Paweł Zając
Zakład Logistyki i Systemów Transportowych Politechniki Wrocławskiej

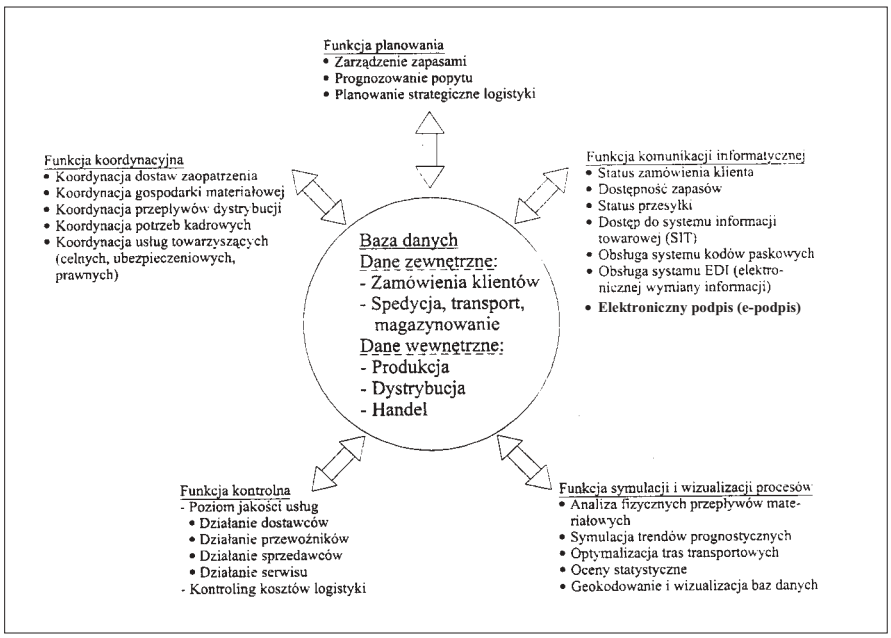
Tworzenie podpisu elektronicznego i jego rola w e-logistyce

Do 11 października 2001 r. e-logistyka stosowana w operacyjnych działaniach polskich przedsiębiorstw zawierała znaną powszechnie technologię elektronicznej wymiany dokumentów EDI (*Electronic Data Interchange*), ale bez stosowania możliwości elektronicznego podpisu. Od tej daty rozpoczęła się nowa rzeczywistość polskiej e-logistyki. **Obecnie dokument papierowy może być całkowicie zastępowany przez dokument elektroniczny**. Jednak by był on równoważny dokumentowi papierowemu musi spełniać odpowiednie wymagania stawiane przez ustawodawcę i w dalszej kolejności przez Parlament Europejski. Przytacza się tu dwie podstawowe cechy dokumentu i podpisu elektronicznego: **poufność i wiarygodność**. Możliwości stosowania technologii podpisu elektronicznego są bardzo szerokie i odnoszą się nie tylko, jak to powszechnie się uważa, do transakcji zawieranych przez Internet (chodzi tu o transakcje klient – przedsiębiorstwo – B2C oraz przedsiębiorstwo – przedsiębiorstwo – B2B), ale również szeroko pojętej problematyki komputerowo wspomaganej logistyki CAL *(Computer Aided Logistics)* rys. 1. Systemy tego typu spełniają następujące szczegółowe funkcje w e-logistyce: planowania i harmonogramowania, koordynacji taktyczno – operacyjnej, kontroli, ewidencji, rozliczeń (z bankiem, urzędem skarbowym, ZUS – em), komunikacji informatycznej (EDI, SAI), symulacji i wizualizacji procesów (pakiety synoptyczne).

Poniżej opisano dwa przypadki w operacyjnych działaniach przedsiębiorstwa, które mają na celu przybliżenie istoty podpisu elektronicznego.

Przykład 1 – ZAKUP W SKLEPIE INTERNETOWYM

Tego rodzaju transakcja (dokonywana przez Internet) zwykle zawiera następujące elementarne czynności: wyszukanie e-sklepu, zamówienie, płatność, dostawa, obsługa posprzedażna. Tak więc trzy czynności można operacyjnie wykonać drogą elektroniczną – wyszukać e-firmę, złożyć elektroniczne zamówienie podpisane e-podpisem i zapłacić kartą elektroniczną lub przelewem bankowym.



