu Certyfikującego, lub
2. 35 % sumy zalecanych poziomów zaufania wszystkich certyfikatów publikowanych przez Organ Certyfikujący, za wyjątkiem certyfikatów unieważnionych oraz wygasłych

202. Akta jawne Organu Certyfikującego

Zawartość

Akta jawne Organu Certyfikującego zawierają:

1. wskazanie, że akta jawne Organu Certyfikującego są udostępniane i zarządzane przez dany stan;
2. nazwę, adres oraz numer telefonu Organu Certyfikującego;
3. numer faksu Organu Certyfikującego, jeżeli taki posiada;
4. adress poczty elektronicznej (e-mail) lub inny adress dzięki któremu można kontaktować się z Organem Certyfikującym drogą elektroniczną;
5. unikalną nazwę Organu Certyfikującego;
6. aktualny klucz lub klucze publiczne Organu Certyfikującego, za pomocą których można weryfikować podpisy cyfrowe na publikowych certyfikatach;

7. ograniczenia, jeżeli takie istnieją, umieszczone na licencji Organu Certyfikującego, stosownie do punktu 201(3);
8. datę oraz przyczyny unieważnienia lub czasowego zawieszenia licencji Organu Certyfikującego, jeżeli takie unieważnienie lub zawieszenie nastąpiło;
9. kwotę odpowiedniego poziomu zaufania Organu Certyfikującego;
10. łączną kwotę wszelkich reklamacji przechowywanych przez Organ Certyfikujący dotyczących zapłaty za odpowiedni poziom zaufania;
11. krótki opis wszelkich znanych Wydziałowi Urzędu ograniczeń dotczących zobowiązań finansowych Organu Certyfikującego oraz możliwości spłaty odszkodowań za niedopełnienie przez niego obowiązków, (o ile ten ustęp nie precyzuje stosownych ograniczeń)
12. klasyfikację wynikającą z ustępu 202 (2) dotyczącą stosowania się Organu Certyfikującego do niniejszego rozdziału, jak również wyniki i datę ostatniej kontroli działalności Organu Certyfikującego;
13. wszelkie zdarzenia, które istotnie wpływają na zdolność prowadzenia działalności przez Organ Certyfikujący lub na prawomocność certyfikatu, publikowanego w rejestrze Wydziału Urzędu lub w uznanym rejestrze;
14. datę unieważnienia lub zawiesznia certyfikatu, zawierającego klucz publiczny, potrzebny do weryfikacji jednego lub więcej certyfikatów Organu Certyfikującego oraz
15. o ile Organ Certyfikujący istotny pierwotny wykazu przepisów wykonawczych, wskazanie jego lokalizacji, prorcedurę dzięki której może on być uzyskany, jego format i strukturę, autora oraz datę, stosownie do punktu 302.

Format

Akta jawne Organu Certyfikującego są podpisywane cyfrowo w ich oficjalnej treści przez Wydział Urzędu.

Zarezerwowane dla przyszłej specyfikacji ASN. 1

Akta publiczne

Zgodnie z ustawą Stanu Utah dotyczącej dostępu rządu do rejestrów prawnych, Kodeksu (Ann.) Stanu Utah (tytuł 63, rozdział 2), akta jawne Organu Certyfikującego są aktami publicznymi Stanu Utah

FUNKCJONOWANIE ORGANU CERTYFIKUJĄCEGO

201. Format i zawartość certyfikatu

Zawartość obowiązkowa

Certyfikat wydany przez uprawniony Organ Certyfikujący zawiera (lub posiada odnośniki do):

1. zapis informujący o zgodności typu certyfikatu z tymi przepisami;
2. zapis, że Organ Certyfikujący wydający dany certyfikat, posiada licencję stanową;
3. numer seryjny certyfikatu, który musi być unikalny pośród certyfikatów ; wydawanych przez Organ Certyfikujący;
4. wskazówkę, jeżeli dany certyfikat jest certyfikatem transakcyjnym;
5. nazwę, pod którą podpisujący certyfikat jest ogólnie znany;

