STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Adam KAPRALSKI
Politechnika Śląska, Instytut Informatyki

ROZPROSZONE SYSTEMY AUTENTYFIKACJI

Streszczenie. Proponowany hierarchiczny system o strukturze drzewa traktuje dokument elektroniczny jako podmiot wszelkiej komercji w Internecie. Wieloraka ochrona dokumentu przed zaginięciem bądź przed fałszerstwem czy też przed nieautoryzowanym dostępem do dokumentu nazywana jest autentyfikacją i jest nadrzędnym celem rozwijanego tutaj systemu. Przypisanie zadań do poszczególnych węzłów systemu pozwala widzieć system jako powiązanie niezależnych podmiotów gospodarczych traktujących każdą operację jako usługę komercyjną.

DISTRIBUTED AUTENTIFICATION SYSTEMS

Summary. The proposed distributed hierarchical system treats the electronic document as an object of e-commerce. Wide protection of the document against losing or forgery or non-authorized access is the basic target of the system developed here. Simultaneously the proposed solutions suggest possibility of investigation of numerous services performed at the Internet.

1. Bezpieczeństwo transakcji internetowych (e-commerce)

Rozwój Internetu i jego coraz szersze wykorzystanie w życiu gospodarczym, społecznym, urzędowym w tworzeniu środowiska dla rozwoju działalności kulturowej i naukowej stwarzają nieograniczone możliwości zastąpienia papieru szeroko rozumianym Interentem dla tworzenia, przekazywania i przechowywania dokumentów. Jednocześnie pewne rodzaje dokumentów wciąż nie są wprowadzane do obiegu elektronicznego z uwagi na wielorakie zagrożenia wiążące się z faktem zastąpienia papieru nośnikiem elektronicznym. Rozwijająca się dziedzina wykorzystania Internetu dla rozwoju działalności gospodarczej nazywana

e-commerce może być postrzegana jako dziedzina informatyki zajmująca się tworzeniem i obiegiem dokumentów w Internecie. Przyjmuje się dotychczas, że zapewnienie bezpieczeństwa związanego z wykorzystaniem e-commerce jest sprawą dwóch lub większej liczby partnerów przeprowadzających różnego rodzaju transakcje poprzez Internet [4]. Dotychczas państwo poza ściganiem przestępców niczego nie robi w sprawie zapewnienia większego bezpieczeństwa dla wszystkich partnerów wchodzących w transakcje za pośrednictwem Internetu. Tymczasem skutki prawne wynikające z rozwoju e-commerce mogą być dalekosiężne nie tylko dla partnerów prawdziwych lub zafałszowanych transakcji. W dalszej perspektywie brak wielorakich zabezpieczeń organizacyjnych stałby się hamulcem rozwoju wykorzystania Internetu w działalności gospodarczej a co najmniej nie pozwoli na dalszą eliminacje dokumentów tworzonych na nośniku papierowym. Zagrożenia mają charakter wieloraki i nieprzewidywalne skutki utraty dokumentów lub pojawienia się błędów lub celowych fałszerstw dokumentów mogą mieć nieobliczalne negatywne skutki dla funkcjonowania i rozwoju cywilizacji [1].

Rozwój systemów szerokiego zabezpieczania dokumentów elektronicznych jest niezwykle ważny przede wszystkim dlatego, że Internet stwarza potencjalnie większe możliwości zabezpieczenia informacji przed wieloraką działalnością przestępczą w porównaniu z informacją przekazywaną na nośniku papierowym. Istnienie bezpiecznych systemów wielorakiego zabezpieczenia dokumentu elektronicznego jest warunkiem dalszego rozwoju naszej cywilizacji, przede wszystkim zaś metod gospodarowania. Wyobraźmy sobie internetowy notariat oparty całkowicie na dokumencie elektronicznym. Poziom zabezpieczenia dokumentu elektronicznego jest wszystkim dla możliwości powstania rozwoju takich urzędów. Notariat to tylko jeden urząd przemawiający do wyobraźni przestępców, który także powinien przemawiać do osób odpowiedzialnych za bezpieczeństwo publiczne. Innym przykładem mogą być sądy, urzędy skarbowe, archiwa różnych organizacji państwowych i społecznych. Wszędzie tam zaginięcie lub sfałszowanie dokumentów może mieć bardzo wymierne skutki dla funkcjonowania i bezpieczeństwa.

Podsumowując dotychczasowe rozważania możemy powiedzieć.

Rozwój działalności gospodarczej z wykorzystaniem i za pośrednictwem Internetu (e-commerce) jest warunkowany wzrostem poziomu ufności dla dokumentów elektronicznych produkowanych, wykorzystywanych i przechowywanych w Internecie. Dokument elektroniczny jest z jednej strony środkiem pozwalającym na przeprowadzenie różnego rodzaju transakcji za pośrednictwem Internetu, z drugiej jednak strony dokument elektroniczny może być podmiotem szeroko rozumianych usług przeprowadzanych za pośrednictwem Internetu. Bezpieczeństwo państwa i jego

obywateli wymaga wielorakich działań poznawczych, organizacyjnych, ustawodawczych i gospodarczych dla rozwoju usług zorientowanych na dokument elektroniczny.

2. Pojęcie autentyfikacji

Poprzez autentyfikację rozumiemy zespół działań prawnych, administracyjnych i technicznych zabezpieczających dokument elektroniczny przed niepowołanym odczytem treści, przed zmianą treści dokumentu, przed zaginięciem dokumentu oraz przed pojawieniem się dokumentów od początku fałszywych.