Rys. 1. Funkcje informatycznych systemów wspomagania logistyki CAL

Przykład 2 – OCHRONA OSOBOWA DANYCH INFORMACYJNYCH

Większość komputerowych systemów wspomagania zarządzania klasy ERP pozwala użytkownikom na prowadzenie daleko idących symulacji biznesowych, wymiany informacji z klientami itp. Wymaga to prowadzenia i administrowania dużą ilością danych (niejednokrotnie bardzo ważnych informacji marketingowych, fizycznych i osobowych). Występuje tu konieczność zapewnienia odpowiedniej ochrony przed dostępem do nich niepowołanych osób. Dotychczas stosowano dwie dość skomplikowane metody: szyfrowania poczty e-mail oraz odpowiedniego upakowania danych i ich kodowania. Obsługa takich przesyłek wiąże się z posługiwaniem się stosownymi kluczami do kodowania. Zmiana klucza (zagubienie, kradzież) wymagała rozesłania zainteresowanym nowych wersji kluczy, które już w czasie przesyłki mogły trafić w niepowołane ręce.

Zastosowanie w obu tych przypadkach technologii elektronicznej korespondencji i e-podpisu umożliwia ich sprawne i bezpieczne przeprowadzenie w ramach komputerowo zintegrowanego systemu, który wspomaga zarządzanie firmą.

Podpis elektroniczny (e-podpis) – podstawowa terminologia

Podpis na dokumencie składa się w końcowej jego części stwierdzając fakt, iż podpisujący zapoznał się z jego treścią i ją akceptuje. Jednak podstawową funkcją podpisu są: **identyfikacja wystawcy dokumentu oraz połączenie danej osoby z treścią dokumentu**. Podobne zadanie ma podpis elektroniczny, choć gdy o nim się mówi, często używa się nieco mniej znanej popularnie terminologii, przez co sprawa podpisu elektronicznego wydaje się być niejasna i skomplikowana. Stąd poniżej zamieszczono definicje podstawowych terminów.

Podpis elektroniczny stanowią dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone, lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej taki podpis. Przyjęte rozwiązania opierają się na systemie domniemań prawnych. W odniesieniu do bezpiecznych podpisów elektronicznych za-

pisano dwa domniemania: dotyczące osoby określonej w certyfikacie jako składającej podpis elektroniczny oraz domniemanie prawdziwości znakowania czasem. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu Cywilnego. Domniemanie to oznacza, że podpis elektroniczny znakowany czasem (tzn. godziną oraz datą) przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi.

Certyfikat to potwierdzenie klucza publicznego wygenerowanego przez daną osobę lub instytucję przez instytucję autoryzacyjną, która autoryzuje dany klucz publiczny. Klucz publiczny instytucji jest autoryzowany przez nią samą lub instytucję działającą w innym kraju, ponadto jest udostępniony do użytku publicznego. Istnieje kilka typów (poziomów) certyfikacji. Niektóre powinny być używane tylko w prostych zastosowaniach. Wówczas weryfikacja tożsamości podczas ich wydawania odbywa się w sposób uproszczony. Są też takie, w których proces ten jest bardzo drobiazgowy. Wówczas – gdyby korzystający z podpisanych elektronicznie dokumentów poniósł straty na skutek niedbałości centrum autoryzacyjnego – urząd gwarantuje ich wyrównanie do pewnej określonej kwoty.

Centrum certyfikacji, na świecie znane jako **PKI** (*Public Key Infrastructure*) – to infrastruktura niezbędna do świadczenia usług związanych z zarządzaniem certyfikatami kluczy publicznych. Jest to jakby trzecia strona w procesie działania podpisu cyfrowego – organizacja odpowiedzialna zajmująca się wydawaniem odpowiednich certyfikatów na klucze publiczne firm i obywateli danego kraju. Przechowuje wszystkie wydane certyfikaty (w repozytoriach) oraz certyfikaty i listy unieważnionych kluczy. Polskie Urzędy Certyfikacyjne: www.centrum.pl; www.polcert.pl; www.signet.pl.

Klucz zwany też frazą (różni się od popularnego hasła tym, że powinien być dłuższy) może się składać z całego zdania, na przykład dobrą frazą jest cytat z jakiegoś dzieła literackiego. Ponieważ w zdaniu znajdują się wielkie litery, odstępy między wyrazami i znaki interpunkcyjne, taka fraza daje stosunkowo dobre zabezpieczenie. Bardzo długa fraza jest niepraktyczna jeżeli często jej używamy (również należy się liczyć z naszymi możliwościami zapamiętania jej). Zbyt długi klucz powoduje zwolnienie procesów przetwarzania dokumentów. Rozsądną długością klucza jest długość ok. 2048 bitów.