6. unikalną nazwa podpisującego;
7. klucz publiczny, odpowiadający kluczowi prywatnemu, będącemu w posiadaniu podpisującego;
8. identyfikator algorytmów skojarzonych z odpowiednim kluczem publicznym podpisującego;
9. datę i czas zarówno wydania jak i akceptacji certyfikatu;
10. datę i czas wygaśnięcia ważności certyfikatu;
11. unikalną nazwa Organu Certyfikującego wydającego certyfiakt;
12. identyfikator algorytmu (algorytmów) stosowanych przy podpisywaniu certyfikatów, w formacie powszechnie przyjętym i stosowanym w przez podpisujących;
13. zalecany poziom zaufania dla danego certyfikatu;
14. unikalny identyfikator jednego lub więcej rejestrów wyznaczonych do publikacji zawiadomień o unieważnieniach lub zawieszeniu, albo sprecyzowanie sposobu w jaki zawiadomienie o unieważnieniach lub zawieszeniu ma być podawane, stosownie do punktów 306 (3) oraz 307 (5) Aktu Stanu Utah;
15. wskazanie miejsca pierwotnego wykazu przepisów wykonawczych, jeżeli te odwołują się do certyfikatu, metodę lub procedurę według której ma on być uzyskany, jego format, strukturę, autora oraz datę, zgodnie z punktem 302.

Zawartość opcjonalna

Certyfikat wydany przez uprawniony Organ Certyfikujący może, zależnie od podpisującego oraz samego Organu Certyfikującego, umieścić lub zawrzeć w odnośnikach dowolną lub wszytkie z poniższych informacji:

1. jeden lub więcej dodatkowych, drugorzędnych kluczy publicznych;
2. identyfikatory lub wska¼niki użytkowania odpowiednie dla danego klucza publicznego;
3. odnośniki do odpowiednich wykazów przepisów wykonawczych procesu ceryfikacji; oraz
4. dowolną inną dostępną dokumentację dotyczącą certyfikatu, Organu Certyfikującego, który go opublikował lub też podpisującego, który go akceptował;

Format

Informacje zawarte w certyfikacie są prezentowane w formacie ogólnie przyjętym dla transakcji, dla których podpisujący pragnie go użyć. Ponadto, o ile nie obowiązuje inny ogólnie przyjęty format, dla takich transakcji:

1. certyfikat przedstawiony jest w formacie zgodnym ze standartem X.509 Międzynarodowego Związku Telekomunikacji;
2. informacje zawarte w poniższych polach mają być podane w sposób następujący: *"Zarezerwowane dla przyszłej specyfikacji ASN. 1"*

202. Format wykazu przepisów wykonawczych procesu certyfikacji

Zawartość certyfikatu lub aktów jawnych Organu Ceryfikującego

Jeślli certyfikat wskazuje lub zawiera odnośniki do wykazu przepisów wykonawczych, lub jeżeli akta jawne Organu Certyfikującego odwołują się do pierwotnego wykazu przepisów

wykonawczych, to akta jawne certyfikatu lub Organu Ceryfikującego dostarczają następujących informacji w formacie opianym w punktach 202 (2), 301 oraz 302 (3):

1. miejsce przechowywania wykazu przepisów wykonawczych, w formacie URL lub w innym formacie ogólnie przyjętym dla transakcji, dla których podpisujący pragnie certyfikat stosować;
2. metodę lub procedurę, według której wykaz przepisów wykonawczych może być odnaleziony;
3. format i strukturę wykazu przepisów wykonawczych, który powinien być przedstawiany w formacie zalecanym przez podrozdział (2) niniejszych zasad, albo jako tekst w formacie HTML wersja 2.0, lub też w formacie ogólnie przyjętym dla transakcji, dla których podpisujący pragnie certyfikat stosować;
4. autora wykazu przepisów wykonawczych, zarówno w formacie zalecanym w podrozdziale (2) niniejszych przepisów, jak i w ogólnie przyjętym formacie, umożliwiającym wykonywanie standardowych operacji, zgodnie z oczekiwaniami podpisującego;
5. jego datę w formacie zalecanym w ustępie (2) niniejszych przepisów lub w formacie ogólnie przyjętym dla transakcji, dla których podpisujący pragnie certyfikat stosować;

