ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 598 EKONOMICZNE PROBLEMY USŁUG NR 58 2010

RYSZARD KOBUS
Instytut Łączności Państwowy Instytut Badawczy
R.Kobus@itl.waw.pl

ELEKTRONICZNE USŁUGI POCZTOWE

Wprowadzenie

Współczesne systemy łączności umożliwiają przesyłanie wiadomości i dokumentów w wielu formach. Chociaż wiadomości w postaci elektronicznej docierają do nas szybciej będziemy jeszcze długo korzystać z przekazu w formie papierowej. Jest wiele przyczyn, które to powodują, na przykład:

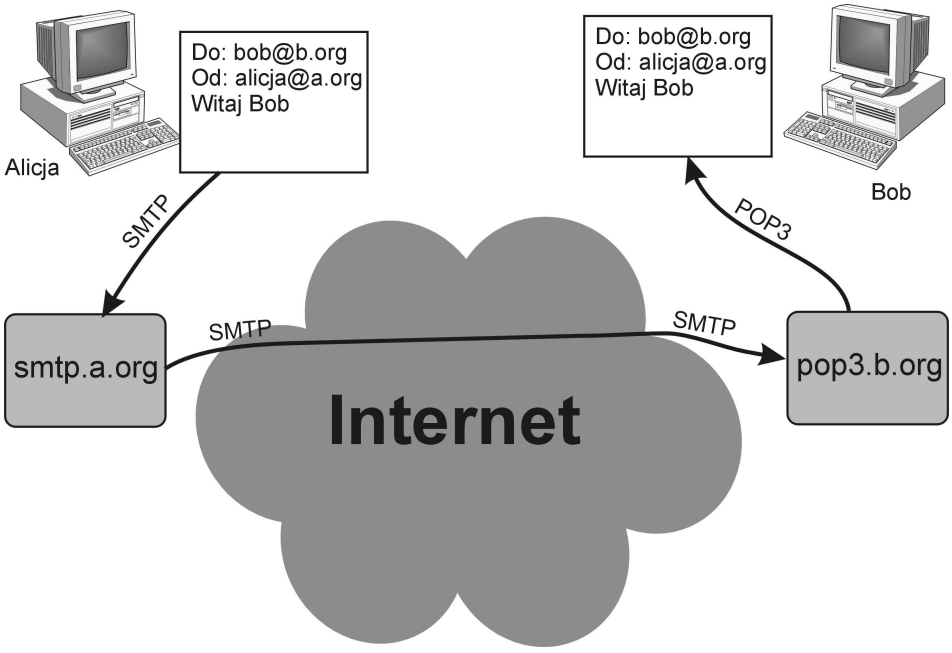
- względy kulturowe,
- względy prawne,
- brak infrastruktury technicznej,
- większy poziom bezpieczeństwa.

Zauważmy, że przekaz wiadomości w formie papierowej nie jest narażony na infekcje wirusem komputerowym, zniekształceniem czy kradzieżą w sieci, co powoduje, że poczta tradycyjna ma opinię usługi znacznie bezpieczniejszej niż poczta elektroniczna.

1. Stosowane technologie

Informacja przesyłana w formie elektronicznej, za pośrednictwem usługi zwykłej poczty elektronicznej, jest narażona na różne zagrożenia. Nie jest to usługa „on-line", co oznacza, że opóźnienie wnoszone w trakcie transmisji jest wystarczająco duże, aby możliwa była zamiana lub zniekształcenie informacji. Adresat nie dostaje także pełnej informacji o jej przebiegu i dokonanych

operacjach. Dostęp do usługi jest prosty i praktycznie każdy użytkownik sieci może korzystać z usługi poprzez jeden z wielu serwerów pocztowych, a nawet uruchomić własny serwer pocztowy. Adresat może więc otrzymać wiadomość z niepewnego źródła, np. zawierającą złośliwe oprogramowanie.