Klucz publiczny (*Public Key*) i **klucz prywatny** (*Priwate Key*) to para z tym, że klucz prywatny przechowuje i używa właściciel danego podpisu elektronicznego, a drugi – publiczny przechowuje centrum certyfikacyjne. Klucz prywatny i publiczny są generowane w jednym czasie i niepowtarzalne w swoim rodzaju. W przypadku zmiany jednego z nich lub wygaśnięcia ważności generuje się nową parę kluczy. Dokumenty popisane kluczem który zaginął (lub jest nieważny) są ważne do daty zaginięcia klucza (lub upłynięcia daty ważności). Program komputerowy używany do tworzenia kluczy gwarantuje ich unikalność. Klucz, każdy może wykonać we własnym zakresie lub skorzystać z odpowiedniej firmy, która świadczy w tym zakresie usługi.

Kryptografia to szyfrowanie zarówno wiadomości jak zbiorów elektronicznych, gdzie używa się do kodowania jak również odszyfrowywania odpowiednich algorytmów. W technologii podpisu elektronicznego używa się systemu szyfrowania niesymetrycznego (od 1970, choć literatura podaje, że rok 1967 był końcem ery tzw. „szyfrowania symetrycznego" w elektronicznej technologii popisywania dokumentów). Celem kryptografii jest poprzez tzw. „klucze" ochrona danych przesyłanych pomiędzy stronami przez Internet.

PIN to ciąg znaków zabezpieczający dostęp do klucza prywatnego. Jest odpowiednikiem kodu PIN znanego z kart bankowych czy dostępu do odpowiednich funkcji w telefonie komórkowym.

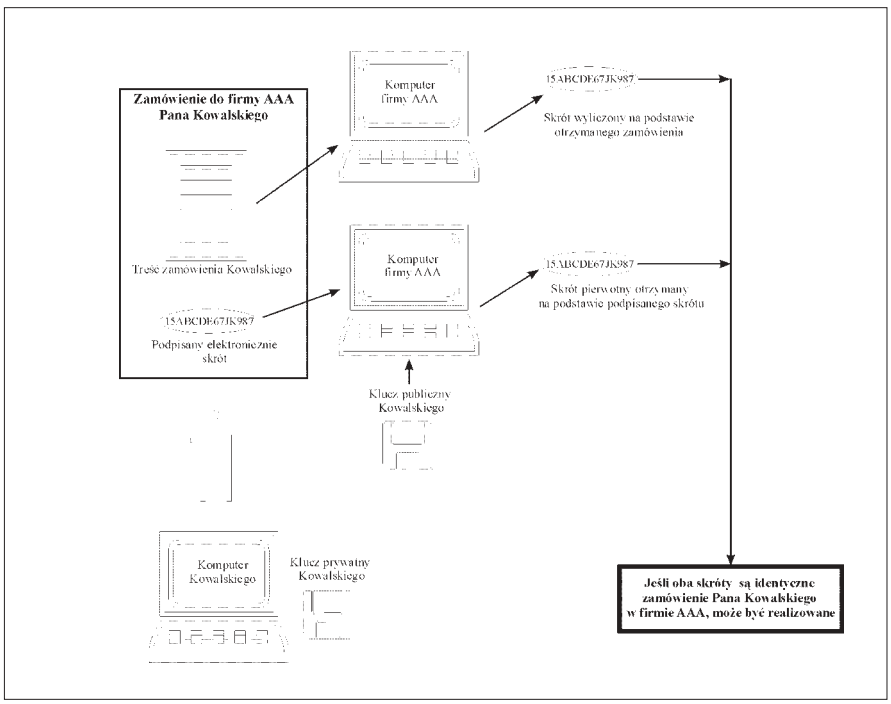
Skrót, nazywany też odciskiem palca, to ciąg kilkunastu znaków wygenerowanych na podstawie dłuższego ciągu, na przykład klucza publicznego. Pozwala łatwo wykryć zmiany fragmentu tekstu bądź podmianę jednego napisu na inny. Względnie trudno jest utworzyć inny klucz publiczny lub napis, który dawałby ten sam skrót. Mając sam skrót, nie można też poznać napisu, na podstawie którego został wygenerowany. Natomiast bardzo szybko odbywa się weryfikacja, czy klucz publiczny bądź inny napis i skrót pasują do siebie.