Format wykazu przepisów wykonawczych

O ile certyfkat lub Akta Jawne Organu Ceryfikującego jawnie nie stanowią inaczej, ani nie obowiązuje żaden inny format ogólnie przyjęty dla transakcji, dla których podpisujący pragnie certyfikat stosować, to wykaz przepisów wykonawczych dotyczących certyfikacji jest dokumentem w formacie SGML (Standard Generalized Markup Language), standart ISO 8879 (1986, w wersji aktualnej 1988), definicja typu dokumentu zawarta jest dalej w Załączniku A.

203. Przechowywanie zapisów przez Organ Certyfikujący

Wymagania

Licencjonowany Organ Certyfikujący przechowuje szczegółowe zapisy dokumentujące zgodność z Aktem Stanu Utah. Akta te stanowią dowód, że Organ Certyfikujący:

1. sprawdził tożsamość osoby wymienionej w certyfikacje, wydanym przez dany Organ Certyfikujący;
2. sprawdził tożsamość osoby wnoszącej o unieważnienie każdego certyfikatu
3. sprawdził i zatwierdził wszystkie inne fakty wyszczególnione jako zatwierdzane w certyfikacie, wydanym przez Organ Certyfikujący, oraz
4. zastosował się do treści niniejszego rozdziału przy wydawaniu, zawieszaniu oraz unieważnianiu certyfikatu.

Za wyjątkiem żądań zawieszenia certyfikatu, licencjonowany Organ Certyfikujący może zażądać od podpisującego lub jego pełnomocnika przedstawienia dokumentacji lub innych oświadczeń, celem zapewnienia zgodności z niniejszym ustępem.

Przechowywanie i opieka

Uprawniony Organ Certyfikujący przechowuje akta dotyczące wydawania, zatwierdzania, zawieszania jak i unieważniania certyfikatów przez okres nie krótszy niż dziesięć lat, licząc od daty unieważnienia lub wygaśnięcia ważności certyfikatu.
Licnencjonowany Organ Certyfikujący samodzielnie chroni powyższe akta, chyba że podpisał on umowę z innym organem o sprawowanie opieki nad powyższymi aktami (zgodnie z założeniami niniejszego dokumentu) lub też przekazuje te akta Wydziałowi Urzędu w związku z zakończeniem działalności jako Organ Certyfikujący.

Bezpieczeństwo przechowywania akt

Uprawniony Organ Certyfikujący przechowuje akta w odpowiednich warunkach niezawodności i bezpieczeństwa mających komercyjne uzasadnienie w odniesieniu do limitów zaufania certyfikatów.

204. Zakończenie działalności Organu Certyfikującego

Uwagi dla podpisującego oraz unieważnienie jednostronne

Przed zakończeniem działalności Organu Certyfikującego jest on zobligowany:

1. na co najmniej 90 dni przed planowaną datą zakończenia działalności dostarczyć wszystim podpisującym pisemne zawiadomenie o planowanym zakończeniu działalności; dotyczy to tylko tych podpisujących, których cerfikaty które nie zostały zawieszone ani unieważnione;
2. co najmiej 90 dni po zawiadomieniem z punktu (1)(a) tego ustępu, unieważnić pozotałe certyfikaty, których ważność dotychczas nie wygasła ani nie zostały unieważnione, bez względu na to czy podpisujący wnosił o unieważnienie, czy nie;
3. dostarczyć wszystim podpisującym certyfikat pisemne zawiadomienie o jego unieważnieniu, stosownie do punktu (1)(b) niniejszego ustępu; oraz
4. o ile zawarty pomiędzy podpisującym a Organem Certyfikującym umowa nie stanowi inaczej, zapłacić podpisującemu odpowiednie odszkodowanie za unieważnienie certyfikatu przed data wygaśnięcia jego ważności;