Rys 1. Klasyczna poczta elektroniczna

Węzeł pocztowy składa się z dwóch logicznych serwerów (rys. 1). Serwer SMTP[1] jest przeznaczony do nadawania poczty przekazywanej przez użytkowników mających swoje konta pocztowe na serwerze, natomiast obieranie dostarczonej poczty jest realizowany poprzez serwer POP3[2] lub IMAP[3]. Użytkownik przy pomocy specjalizowanej aplikacji pocztowej łączy się z serwerem SMTP i przesyła swoje wiadomości wraz z załącznikami. Następnie serwer pocztowy odszukuje w sieci adres serwera pocztowego adresata

[1] *Simple Mail Transfer Protocol* – protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie

[2] *Post Office Protocol version 3* – protokół internetowy pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP.

[3] *Internet Message Access Protocol* – internetowy protokół pocztowy - następca POP3, pozwala na zarządzanie wieloma folderami pocztowymi oraz pobieranie i operowanie na listach znajdujących się na zdalnym serwerze.

i przesyła wiadomość do serwera adresata. Wiadomość jest przechowywana na serwerze pocztowym adresata do czasu, gdy adresat odbierze wiadomość po połączeniu się z serwerem pocztowym. Nadawca jest informowany o nieudanej próbie przesłania wiadomości oraz opcjonalnie o dostarczeniu lub odczytaniu wiadomości.

2. Zalety poczty rejestrowanej

Elektroniczna poczta rejestrowana – PReM[4] łączy w sobie szybkość poczty elektronicznej i bezpieczeństwo poczty rejestrowanej. W projekcie PReM zwrócono szczególną uwagę na silne procedury uwierzytelniania, wysoki poziom zapewnienia poufności i integralności wiadomości. Do zapewnienia pełnej ochrony przesyłanej informacji, począwszy od potwierdzenia nadania wiadomości aż do momentu jej doręczenia, wykorzystuje się narzędzia kryptograficzne. PReM zapewnia uwierzytelnienie wiadomości dla obu stron, tym samym adresat jest zabezpieczony przed wiadomościami z niepewnego, niezweryfikowanego źródła. Elektroniczną pocztę rejestrowaną definiują normy UPU[5] [1, 2] oraz specyfikacje ETSI[6] [3, 4, 5, 6, 7]. W niniejszym artykule opisano model przedstawiony w normie UPU S52-1 [2].

Usługa jest realizowana poprzez bezpieczne mechanizmy przesyłania wiadomości stosowane na każdym etapie realizacji usługi. Poszczególne etapy realizacji usługi są rejestrowane w logu i mogą służyć do potwierdzenia autentyczności wiadomości.

Usługa PReM zawiera następujące funkcje:

- **Bezpieczne wysyłanie i doręczanie wiadomości**: PReM zapewnia poufność przesyłanych wiadomości (poprzez szyfrowanie) oraz jej integralność (brak możliwości wprowadzenia zmian w wiadomości) oraz autentyczność i niezaprzeczalność użytkowników (nadawcy i adresata) oraz wyznaczonych operatorów (serwera operatora nadawcy

[4] *Postal Registered e-Mail* – Elektroniczna Poczta Rejestrowana
[5] *Universal Postal Union* – Międzynarodowa Unia Pocztowa
[6] *European Telecommunications Standards Institute* – Europejski Instytut Norm Telekomunikacyjnych

i serwera operatora adresata). Gwarantowane jest także bezpieczne przesyłanie wiadomości od nadawcy do adresata.

- **Rejestracja zdarzeń**: śledzone są wszystkie istotne zdarzenia w pełnym cyklu realizacji usługi.
- **Powiadamianie o zdarzeniu**: szczegółowa informacja o zdarzeniach i operacjach dotyczących realizacji usługi jest przesyłana do obu korespondujących stron,
- **Archiwizowanie rejestrowanych zdarzeń**: składowane są rekordy zdarzeń na potrzeby przyszłych działań.