Istota tworzenia i posługiwania się podpisem elektronicznym

Rozróżnia się dwa podstawowe działania w zakresie tworzenia podpisu elektronicznego. Są to:

1. **Tworzenie podpisu elektronicznego bez udziału centrum certyfikacji**.

- Strona wysyłająca dokument (np. Kowalski) podpisuje go elektronicznie i wysyła przez Internet do kontrahenta (np. firmy AAA). Kowalski generuje więc na swoim komputerze dwa klucze: pry-



Rys. 1. Funkcje informatycznych systemów wspomagania logistyki CAL

watny i publiczny. Pierwszy służy do składania cyfrowego podpisu i nie należy go nikomu udostępniać. Publiczny pozwala zweryfikować sygnowany elektronicznie dokument. Powinien więc zostać dostarczony każdej osobie, która będzie korzystała z takich dokumentów. Kowalski zapisuje klucz prywatny w pamięci karty mikroprocesorowej (chipie) lub na dyskietce. Dodatkowym zabezpieczeniem klucza prywatnego jest PIN, niezbędny do tego by korzystać z usług podpisu elektronicznego.

- Kowalski idzie do swojego partnera biznesowego firmy AAA z kluczem publicznym. Pracownicy firmy AAA sprawdzają tożsamość klienta na przykład na podstawie dowodu osobistego lub innego dokumentu tożsamości. Podpisywana jest odpowiednia umowa upoważniająca firmę AAA do honorowania korespondencji od Kowalskiego, których autentyczność można potwierdzić za pomocą dostarczonego klucza publicznego. W umowie powinien zostać wydrukowany albo cały ten klucz jako ciąg liter i cyfr, albo jego skrót. Inaczej Kowalski mógłby później próbować zakwestionować treść przesłanego dokumentu, twierdząc, że dostarczył zupełnie inny klucz publiczny.
- W opisywanej sytuacji Kowalski osobiście musi podpisać umowę. Jeśli przesłał by swój klucz publiczny przez Internet, pracownicy firmy AAA nie mieliby żadnej pewności, że pochodzi on od osoby, za którą partner w biznesie się podaje.
- Kowalski po powrocie do swojej firmy pisze na swoim komputerze, na przykład zamówienie na pewne usługi w firmie AAA. Do dokumentu często automatycznie dodawana jest data i czas, wskazujące na moment podpisania w tym wypadku zamówienia. Następnie Kowalski wkłada kartę (dyskietkę) do czytnika komputera ze swoim kluczem prywatnym. Podaje kod PIN. W pierwszej sytuacji komputer wysyła dyspozycję do układu na karcie chip, który wykonuje obliczenia matematyczne na podstawie klucza prywatnego i treści zamówienia, tworząc dokument podpisany elektronicznie, gotowy do przesłania do firmy AAA. Jeśli Kowalski przechowuje klucz na dyskietce, wszystkich przekształceń dokonuje komputer.
- Zamówienie w jawnej postaci wraz z podpisanym skrótem wędruje przez Internet do firmy AAA, z którą Kowalski kooperuje. Na podstawie klucza publicznego Kowalskiego system komputerowy firmy AAA może zweryfikować, czy zamówienie zostało przesłane przez uprawnioną osobę. Dokładniej – komputery przekształcają podpisany elektronicznie skrót do wersji pierwotnej, niezaszyfrowanej. Następnie generują drugi skrót bezpośrednio z dostarczonego zamówienia. Jeśli oba są identyczne, zamówienie należy realizować. Gdyby były różne, wykryto by próbę oszustwa. Oznaczałoby to, że dokument został utworzony przez nieuprawnioną osobę lub zmodyfikowany już po wysłaniu go przez Kowalskiego.
- Firma AAA powinna przechowywać w pamięci komputerów nie tylko treść samego zamówienia, ale też podpisany przez Kowalskiego skrót. Tylko oba elementy tworzą łącznie dokument sygnowany elektronicznie i pozwalają dowieść firmie AAA Kowalskiemu, że złożył zamówienie, gdyby później wypierał się tego. Inaczej, w razie jakiejkolwiek reklamacji firma AAA ponosi winę. Ponieważ na podstawie klucza publicznego nie można wygenerować klucza prywatnego, nie ma ryzyka, że nieuczciwy pracownik firmy AAA zmieni zamówienie Kowalskiego. Poniższy tok złożenia zmówienia przez Kowalskiego w firmie AAA przedstawiono na rysunku 2.