Reedycja pozostałych certyfikatów przez kolejny Organ Certyfikujący

Aby zapewnić ciągłość działalności Organu Certyfikującego w zakresie certyfikacji, Organ Certyfikujący kończący swą działalność może zlecić innemu Organowi Certyfikującemu przejęcie jego dotychczasowych obowiązków w zakresie pozostałych certyfikatów na dotychczasowych zasadach; nie dotyczy to, opisanego poniżej, wykazu przepisów wykonawczych dotyczących certyfikacji, chyba że podpisujący zgodzi się na wprowadzenie zmian.
Nowy Organ Certyfikujący powinien stowrzyć swoj własny podpis cyfrowy dla reemitowanych przez niego certyfikatów. W reemitowanych certyfikatach stosownie do niniejszego ustępu:

1. nowy Organ Certyfikujący nabywa prawa i obowiązki dotychczasowego Organu Certyfikującego; oraz
2. o ile zawarty pomiędzy podpisującym a Organem Certyfikującym umowa nie stanowi inaczej, wszystkie wykazy przepisów wykonawczych dotychczasowego Organu Certyfikującego przechodzą we władanienie nowego Organu Certyfikującego i stają się obowiązujące, chyba że nowy Organ Certyfikujący, na co najmniej 60 dni przed wprowadzeniem w życie wyda oświadczenie o planowanych zmianach w odpowiednim wykazie przepisów wykonawczych.

Dalsze postanowienia dotyczące umowy

Postanowienia tego paragramu mogą być zmienione w umowie. Poza tym umowa nie może zezwalać Organowi Certyfikującemu na zaprzestanie działalności bez uprzedniego dostarczenia wszystkim podpisującym pisemnego oświadczenia w tej spawie, doręczonego na co najmniej dziesięć dni przed datą zaprzestania działalności (dotyczy certyfikatów nie wygasłych ani tych, które nie zostały wcześniej unieważnione); lub
bez uprzedniego unieważnienia wszystkich zaległych certyfikatów

Przechowywanie dokumentów przez Wydział Urzędu

Przed zaprzestaniem działalności Organ Certyfikujący musi powiadomić o swoich zamiarach Wydział Urzędu. Zawiadomienie powinno być złożone w aktach Wydziału Urzędu najpó¼niej na dwa miesiące przed i nie wcześniej niż sześć miesięcy przed datą zaprzestania działalności jako Organu Certyfikującego. Ponadto oświadczenie to powinno mieć poniższą formę:

Oświadczenie o zamierzanym zakończeniu działalności jako Oganu Certyfikującego
Nazwa Organu Certyfikującego: _____
Unikalna nazwa kończącego działalność Organu Certyfikującego:
_____
Liczba wydanych i ważnych aktualnie certyfikatów: _____
Data przewidywanego zakończenia działalności Organu Certyfikującego: _____
Data dostatrczenia oświadczenia dla podpisujących certyfikaty (dotyczy certyfikatów ważnych):
_____ (dostarczenie kopii oświadczenia dla podpisującego)
Czy kończący działalność Organ Certyfikujący przekaże działalość innemu Organowi Certyfikującemu (tak/nie)?
:_____
Nazwa przejmującego działalność Organu Certyfikującego, jeśli taki istnieje:
_____
Unikalna nazwa przejmującego działalność Organu Certyfikującego, jeśli taki istnieje:
_____

Zgon osoby posiadającej licencję Organu Certyfikującego lub niezdolność do działania Organu Certyfikującego

W wypadku śmierci osoby posiadającej licencję, zarządzanie jej mieniem odbywa się zgodnie z postanowieniami niniejszego ustępu lub odpowiedniej umowy regulującej zakończenie działalności Organu Certyfikującego. Jeżeli Organ Certyfikujący ogłasza niezdolność do działania w znaczeniu ustępu 75-1-201(18) kodeku UCA (Utah Code Annotated), sąd może wyznaczyć opiekuna zgodnie z UPC (Uniform Probate Code) Stanu Utah (artykuł 5, część 3),

lub też w oparciu o petycję zainteresowanych stron może wyznaczyć zarządcę masy upadłościowej, celem zakończenia działalności Organu Certyfikującego, zgodnie z wymaganiami niniejszego ustępu.