Przedmiotem naszych rozważań jest organizacja systemu pozwalająca zabezpieczyć cele autentyfikacji dokumentu.Generalnie cele autentyfikacji można uzyskać poprzez wymuszenie protokolarnych zasad tworzenia i wykorzystania dokumentu elektronicznego w Internecie. Przedstawiając to zagadnienie bardziej obrazowo powiemy na przykład, że osoba sporządzająca dokument lub będąca stroną transakcji nie może mieć możliwości skutecznej zmiany dokumentu po jego autoryzacji. Osoba, która tworzy dokument, nie powinna mieć możliwości dotarcia do fizycznego nośnika przechowującego ten dokument jako dokument autoryzowany. Osoba (komponent systemu), która posiada wszystkie potrzebne kody nie powinna mieć możliwości odszyfrowania dokumentu, gdy dotrze do niego przypadkowo w czasie do tego nie przewidzianym. Szczegółowa specyfikacja zabezpieczeń dokumentu elektronicznego przed nieautoryzowanym utworzeniem, sfałszowaniem treści i niepowołanym odczytaniem zostanie przedstawiona w kolejnych sekcjach omawiających poszczególne rozwiązania organizacyjne i techniczne.

Uzyskanie takiego celu jest generalnie możliwe w systemie, gdzie każda operacja dokonywana na dokumencie ma charakter transakcji wielostronnej, przy czym strony (partnerzy) nie muszą być ustaleni dla wszystkich transakcji dokonywanych na danym dokumencie. Bezpieczeństwo przed atakiem globalnym lub terrorystycznym dotykającym zarchiwizowanych dokumentów zapewnia rozproszone fizycznie archiwum oraz ukrycie fizycznych adresów poszczególnych komponentów systemu. Zabezpieczenie działania systemu przed praktykami korupcyjnymi daje rozproszenie i niestałość komponentów systemu pełniących funkcje kontrolne i nadzorcze oraz ich możliwie największą anonimowość oraz rozproszenie dokumentu w różnych węzłach systemu. Ukryciem najlepszym dokumentu w archiwum internetowym jest jego „przeźroczystość" dla wyszukiwarek internetowych w przypadku, gdy zamierzona operacja nie ma charakteru autoryzowanej transakcji.

Podsumowując uważamy, że dokument elektroniczny powstały i istniejący w Internecie pod kontrolą systemu autentyfikacji nie jest produktem dotyczącym wyłącznie jego merytorycznych sygnatariuszy, lecz jest obiektem systemowym, a celem systemu jest ochrona dokumentu przed utratą, fałszerstwem oraz przed nie- autoryzowanym dostępem do niego. Działania polegające na zapewnieniu bez- pieczeństwa dokumentów mogą być przedmiotem usług wykonywanych poprzez wy- specjalizowane agencje posiadające różne prerogatywy państwa jako gwaranta na- leżytej ochrony dokumentu.

3. Podstawowa organizacja rozproszonego systemu autentyfikacji dokumentów

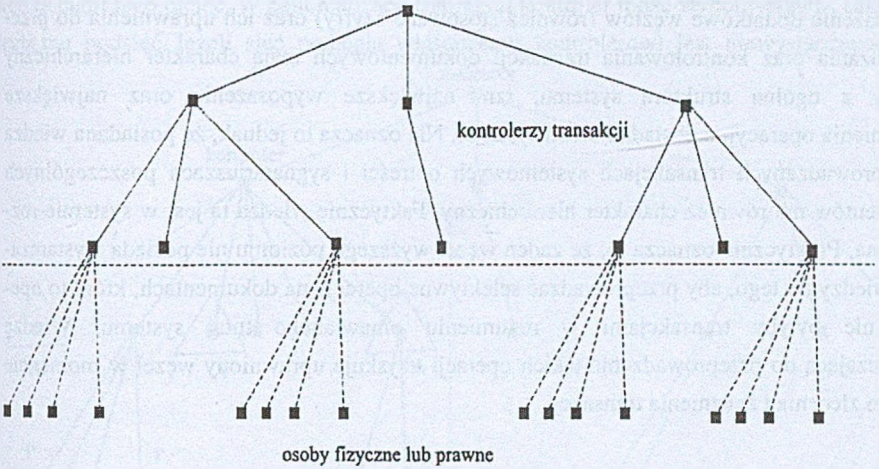
Omawiany system autentyfikacji jest systemem hierarchicznym o strukturze drzewiastej, którego zadaniem jest kreowanie, przeprowadzanie, kontrolowanie i nadzorowanie operacji na dokumentach elektronicznych w Internecie. System jest otwarty posiadając zdolność autokreacji i ciągłego wzrostu poprzez dołączanie i rejestrację nowych węzłów. Szczegóły tego procesu nie są przedmiotem rozważań niniejszego tekstu. Podstawowy schemat strukturalny omawianego systemu autentyfikacji przedstawiono na rys.1. Komponentem każdego węzła systemu jest model podpisowo-rejestracyjny. Ponadto pewne węzły systemu wyposażone są w urządzenia dla elektronicznej archiwizacji dokumentów (nie własnych) zaistniałych w systemie. W ten sposób zbiór węzłów systemu posiadających urządzenia do archiwizacji tworzy rozproszone archiwum systemu. Obecność własnych archiwów wszystkich węzłów systemu jest wystarczająco oczywista; archiwa takie nie powinny być przyłączone do Internetu. Węzły w momencie powołania otrzymują uprawnienia do wykonywania określonych transakcji. Uprawnienia te są zależne przede wszystkim od miejsca węzła w hierarchii systemu. Węzły będące liśćmi systemu hierarchii reprezentują osoby fizyczne lub prawne, będące klientami systemu, posiadające uprawnienia do zlecania transakcji.