2. Tworzenie podpisu elektronicznego z udziałem centrum certyfikacji.

- Podobnie jak wcześniej Kowalski generuje dwa klucze: prywatny i publiczny. Publiczny klucz dostarcza do centrum autoryzacyjnego. Następuje sprawdzenie tożsamości Kowalskiego. Do klucza dołączane są dane osobowe Kowalskiego. Całość urząd podpisuje swoim kluczem prywatnym. W ten sposób powstaje potwierdzony certyfikat Kowalskiego.
- Zakładamy, że firma AAA ufa instytucji, która potwierdziła klucz publiczny Kowalskiego. Kowalski nie musi, więc osobiście udawać się do firmy AAA aby podpisać umowę o wspólnym działaniu. Wystarczy, że wypełni odpowiedni formularz na stronie internetowej firmy AAA, podpisze go swoim kluczem prywatnym i prześle do firmy AAA wraz z certyfikatem poświadczonym przez zaufaną instytucję autoryzacyjną.
- Firma AAA zna klucz publiczny firmy autoryzującej klucz publiczny Kowalskiego. Łatwo więc sprawdzi, czy dostarczony przez Kowalskiego certyfikat rzeczywiście do niego należy. Skontroluje też, czy został podpisany elektronicznie przez centrum i czy zawarte w nim dane osobowe zgadzają się z informacjami podanymi przez Kowalskiego.
- Następnie firma AAA upewni się, czy zamówienie przesłane od Kowalskiego było sygnowane przez tę samą osobę, sprawdzając, czy podpisano go kluczem prywatnym, do którego pasuje klucz publiczny Kowalskiego. Schemat działania podpisu elektronicznego zamieszczony na rys. 2 dotyczy również powyższego przypadku (istotna różnica w/w metod dotyczy sposobu dostarczenia do firmy AAA klucza publicznego Kowalskiego i zawarcie umowy z firmą AAA).

Wprowadzanie podpisu elektronicznego w Polsce

Po podpisaniu ustawy o podpisie elek-

tronicznym przez Prezydenta Rzeczpospolitej Polskiej szczegółowe wdrożenia powinny być dokładnie analizowane, sprawdzane i koordynowane przez upoważnione w ustawie jednostki rządowe. W dzieło wdrażania podpisu elektronicznego angażuje się obecnie polska: gospodarka, instytucje prawa, instytucje zajmujące się standaryzacją i administracja.

Polska ma przed sobą wejście do Unii Europejskiej, w której sprawy podpisu elektronicznego reguluje dyrektywa o podpisach elektronicznych Parlamentu Europejskiego i Rady UE z 13.12.99 r. Powyższa dyrektywa mówi, że podpis elektroniczny powinien być oparty na zasadzie pary „kluczy", z których każdy byłby algorytmem kryptograficznym i służył do kodowania i dekodowania podpisu. Podpis elektroniczny w UE nie jest tak rozwinięty jak w USA, które uważa się za kolebkę popisu elektronicznego. Różnice w technologii kryptografii i działań związanych z udostępnianiem doświadczeń pomiędzy UE i USA stopniowo powinny się zmniejszać po wycofaniu przez USA przepisów o zakazie eksportu najnowszych technologii o podwójnym znaczeniu: cywilnym i wojskowym.

Polska w tej części świata jest największym rynkiem elektronicznego biznesu, zaraz po Czechach, wg wyników badań IDC (z 2001 roku). Do roku 2005 może się wysunąć na czoło. Jednak wymaga to pewnej strategii działania rządu polskiego. Należy zauważyć, że rząd polski nie posiada obecnie własnego portalu internetowego (poszczególne ministerstwa posiadają). Nie ma też programu zmodernizowania swoich usług, tak by były zwrócone ku obywatelowi. Podpis elektroniczny daje możliwości załatwienia wszystkich spraw, szybko i w jednym miejscu – tak jak zakupy w supermarkecie. Jest to jednak odległa przyszłość. Choć można sobie wyobrazić powszechne wybory do Sejmu, wybory samorządowe – w których głosowanie odbywa się poprzez Internet z wykorzystaniem podpisu elektronicznego.