REJESTRY

Uznanie prawne rejestrów

Aby rejestr został prawnie uznany, zgodnie z paragrafem §501 Aktu Stanu Utah, osoba sparawująca naczelną kontrolę prawną nad rejestrem musi ewidencjonować wraz z Wydziałem Urzędu informacje, które:

1. zawierają pełne nazwisko, adres, numer telefonu, adress poczty elektronicznej (e-mail) oraz unikalna nazwa osoby wypełniającej tę aplikację;
2. zawierają pełne nazwisko, adres, numer telefonu, adress poczty elektronicznej (e-mail) oraz unikalna nazwa Organu Certyfikującego, dla którego dany rejestr jest wykorzystywany;
3. dokładnie opisują, przedstawiając zarazem zgodność z odpowiednimi stanartami technicznymi:
    1. projekt i implementację wiarygodnego systemu rejestrów
    2. zawartość rejestrów;
    3. różnego rodzaju wymagania odpowiednie do zawartości rejestrów;
    4. kryteria wyznaczające, kto może publikować informacje w rejestrze oraz środki prawne na których takie kryteria się opierają;
    5. procedurę obiegu nowo publikowanych certyfikatów oraz oświadczeń o ich zawieszeniu lub unieważnieniu;
    6. sposób naliczania opłat za użytkowanie oraz dostęp do informacji w nim zawartych; oraz
    7. wysokości opłat za korzystanie z akt jawnych Organu Certyfikującego oraz przepisów i raportów doradczych, publikowanych przez Wydział Urzędu, o ile dokumenty takie zostały prawnie zatwierdzone;
4. zawierają zatwierdzone prawnie zobowiązania i obietnice, celem łatwiejszego sporządzania odpisów:
    1. wszekich akt jawnych Organu Certyfikującego wydawanych w rejestrze przez Wydział Urzędu;
    2. wszelkich poprawek oraz unieważnień w obowiązujących aktach jawnych Organu Certyfikującego wydawanych w rejestrze przez Wydział Urzędu;
    3. wszelkich przepisów oraz raportów doradczych publikowanych w rejestrze przez Wydział Urzędu;
5. zawierają kopie odpowiednich przepisów wykonawczych procesu certyfikacji pozyskiwanych z rejestru bieżącego lub jego archiwów;

Należy jedocześnie podkreślić, że treść tego ustępu nie przymusza do ujawniania jakichkolwiek tajemnic handlowych, ani informacji, których ujawnienie mogłyby naruszyć bezpieczeństwo wiarygodnego systemu.

Przesłuchanie

Aby poddawać rewizji podania o uznanie prawne Wydział Urzędu zobowiązany jest postępować według formalych procedur sądowych, zgodnie z Ustawą o Postępowaniu Administracyjnym Stanu Utah, tytuł 63, rozdział 46b; wyjątki stanowią sytuacje, gdy:

1. podanie dotyczy przedłużenia ważności;
2. podanie zostało złożone w ciągu trzech miesięcy od daty przewidywanego wygaśnięcia ważności, oraz
3. gdy Wydział Urzędu, w świetle dotychczasowych akt rejestru dotyczących usług i działalności, uzna, iż rozprawa sądowa nie jest konieczna.

Delegowanie przywilejów

Wydział Urzędu deleguje w ten sposób do każdego uznanego rejestru wszelkie swoje przywileje w zakresie prawa powszechnego w odniesieniu do publikacji akt jawnych Organu Certyfikującego oraz raportów doradczych Wydziału Urzędu.

Załącznik 4.

Przegląd wybranych regulacj prawnych i rozwiązań organizacyjnych związanych z dematerializacją faktury.