Działania z poziomu liści systemu dokonywane za pośrednictwem modelu rejestracyjno-podpisowego:

a) generacja zmiennego podpisu elektronicznego w celu przedstawienia danych dla autentyfikacji węzła lub jego działań,
b) rejestracja własnych kolejnych działań.

Węzły mogą komunikować się z innymi węzłami poprzez Internet w celu nawiązania kontaktu dla wszczęcia transakcji dokumentowych, które jednak mogą być skutecznie dokonane

po wypełnieniu funkcji kontrolnych lub operacyjnych poprzez inne węzły właściwe dla poszczególnych transakcji.



Rys. 1. Struktura systemu autentyfikacji
Fig. 1. The structure of autentification system

Węzły systemu znajdujące się poza najniższym poziomem hierarchii mogą wykonywać wszystkie te funkcje które wykonują liście systemu hierarchii. Ponadto mogą spełniać następujące funkcje dodatkowe o charakterze kontrolnym, operacyjnym lub nadzorującym.

Działania dokonywane z wyższego poziomu hierarchii za pośrednictwem modelu rejestracyjno-podpisowego:

a) rejestracja kolejnych węzłów potomnych następnego poziomu (wyłącznie synów), generacja ich modeli podpisowo-rejestracyjnych,
b) wykorzystanie modeli (synów) celem dokonania ich każdorazowej autentyfikacji lub autentyfikacji ich działań,
c) przeprowadzanie pełnej rejestracji transakcji inicjowanych poprzez synów lub rejestracja skrócona i kontrola lub nadzór transakcji wykonywanych poprzez węzły potomne.

Ponadto węzły te mogą dokonywać przydziału konkretnych węzłów systemu dla rozproszonej archiwizacji dokumentu lub mogą same dokonywać rozproszonej archiwizacji dokumentu, lub mogą udostępniać rozproszone archiwum w celu kontroli autentyczności dokumentu czy w celu odczytania treści tego dokumentu. Każdy węzeł systemu posiada uprawnienia odnośnie do inicjowania określonych transakcji. Jeżeli transakcja wymaga inicjacji lub obecności dwóch lub większej liczby węzłów systemu, wtedy funkcje kontrolne i sterownicze

przyjmuje węzeł będący najbliższym przodkiem wszystkich partnerów transakcji a do wykonania transakcji kontroler ma do dyspozycji całą podległą mu sieć.

Wyposażenie dodatkowe węzłów (również stosowane szyfry) oraz ich uprawnienia do przeprowadzania oraz kontrolowania transakcji dokumentowych mają charakter hierarchiczny zgodny z ogólną strukturą systemu, tzn. największe wyposażenie oraz największe uprawnienia operacyjne posiada korzeń systemu. Nie oznacza to jednak, że posiadana wiedza o przeprowadzanych transakcjach systemowych o treści i sygnatariuszach poszczególnych dokumentów ma również charakter hierarchiczny. Faktycznie wiedza ta jest w systemie rozproszona. Praktycznie oznacza to, że żaden węzeł wyższego poziomu nie posiada wystarczającej wiedzy do tego, aby przeprowadzać selektywne operacje na dokumentach, które to operacje nie byłyby transakcjami w rozumieniu omawianego tutaj systemu. Wiedzę wystarczającą do przeprowadzenia takich operacji uzyskuje uprawniony węzeł w momencie pełnego zlecenia i zaistnienia transakcji.

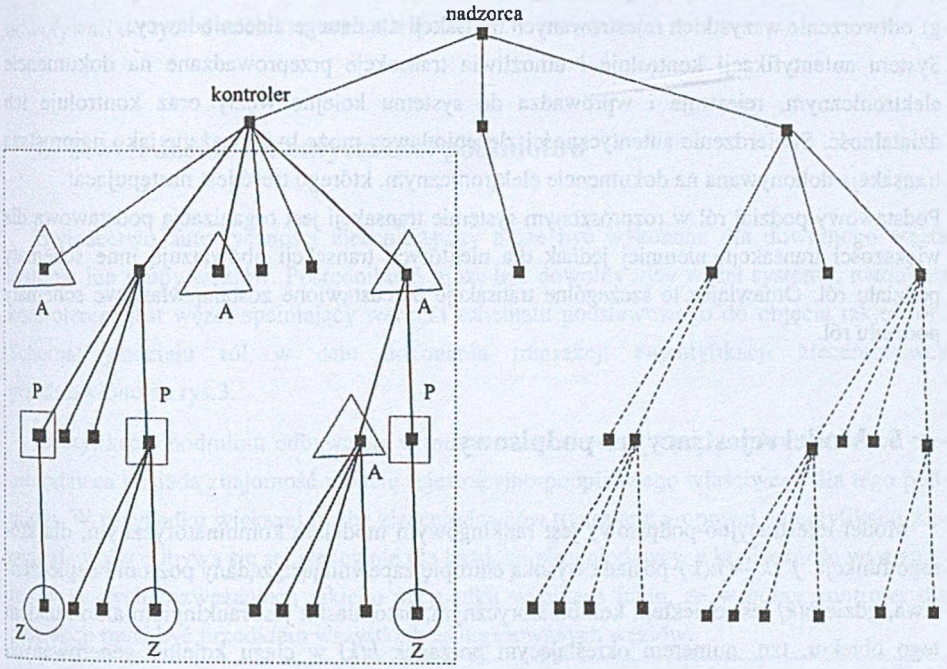
4. Transakcje autentyfikacji

Dokument elektroniczny rozumiany jest jako stwierdzenie dowolnego faktu o charakterze prawnym, obejmującego co najmniej jeden podmiot systemu lub większą ich liczbę. Środowiskiem dla systemu autentyfikacji dokumentów jest Internet.