System obiegu dokumentów i informacji w systemach ERP

Najnowszej generacji komputerowe systemy wspomagania zarządzania przedsiębiorstwami do tej pory nie mogły korzystać (ze zrozumiałych względów) z udogodnień jakie niesie z sobą używanie elektronicznego podpisu w komputerowo wspomaganym zarządzaniu firmą. Pozwalały zaprojektować przepływ dokumentów towarzyszący produkcji i dystrybucji towarów i usług, koordynowały również działanie poszczególnych ogniw w łańcuchu dostaw, ale jednak jeżeli nawet akceptowano elektroniczne dokumenty, to po realizacji lub w trakcie realizacji przedmiotowej transakcji należało obligatoryjnie dostarczyć dokument papierowy. Obecnie rzeczywistością staje się „biuro bez papie-

rów". Procesy gospodarcze będą się odbywać znacznie szybciej niż dotąd to było możliwe. Zwłaszcza w zakresie dostępności do informacji, pracy z aktualnymi dokumentami, szybkiej i rzetelnej wymiany informacji pomiędzy stronami w biznesie. Zintegrowany komputerowo system wspomagania pracy firmy pozwoli na „bezpapierową" obsługę finansów, księgowości, płac, gospodarki materiałowej, środków trwałych, transportu, zleceń, eksploatacji poszczególnych środków itp. Przełomem stanie się np. bezpośredni kontakt pracownika niskiego szczebla firmy z jej management'em.

Pewien przedsmak działania „**bezpapierowego biura**" poznaliśmy już w Polsce przy okazji wprowadzenia przez Zakład Ubezpieczeń Społecznych (ZUS) możliwości dostarczania wymaganych przez tę instytucję dokumentów poprzez Internet lub pocztę elektroniczną (e-maila) – ta możliwość należy do 2 grupy, tzn. nie wymaga elektronicznego podpisu, a polega na szyfrowaniu dokumentu i przesłaniu go e-mail'em. Pracodawcy, którzy zdecydowali się na rozpoczęcie przesyłania dokumentów rozliczeniowych do ZUS – u na pewno byli zaskoczeni faktem, że gdy przeszli pomyślnie ścieżkę certyfikacji, napotykali na problemy typu przepustowości sieci, szybkości transmisji danych itp. (to nowe problemy e-logistyki).

Jest rzeczą oczywistą, że w najbliższym czasie będzie konieczne opracowanie ogólnodostępnych i powszechnie obowiązujących dokumentów elektronicznych. Dokumenty te powinny być dostępne z odpowiednich stron WWW dla wszystkich zainteresowanych, lub przechowywane w swego rodzaju magazynach e-dokumentów zwanych repozytoriami.

Rola elektronicznego podpisu w e-logistyce

Upowszechnienie umiejętności korzystania z dobrodziejstw e-podpisu zmieni przede wszystkim istniejący stan rzeczy i dotychczasowe przyzwyczajenia w e-logistyce. Aby to osiągnąć, niezbędne będzie kreślenie podstawowych standardów postępowania w określonych sytuacjach biznesowych – uchwalenie odpowiednich przepisów prawnych, oraz zmiana świadomości ludzi pracujących w e-logistyce.

Należy spodziewać się następujących efektów działań upowszechnienia i stosowania technologii podpisu elektronicznego w e-logistyce:

- upowszechnienie i stosowanie standardów elektronicznych dokumentów podpisanych elektronicznie (w kontaktach B2B i B2C, w przetwarzaniu i obiegu dokumentów w firmie)
- zwiększenie handlu (transakcji) internetowego
- dostępu firm do internetowych giełd towarowych, transportowych
- ułatwienie dostępu do obiegu dokumentów w firmie (e-dokumentów) – zmniejszenie czasu uzyskiwania niezbędnych podpisów
- używania w korespondencji między stronami w biznesie elektronicznych wzorców dokumentów wg rodzajów zastosowań oraz tworzenia baz danych tych wzorców wraz z oprogramowaniem ich obsługi opracowanych specjalnie dla e-logistyki
- skrócenie czasu dokonywania transakcji, a tym samym zwiększenie ich ilości
- powstania odpowiednich systemów zaopatrzeniowo-dystrybucyjnych reagujących na szybkie zmiany popytu (dalszy rozwój systemów komputerowego wspomagania zarządzania i gospodarki magazynowej)
- powstanie portali posiadających zasoby i informacje dot. elektronicznej wymiany danych o klientach, transakcjach itp.

Ważną rzeczą jest przejście „ścieżki" uzyskiwania certyfikacji podpisu elektronicznego. W artykule tego nie omówiono, gdyż każda firma udzielająca certyfikacji pomaga swojemu przyszłemu klientowi wypełnić wszystkie formalności cywilno-prawne, ponieważ pobiera opłaty za swoje usługi wg określonego cennika. Rzeczą bardzo ważną jest opracowanie odpowiednich systemów implementacji e-podpisu w firmach, aby jego przebieg oparty był na pewnej strategii wdrożenia.