Włochy

We Włoszech najwcześniej zaakceptowano fakturę w postaci elektronicznej. Dekret Ministerstwa Finansów z 30.11.1990 r. uznaje legalność procedury fakturowania za pomocą teletransmisji zgodnie z wnioskiem przedstawionym przez Stowarzyszenie Włoskich Spółek Akcyjnych - ASSONIME. Wniosek ten formułował propozycje następujących punktów procedury teletransmisji faktury:

Wystawianie faktur

Wystawienie faktury następuje w tym momencie, gdy podmiot przekazujący towar lub świadczący usługę przekazuje dane tego dokumentu odbiorcy. Wydruk faktury powinien nastąpić w terminie 15 dni od daty wystawienia/przekazania danych rachunkowości.

Przekazanie (transmisja) faktury

Podmiot wystawiający fakturę przekazuje zawarte w niej dane klientowi albo bezpośrednio lub za pośrednictwem podmiotu trzeciego.

Odebranie faktury

Fakturę należy uważać za odebraną w momencie „wyjęcia" przez adresata odnośnych danych z elektronicznej skrytki pocztowej, z jednoczesnym przypisaniem im obowiązkowej numeracji, utworzonej z ciągu rosnących liczb porządkowych.

Rejestrowanie faktury

Rejestrowanie faktury dzieli się na dwa oddzielne etapy:

- Gromadzenie odnośnych danych w elektronicznej pamięci, w wyznaczonych terminach.

- Wydruk na oddzielnych arkuszach, tworzących rejestr wystawionych i otrzymanych faktur, dokonywany w ciągu 60 dni od daty, w której dokumenty te uzyskały przydatność do celów tu rozważanej rejestracji.

Należy wspomnieć, że we Włoszech już wcześniej Ministerstwo Finansów uregulowało zasady prowadzenia księgowości elektronicznie, a w roku 1984 rozpoczęło wprowadzanie obowiązku stosowania kas fiskalnych - elektronicznych liczników podatku VAT, naliczanego przy transakcjach. Prawo fiskalne było więc już przygotowane i zweryfikowane do posługiwania się elektronicznymi nośnikami dokumentów.

Francja

W 1991 zalegalizowano fakturę elektroniczną we Francji. Instrukcja D.G.I. (Direction Général des Impôts) określała procedurę autoryzacji systemów EDI w których mogły być realizowane transakcje handlowe.

Używany system powinien zapewniać następującą specyfikę realizowanych funkcji:

1 - Identyczność komunikatów emitowanych i odebranych zawierających obligatoryjnie następujące informacje:

Nazwisko (lub firma) i adres sprzedawcy i klienta, datę fakturowania, oznaczenie, ilość dóbr lub usług, cenę jednostkową i kwotę pozycji, sumę ogólną i obligatoryjne dane do kopii streszczenia.

2 - Emisja i archiwowanie (6 lat) kopii streszczenia na nośniku papierowym.

Emitowanie podczas każdej teletransmisji (emisja lub odbiór) lub conajmniej raz dziennie listy kopii streszczeń, bezpośrednio tworzonych przez system teletransmisji, powinien zawierać conajmniej następujące pozycje:

1° informacje identyfikacyjne faktury:

Datę i numer faktury, datę i godzinę emisji lub przyjęcia faktury, numer przyjęcia, kwotę pozycji i sumę całkowitą (warunki płatności, kod waluty), identyfikator nadawcy i odbiorcy danych w systemie.

2° informacje identyfikujące systemy teletransmisji:

Data edycji i wersja zastosowanego programu.

3 - Archiwowanie danych w ich postaci orginalnej i w porządku chronologicznym ich emisji i odbioru.

Sprecyzowano, że obowiązek zachowania integralności komunikatu faktury emitowanej lub otrzymanej w czasie określonym przez prawo fiskalne (3 lata przez system informatyczny i 3 lata wg wyboru medium przez przedsiębiorstwa).

4 - Odtworzenie faktury wyemitowanej lub odebranej w języku jawnym.