Do opisu transakcji przeprowadzanych w systemie zdefiniujemy role, które pełnią właściwe dla danej transakcji węzły systemu. Przykładowe przypisanie określonych ról do węzłów systemu przedstawiono na rys.2. Każda transakcja jest inicjowana poprzez jeden lub więcej węzłów systemu nazywanych **zleceniodawcą;** zleceniodawców oznaczono na rys.2 poprzez literę Z. W większości przeprowadzanych transakcji zleceniodawcami są liście systemu, tzn. osoby fizyczne lub prawne niemniej jednak zleceniodawcą może być również inny węzeł, z wyjątkiem korzenia, zlecający transakcje na zamówienie osób lub instytucji nie reprezentowanych w systemie. Przykładowo, transakcje w systemie mogą być dokonywane na zlecenie sądów, prokuratury, organów administracji lub organów śledczych. Instytucje te nie muszą być w systemie reprezentowane, lecz mogą być zainteresowane zlecaniem transakcji o charakterze kontrolnym.

Każdy węzeł, którego jeden lub więcej węzłów synowskich pełni rolę zleceniodawcy, nosi nazwę **pośrednika** i oznaczony jest na rys.2 poprzez literę P.

Najbliższy węzeł wspólny przodek wszystkich zleceniodawców oraz wszystkich pośredników nosi nazwę **kontrolera**. Jeżeli transakcja dotyczy tylko jednego pośrednika, to funkcje kontrolera pełni jego ojciec. W celu realizacji transakcji kontroler może wykorzystywać całą podległą mu podsieć. Jeżeli sieć podległa właściwemu kontrolerowi jest niewystarczająca do



Rys. 2. Podstawowy podział ról w rozproszonym systemie transakcji
Fig. 2. Basic distribution of roles at the transaction system

wykonania określonej transakcji, wtedy kontroler przekazuje swoje funkcje swojemu przodkowi (bezpośredniemu lub kolejnemu), który dysponuje wystarczającą podsiecią do wypełnienia zlecanej transakcji. Ponadto dla niektórych transakcji, przede wszystkim korzystających z rozproszonego archiwum systemowego, powoływany jest **nadzorca,** który dzieli funkcje kontrolno-operacyjne z kontrolerem. Nadzorca nie musi być równocześnie korzeniem systemu, chociaż takie przypisanie nie jest wykluczone.

Dokument elektroniczny wchodzi do obiegu internetowego i jest przedmiotem różnych operacji wykonywanych na nim w wyniku zaistnienia rozmaitych transakcji, takich jak:

a) stwierdzenie autentyczności zleceniodawców,
b) rejestracja dokumentu,

c) kreacja dokumentu w Internecie,
d) archiwizacja rozproszona w Internecie,
e) stwierdzenie autentyczności dokumentu lub odczytanie dokumentu zarchiwizowanego,
f) odczytanie treści całego rozproszonego archiwum,
g) odtworzenie wszystkich rejestrowanych transakcji dla danego zleceniodawcy.

System autentyfikacji kontroluje i umożliwia transakcje przeprowadzane na dokumencie elektronicznym, rejestruje i wprowadza do systemu kolejne węzły oraz kontroluje ich działalność. Stwierdzenie autentyczności zleceniodawcy może być uważane jako najprostsza transakcja dokonywana na dokumencie elektronicznym, którego treść jest następująca: Podstawowy podział ról w rozproszonym systemie transakcji jest organizacją podstawową dla większości transakcji, niemniej jednak dla niektórych transakcji obowiązują inne schematy podziału ról. Omawiając te szczególne transakcje przedstawione zostaną właściwe schematy podziału ról.

5. Model rejestracyjno-podpisowy

Model rejestracyjno-podpisowy jest rankingowym modelem kombinatorycznym, dla którego funkcja $f : k \rightarrow h(k)$ posiada wysoką entropię zapewniającą żądany poziom bezpieczeństwa, gdzie $h(k)$ jest obiektem kombinatorycznym, natomiast k jest rankingiem albo rankiem tego obiektu, tzn. numerem określającym porządek $h(k)$ w ciągu kolejno generowanych obiektów [2][3] . Węzeł (ojciec) generuje model rejestracyjno-podpisowy dla każdego swojego węzła (syna) i nadaje mu identyfikator obowiązujący w systemie. Ponadto przekazuje początkową wartość k_0 rankingu k użytkownikowi tego modelu. Użytkownik dokonując rejestrowanych transakcji w Internecie dla tego modelu każdorazowo po dokonaniu transakcji zwiększa bieżącą wartość k (pierwsza rejestrowana transakcja jest przeprowadzana przy $k=k_0$). Użytkownik modelu jest zobowiązany ponadto do zapisu wszystkich rejestrowanych transakcji lub może zlecić prowadzenie takiego rejestru węzłowi-ojcu. Jak to zostanie pokazane w kolejnych sekcjach odtworzenie rejestru transakcji rejestrowanych dla każdego podanego węzła jest w systemie możliwe, jednakże jest to transakcja najbardziej czasochłonna i wymagająca zaangażowania wszystkich węzłów systemu. Dlatego transakcja ta nie może być przeprowadzana zbyt często i w związku z tym w systemie komercyjnym powinna być obciążona wysokim kosztem.

Ponieważ model rejestracyjno-podpisowy może być wykorzystany zasadniczo na dwa sposoby, dlatego dla każdego modelu określić należy podział dopuszczalnych wartości k na

dwie klasy: klasa małych wartości k oraz klasa dużych wartości k. Na przykład możemy przyjąć, że zbiór wartości małych tworzy przedział [1÷10000], wartości duże są dla $k>10000$. W zastosowaniach specjalnych konkretnego modelu rejestracyjno-podpisowego przedział wartości małych może zostać znacznie rozszerzony. W opisie transakcji będziemy się odwoływali do tych dwóch klas wartości k.

6. Stwierdzenie autentyczności podmiotów

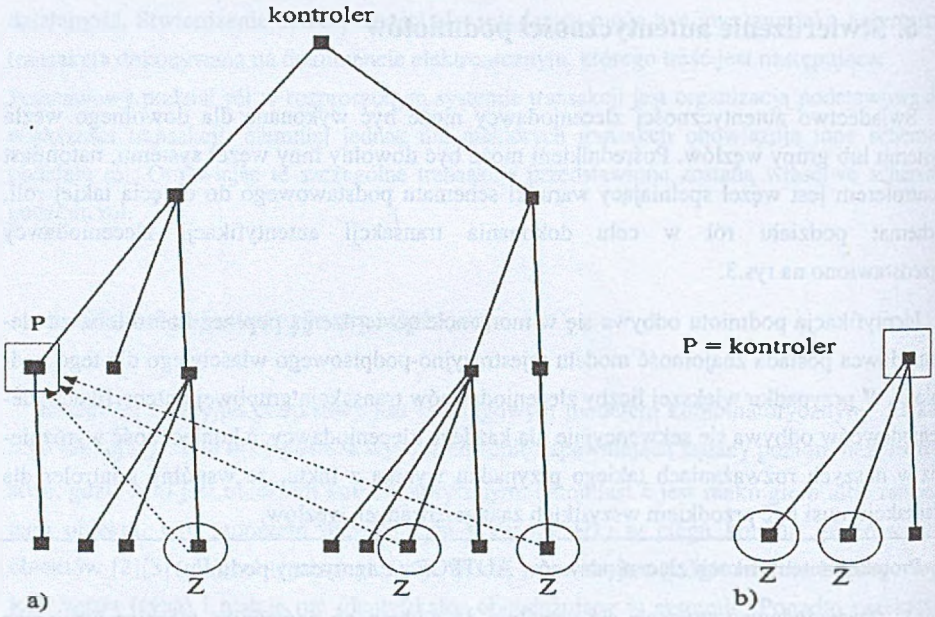
Świadectwo autentyczności zleceniodawcy może być wykonane dla dowolnego węzła systemu lub grupy węzłów. Pośrednikiem może być dowolny inny węzeł systemu, natomiast kontrolerem jest węzeł spełniający warunki schematu podstawowego do objęcia takiej roli. Schemat podziału ról w celu dokonania transakcji autentyfikacji zleceniodawcy przedstawiono na rys.3.

Identyfikacja podmiotu odbywa się w momencie stwierdzenia poprzez kontrolera, że zleceniodawca posiada znajomość modelu rejestracyjno-podpisowego właściwego dla tego podmiotu. W przypadku większej liczby zleceniodawców transakcja grupowej autentyfikacji zleceniodawców odbywa się sekwencyjnie dla każdego zleceniodawcy, a konieczność wyróżnienia w naszych rozważaniach takiego przypadku wynika z faktu, że wspólny kontroler dla transakcji musi być przodkiem wszystkich zaangażowanych węzłów.

Protokół autentyfikacji zleceniodawców AUTPOD (autentyczny podmiot)

1. Zleceniodawcy zwracają się wspólnie do wybranego pośrednika zlecając wzajemną autentyfikację i przekazują pośrednikowi identyfikatory własnych modeli rejestracyjno-podpisowych.
2. Pośrednik wybiera węzeł do wypełnienia roli kontrolera i nawiązuje z nim kontakt przesyłając identyfikatory modeli zleceniodawców.
3. Kontroler dla każdego zleceniodawcy indywidualnie generuje liczbę k (generacja jest losowa) i oblicza dla każdego modelu rejestracyjno-podpisowego podmiotu obiekt kombinatoryczny $h(k)$. W celu uniknięcia niebezpieczeństwa przechwycenia poprzez obserwatorów zewnętrznych pary $(k, h(k))$ dla jakiegokolwiek modelu rejestracyjnego i wykorzystania go w terminie późniejszym niezgodnie z intencją właściciela modelu rejestracyjno-podpisowego wartość k musi należeć do strefy wartości wielkich.
4. Kontroler przekazuje do pośrednika liczby k informując, dla którego zleceniodawcy jest każda liczba.

5. Pośrednik przekazuje każdemu zleceniodawcy wygenerowaną dla niego liczbę *k*.
6. Każdy zleceniodawca oblicza *h(k)* w swoim modelu i przekazuje wynik pośrednikowi.
7. Pośrednik przesyła obliczone przez każdego zleceniodawcę *h(k)* do kontrolera.
8. W przypadku zgodności *h(k)* podanych przez każdego zleceniodawcę i obliczonych uprzednio poprzez kontrolera stwierdzającego autentyczność zleceniodawców. W przypadku jakiejkolwiek niezgodności kontroler produkuje protokół niezgodności. W każdym przypadku wynik jest przesyłany do pośrednika.