Przedsiębiorstwa powinny być szczególnie uczulone na ten obowiązek, gdyż na żądanie administracji, faktura powinna być odtworzona na papierze.

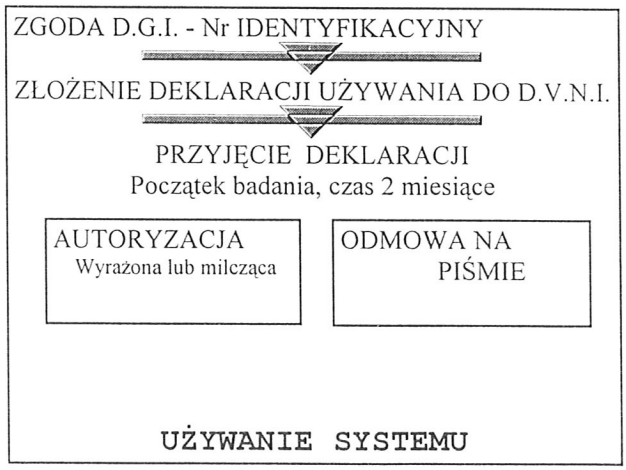
Prawo francuskie przewiduje 3 typy autoryzacji systemów EDI przez administrację fiskalną D.V.N.I (Direction de Vérification Nationales et Internationales)

PROCEDURY DGI

1 - Autoryzacja inicjalna

2 - Zgłoszenie modyfikacji

3-Deklaracja używania



Prawo francuskie przewiduje sankcje za używanie systemu niezgodnego z autoryzacją. Autoryzacja używania systemu jest cofnięta, gdy inspektorzy administracji stwierdzą mankamenty nie usuwalne w przeciągu trzech miesięcy.

Konsekwencje finansowe są poważne dla wszystkich partnerów handlowych:

- Klient (przedsiębiorstwo odbierające) nie ma więcej prawa odliczać podatku VAT fakturowanego pod EDI przez swojego dostawcę (za wyjątkiem gdy będzie to na papierze);

- Dostawca (przedsiębiorstwo nadające) traci swoje korzyści konkurencyjne wraz z obowiązkowym powrotem do fakturowania papierowego ze swoim partnerem.

Walidacja faktury elektronicznej ma dwa zasadnice ograniczenia:

* Pierwsze dotyczy charakteru wielo-funkcyjnego faktury

Prawo handlowe przewiduje przechowywanie dokumentu przez 10 lat, podczas gdy fiskalne tylko 6. Z tego względu należy podkreślić zainteresowanie zgodą na EDI, które dostarcza środków do zarządzania dowodami w prawie handlowym, ale w ramach sieci zamkniętych.

* Drugie wynika ze sfery aplikacji prawa francuskiego

System prawny faktury powyżej wyłożony, stosuje się wyłącznie w stosunkach pomiędzy administracją i przedsiębiorstwami podlegającymi jurysdykcji francuskiej. Stanowi to prawdziwy kłopot przy używaniu faktury w relacjach międzynarodowych.

Belgia

Dekretem Królewskim z dn. 7 Grudnia 1994 została dopuszczona w Belgii faktura elektroniczna. Dekret formułuje warunki dopuszczenia następująco:

Art. 1

Wydanie faktury lub dokumentu w postaci odtworzenia, może zostać dokonane przez transmisję danych, które ten dokument winien zawierać, za pomocą systemu wykorzytującego techniki teleinformatyczne.

Art. 2

§1. Każdy podatnik chcący dostarczać/otrzymywać dokumenty elektroniczne powinien poinformować drogą pocztową kontrolera w biurze kontroli podając, nazwisko/nazwę firmy adres i NIP.

§2. Po miesiącu przy braku odpowiedzi, podatnik może korzystać z EDI.

Art. 3

Podatnik musi posiadać i przechowywać pełną dokumentację dotyczącą używanego systemu. System nie może być modyfikowany bez naniesienia zmian w dokumentacji.