Rys. 3. Schemat blokowy dla realizacji autentyfikacji zleceniodawców
Fig. 3. Block diagram for autentification of customers

9. Pośrednik informuje zleceniodawców o wyniku i wynik transakcji rejestruje w swoich urządzeniach archiwizujących.

W przypadku gdy pośrednik pełni również funkcję kontrolera, protokół AUTPOD ulega stosownemu uproszczeniu jedynie poprzez eliminację przesłań pomiędzy kontrolerem i pośrednikiem. Wszystkie inne funkcje wypełniane są analogicznie. Autentyfikacja zleceniodawcy może również mieć miejsce w siedzibie kontrolera, co wyłącza pośrednictwo Interentu dla tej transakcji, czyniąc ją wolną od jakichkolwiek zagrożeń wynikających z faktu, że podstawowy protokół AUTPOD realizowany jest w Internecie.

7. Podpis rejestrowany

Celem transakcji podpis rejestrowany jest stwierdzenie, że każdy zleceniodawca złożył podpis na dokumencie i że jest to kolejny jego podpis w sekwencji podpisów rejestrowanych.

Sens podpisu rejestrowanego jest następujący:

a) podpis może zostać wykorzystany tylko raz, co eliminuje zagrożenia związane z więcej niż jednokrotnym jego użyciem,

b) aktualna wartość *k* dla danego modelu rejestracyjno-podpisowego informuje, że posiadacz tego modelu podpisał *k-1* dokumentów rejestrowanych i rejestr tych dokumentów znajduje się u węzła-ojca.

W przypadku gdy dokument jest sygnowany podpisem rejestrowanym przez szereg węzłów systemu posiadających relatywnie odległego wspólnego przodka, wtedy dokument posiada szereg rozproszonych w systemie śladów, które są stosunkowo trudne do usunięcia, tym bardziej, że usunięcie wszystkich śladów nie jest możliwe z uwagi na istnienie archiwów prywatnych sygnatariuszy dokumentu i co istotne - usunięcie oznaczałoby niewytłumaczalne dziury w rejestrach dokumentów sygnowanych przez sygnatariuszy. Rejestrowany podpis nie oznacza, że w systemie istnieje kopia dokumentu, a jedynie oznacza, że system posiada informacje o zaistnieniu transakcji w określonym czasie i przy udziale określonych partnerów.

Protokół autentyfikacji podpisów rejestrowanych REJPOD (rejestrowany podpis)

1. Każdy ze zleceniodawców zwraca się do swojego właściwego pośrednika, przekazując identyfikator wspólnego dokumentu oraz identyfikatory pośredników pozostałych partnerów i zamawia transakcje podpisu rejestrowanego, dotyczącego wspólnego dokumentu.
2. Pośrednicy kontaktują się ze sobą i powołują kontrolera transakcji zgodnie z ogólnymi regułami posługując się w korespondencji identyfikatorem dokumentu.
3. Każdy zleceniodawca przekazuje swojemu pośrednikowi aktualną wartość *h(k)*, a następnie zwiększa o jeden wartość *k* w swoim modelu rejestracyjno-podpisowym.
4. Każdy pośrednik sprawdza zgodność podpisu oraz zwiększa o jeden wartość *k* w przechowywanym modelu rejestracyjno-podpisowym zleceniodawcy.
5. Pośrednicy przekazują podpisy (wartości *h(k)*) do kontrolera, który stwierdza zgodność podpisów i sporządza raport zgodności umieszczając na nim wszystkie wartości *h(k)* oraz identyfikatory pośredników. Identyfikatory modeli rejestracyjno-podpisowych oraz bieżące wartości *k* nie są umieszczane w raporcie.

6. Raport jest archiwizowany u kontrolera oraz jego kopie są przesyłane do pośredników, którzy uzupełniają dane identyfikacyjne swoich zleceniodawców i tak uzupełniony raport archiwizują oraz jego kopię przekazują zleceniodawcy.

Zaletą przedstawionego protokołu REJPOD jest autoryzacja dokonania podpisu rejestrowanego na wspólnym dokumencie, natomiast informacja o uczestnikach transakcji jest rozproszona w systemie. Dokument sam jako taki nie jest znany żadnemu elementowi systemu poza partnerami. Pomimo tego żaden z partnerów transakcji nie może zaprzeczyć, że wspólnie z pozostałymi partnerami złożył podpis rejestrowany na wspólnym dokumencie.

8. Transformacja podpisu

W przedstawionym systemie każdy węzeł posiada swój własny model rejestracyjno-podpisowy wykorzystywany do składania zmiennych podpisów oraz do rejestracji aktualnej wartości k w celu zapewnienia funkcjonowania podsystemu podpisu rejestrowanego. Ponadto dla każdego modelu rejestracyjno-podpisowego parametrem łatwym do wyliczenia jest liczba różnych funkcji wyboru (obiektów kombinatorycznych), właściwa dla danego modelu. Liczbę różnych obiektów kombinatorycznych dla danego modelu oznaczamy przez $|\{h\}|$. Entropia wartości $|\{h\}|$ podobnie jak entropia pary $(k, h(k))$ dla nieznanego modelu rejestracyjno-podpisowego rośnie wykładniczo w zależności od wartości parametrów n i m, charakteryzujących rozmiar modelu.

Niech będą dane dwa modele rejestracyjno-podpisowe oznaczone odpowiednio: R_1 oraz R_2. Dany jest model R_2 oraz podpisy $(k_1, h_1(k_1))$, będące produktem danego modelu R_1. Niech $w1=|\{h\}|_1$, i $w2=|\{h\}|_2$. Stosunek $q=\frac{w1}{w2}$ dla w2>w1 lub $q=\frac{w2}{w1}$ dla w1>w2 stanowi podstawę do obliczenia wartości $k=f(k_1, q)$, gdzie funkcja $k=f(k_1, q)$ jest dowolnym odwzorowaniem izomorficznym. Wtedy mamy $k_1=f^{-1}(k_1, q)$. Mając wartość k oraz model R_1 można obliczyć nowy podpis $(k,\{k\})$, który oznaczamy poprzez $T((k_1, h_1(k_1)))$, podkreślając w ten sposób, że podpis $(k, h(k))$ jest transformacja podpisu $((k_1,h_1(k_1))$ dokonaną przy wykorzystaniu modelu R_2. Zakładamy, że model R_2 jest własnością kontrolera i on dokonuje transformacji mając wszystkie potrzebne dane.

Zaszyfrowanie treści dokumentu szyfrem systemowym oraz przeprowadzenie transformacji podpisu czyni dokument „przeźroczystym" (nierozpoznawalnym) dla wszystkich użytkowników Internetu, włączając w to sygnatariuszy dokumentu i ich pośredników. Faktycznie węzły posiadające większe uprawnienia w systemie posiadają również szyfry,

którymi taki dokument został zaszyfrowany, co oznacza, że takie węzły mogą teoretycznie odszyfrować treść dokumentu, jednakże sygnatariuszy rozpoznać nie mogą.

9. Rejestrowany dokument

Rejestracja dokumentu oznacza transakcję polegającą na archiwizacji kopii dokumentu w systemie. Treść dokumentu nie musi zostać ujawniona żadnemu elementowi systemu, ponieważ dokument w systemie może być reprezentowany wyłącznie jako szyfrogram powstały w wyniku kontaktu poprzez Internet lub kontaktu osobistego zleceniodawców. Schemat organizacyjny do dokonania tej transakcji jest taki, jak to przedstawiono na rys.2, z tym, że środki do rozproszonej archiwizacji nie muszą zostać zaangażowane do wypełnienia transakcji. Istotą tej transakcji jest archiwizacja jawna, tzn. miejsca w systemie, gdzie przechowywane są wszystkie kopie dokumentu, znane są wszystkim zleceniodawcom, ich pośrednikom oraz kontrolerowi. Protokół w swojej głównej części nie różni się od podpisu rejestrowanego, z tym, że pośrednicy oraz kontroler otrzymują od zleceniodawców kopię tekstu dokumentu, na której każdy zleceniodawca dopisuje swoje $h(k)$ zgodnie z protokołem REJPOD. Kontroler oprócz stwierdzenia autentyczności podpisów stwierdza zgodność wszystkich kopii tekstu, następnie umieszcza wszystkie wartości $h(k)$ na jednej kopii, którą zapisuje i dalej przesyła wszystkim pośrednikom. Pośrednicy archiwizują u siebie otrzymane kopie zarejestrowanego dokumentu od kontrolera i przesyłają dalej do swoich zleceniodawców. Słabością takich działań systemowych jest stosunkowo duża łatwość dotarcia do fizycznych nośników kopii dokumentu, co umożliwia różnego rodzaju fałszerstwa.

10. Rozproszona archiwizacja dokumentu

Archiwum rozproszone systemu zawiera dokumenty elektroniczne będące wynikiem transakcji zawartych w systemie. Celem rozproszonej archiwizacji może być zabezpieczenie dokumentu przed utratą na wypadek awarii części systemu lub przed fałszerstwem dokonanym przez osoby zainteresowane zmianą treści lub usunięciem dokumentu po jego rejestracji w systemie. Pierwszy cel osiągamy poprzez archiwizację wielu kopii dokumentu w węzłach rozproszonego archiwum. Drugi cel osiągany jest poprzez ukrycie treści archiwizowanych plików w wyniku szyfrowania systemowego oraz poprzez ukrycie przed

węzłami systemu nie posiadającymi autoryzacji dostępu do danego archiwizowanego pliku wszystkich identy-fikatorów (złożonych na dokumencie podpisów) tego dokumentu. Ukrycie podpisów doko-nywane jest w przypadku ogólnym poprzez zastąpienie złożonych na dokumencie podpisów (k, $h(k)$) ich transformacjami $T(k, h(k))$.

Protokół archiwizacji rozproszonej przedstawiono jak następuje.

Protokół archiwizacji rozproszonej AUROZ (archiwizacja rozproszona)

Struktura archiwizacji rozproszonej jest podobna do ogólnej struktury transakcji dokumentowych przedstawionej na rys. 2. Jednakże funkcje kontrolne nie są wykonywane tylko poprzez jeden węzeł kontrolny, lecz zamiast tego są podzielone pomiędzy dwa węzły- jeden z nich jest kontrolerem (w sensie rys. 2), natomiast drugi węzeł, będący przodkiem kontrolera, pełni funkcję nadzorcy.