Art. 4

§1 Nadane i odebrane komunikaty muszą być identyczne. Na żądanie administracji muszą zostać odtworzone na papierze.

§2 Komunikaty muszą być skopiowane i przechowywane bez zmian w porządku chronologicznym.

Art. 5

Każdy komunikat musi zawierać numer sekwencji emisji lub numer sekwencji odbioru.

Art. 6

§1 Raz w miesiącu podatnik powinien przesyłać listę komunikatów z podziałem na kontrahentów i ewenetualne anomalie.

§2 Podsumowujące listy z poprzedniego paragrafu powinny być przechowywane przez okres przewidziany w Kodeksie.

§3 Lista zbiorcza niezależnie od daty nadania obejmuje:

- identyfikacja nadawcy i odbiorcy;

- datę i nr faktury nadawcy;

- datę emisji lub odbioru faktury;

- nr sekwencji emisji lub odbioru;

- sumę podstawy opodatkowania i należnego VATu.

Art. 7

Każdy podatnik korzystający z EDI podaje w deklaracji określonej w Kodeksie ilość komunikatów nadanych i otrzymanych w ciągu okresu podanego w deklaracji w rozbiciu na kontrahentów identyfikowanych NIPem.

* Otrzymywanie przez teletransmisję faktur zagranicznych jest zabronione przez prawo.

Licencja na faktury ICOM i EANCOM

ICODIF (Belgijska Organizacja Narodowa EAN) wprowadził wymóg otrzymywania licencji na fakturę elektroniczną na kanwie ICOM i EANCOM. Po uzyskaniu tej licencji przedsiębiorstwa moą wysyłać w jednym z tych dwu standardów faktury w sposób elektroniczny i dokumenty papierowe nie muszą być archiwowane dla administracji TVA.

Holandia

Ministerstwo Finansów Holandii 23. Grudnia 1992 r wprowadziło dopuszczenie faktur elektronicznych w okresie próbnym, co ma pozwolić na praktyczną weryfikację przyjętych zasad i opracowania właściwego aktu prawnego.

1. Warunki próby „elektronicznego fakturowania"

Okres próbny = dwa lata 1993/1994. Warunki zezwolenia będą w tym czasie regulowane.

2. Procedura uczestnictwa w próbie

Strona nadająca i odbierająca muszą wnioskować o zezwolenie w Jednostce Podatkowe, której podlegają. Przed udzieleniem zezwolenia Jedostka Podatkowa zarządza próbę systemu przez biegłego EDP. W zezwoleniu są określone warunki pracy.

3. Warunki stosowania „elektronicznego fakturowania"

Dla decyzji podejmowanych niefiskalnie musi być spełniona pewna ilość warunków formalnych i kontrolno-technicznych. Warunki są tak dostosowane, aby odtworzenie faktury elektronicznej na papierze nie utrudniało kontroli organom podatkowym.

4. Prawo ogólne dotyczące podatków

Administracja powinna być tak urządzona i prowadzona, aby nośniki informacji były przechowywane w określonym terminie do kontroli przez inspektora.

5. Ustawa o podatku obrotowym 1968

W art. 35 określa wymagania jakie musi spełniać faktura.

W ramach dopuszczalnych zezwoleń przyznawane jest warunkowo „elektroniczne fakturowanie"., na warunkach:

- komplet danych musi być identyczny,

- reguły w odniesieniu do zadłużenia i prawa do wyprzedzenia stosowane w ten sam sposób,

- moment wręczenia faktury jest określany datą faktury.

6. Aspekty kontrolno-techniczne

Strony muszą okresowo wymieniać sprawozdania z wysłanych/odebranych faktur. Sprawozdanie musi zawierać:

- datę faktury,

- nr faktury,

- kwotę faktury i stawkę podatkową,

- ogólną ilość faktur na sesję i na sprawozdanie.

7. Ogólne

Wniosek o zezwolenie powinien mieć dołączony projekt systemu elektronicznego fakturowania.

Testowanie systemu może trwać do 6 miesięcy.

Pozwolenia udziela się na ograniczony okres.