1. Nadzorca i kontroler wybrani przez pośredników otrzymują zaszyfrowany szyframi pośredników dokument, z tym, że kontroler otrzymuje ponadto podpisy zlecenio-dawców oraz identyfikatory ich modeli rejestracyjno-podpisowych.
2. Kontroler dokonuje podziału dokumentu na części i każdą część szyfruje własnym szyfrem.
3. Podpisy (k,$h(k)$ sygnatariuszy kontroler transformuje na podstawie swojego modelu rejestracyjno-podpisowego do postaci $T(k,h(k))$.
4. Każda zaszyfrowana część dokumentu jest etykietowana jedną z transformat $T(k, h(k))$ oraz wszystkie zaetykietowane części są przesyłane do nadzorcy, który kontroluje poprawność podziału i szyfrowania dokumentu.
5. Nadzorca przekazuje potwierdzenie zgodności kontrolerowi i pośrednikom oraz zapisuje każdą część w rozproszonym archiwum systemowym.

Rozważmy teraz przypadek, gdy jest tylko jeden sygnatariusz dokumentu i dokument jest opatrzony jednym jego elektronicznym podpisem lub gdy liczba umieszczonych sygnatariuszy jest mniejsza od liczby wymaganych części do archiwizacji. Wtedy kontroler modyfikuje kroki 2 oraz 3 przeprowadzając kilka transformacji tego samego podpisu i wykorzystując dla każdej transformacji inne odwzorowanie izomorficzne. Symbolicznie oznacza to, że kontroler produkuje transformacje $T_1(k, h(k))$, $T_2(k, h(k))$, ... $T_u(k, h(k))$ dla jednego podpisu (k, $h(k)$). Następnie dzieli on dokument na u części każdej q-tej części przypisując transformację $T_q(k, h(k))$ jako jej identyfikator $1 \leq q \leq u$. Każda część jest szyfrowana i może zostać indywidualnie zarchiwizowana.

Zauważmy, że zarchiwizowany w ten sposób dokument jest w normalnych warunkach „przeźroczysty" dla wszystkich węzłów systemu poniżej kontrolera i nadzorcy, gdyż nawet pośrednicy i zleceniodawcy nie znają transformat swoich podpisów. Jednakże przeszukiwanie zupełne przy wykorzystaniu wyszukiwarek internetowych wszystkich możliwych podpisów danego modelu rejestracyjno-podpisowego umożliwia odszukanie wszystkich plików w archiwum opatrzonych jakimś podpisem tego modelu. Z uwagi jednak na wykładniczo rosnącą liczbę możliwych podpisów dla danego modelu wyszukiwanie takie w większości przypadków jest czasowo niewykonalne, ponadto duże liczby operacji wyszukiwania przeprowadzane z jednego miejsca powinny zwrócić uwagę służb odpowiedzialnych za bezpieczeństwo w Internecie.

Względy bezpieczeństwa nakazują tworzyć szereg rozproszonych archiwizacji tego samego dokumentu. Wtedy prawdopodobieństwo nieautoryzowanego usunięcia wszystkich śladów zarchiwizowanego dokumentu może być dowolnie małe. Zauważmy jednak, że przeszukiwanie zupełne (sekwencyjne) rozproszonego archiwum pozwala na odnalezienie i identyfikację dokumentów rozproszonych w archiwum. Takie jednak przeszukiwanie wymaga posiadania pełnych uprawnień i wszystkich potrzebnych informacji systemowych, dlatego nieautoryzowane dokonanie takiego przeszukiwania wydaje się być mało prawdopodobne.

11. Podsumowanie

Koncepcja i funkcje przedstawionego systemu dla szeroko rozumianej ochrony dokumentu elektronicznego są konsekwencją szczególnych własności zmiennego podpisu elektronicznego, rozwiniętego na podstawie własności niemonotonicznych modeli rankingowych. Zwłaszcza te własności omówionego tutaj systemu, które dotyczą zabezpieczenia dokumentu przed fałszerstwem dzięki rozproszonej i ukrytej dla sygnatariuszy archiwizacji mają szczególne znaczenie dla szerokiego rozwoju usług przeprowadzanych w Internecie. Stwarza to w perspektywie nieograniczone możliwości zastąpienia urzędów i biur tradycyjnych urzędami i biurami funkcjonującymi w Internecie. Podkreślenia wymaga fakt, że przedstawione możliwości oznaczają nie tylko większą wygodę szeroko rozumiane pozytywne konsekwencje ekonomiczne, ale także większą ochronę społeczności ludzkiej przed działalnością przestępczą.

LITERATURA

1. Boni W. Kovacich G. L.: I-Way Robbery: Crime on the Internet. New York Butterworth- Heinemann 1999.
2. Kapralski A.: Modeling and Generation of Arbitrary sets of Combinatorial Objects and their Sequential and Parallel Generation. Studia Informatica Vol. 21, No 2(40) Silesian University of Technology Press, Gliwice 2000.
3. Kapralski A.: Niemonotoniczne modele rankingowe. Studia Informatica Vol. 21, No 1 (40) pp. 601-612, Gliwice 2000.
4. Trepper Ch. H.: E-Commerce Strategies. Publication of Microsoft Corporation, Washington 2000.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 28 marca 2001 r.

Abstract

The presented in this paper system for distributed autentification is developed for wide protection of electronic document against losing, forgery and no authorized access. The hierarchical open system of authentification possess the tree structure enabling us its wide spreading within Internet. Each node can be seen as an independent company taxing customers for their services. The foundation of the system create specific properties of the changeable digital signature built basing on the properties of non- monotonic ranking models. We reach the targets of document protection by registered or not registered signature and/or by distributed archive in which copies of numerous parts of the document can be stored. The system give perspective of wide development of e-commerce concerning document as a subject of numerous services.