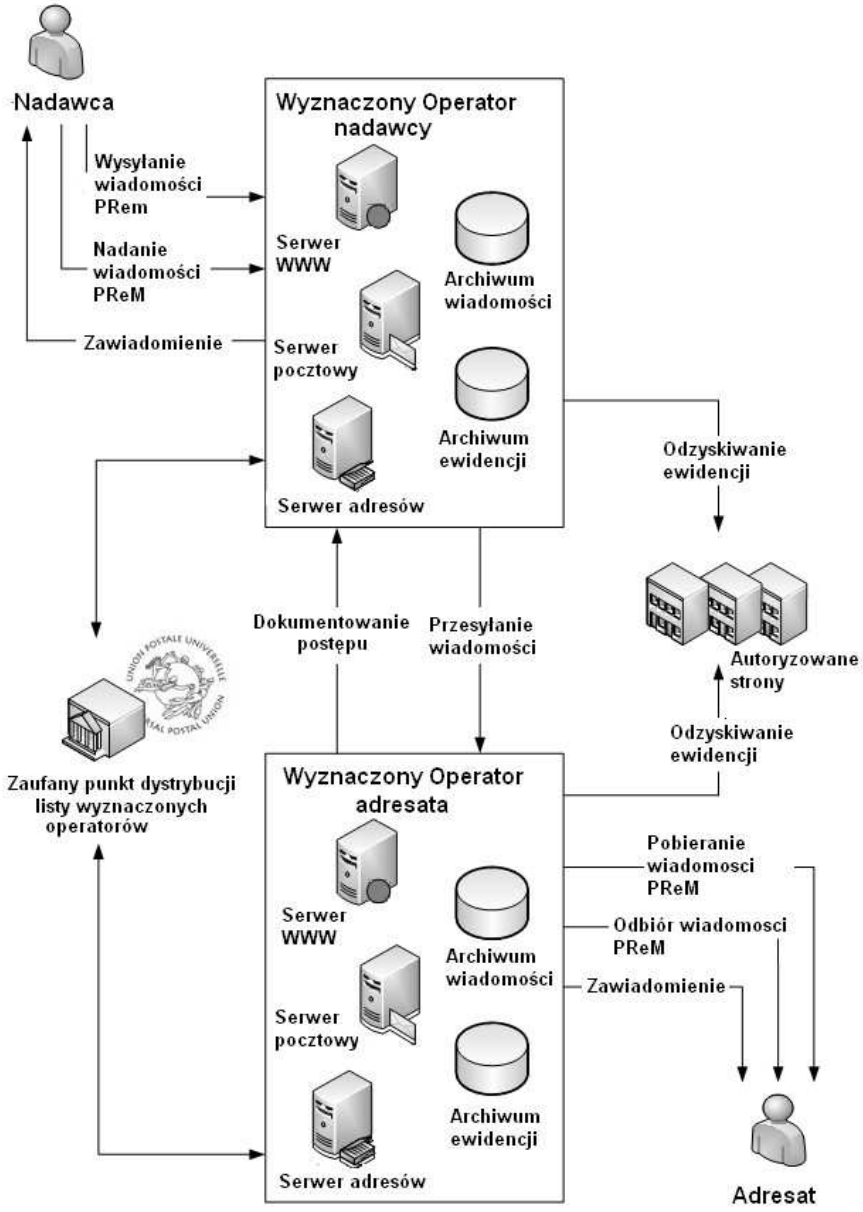
3. Architektura systemu

W modelu koncepcyjnym Systemu PReM (rys 2) pokazano nadawcę, adresata, autoryzowane strony, wyznaczonego operatora nadawcy wiadomości, wyznaczonego operatora adresata wiadomości, zaufany punkt dystrybucji listy wyznaczonych operatorów oraz podstawowe powiązania między nimi.

Model zakłada, że autoryzację operatorów wyznaczonych prowadzić będzie UPU, jako organizacja międzynarodowa o uznanym autorytecie. PReM zapewnia przekazywanie wiadomości nadawanych jedynie przez użytkowników zarejestrowanych u swoich wyznaczonych operatorów. Możliwe jest przy tym nadawanie wiadomości do adresatów poza systemem PReM, ale przy ograniczeniu funkcji kontrolnych nad jej przekazywaniem.

W przedstawionym modelu, wyznaczony operator nadawcy jest odpowiedzialny za przyjęcie wiadomości PReM od nadawcy, przekazanie jej do serwera adresata oraz za zarządzanie wiadomością. Jest także odpowiedzialny za zarządzanie własną domeną. Podobnie wyznaczony operator adresata jest odpowiedzialny za doręczenie wiadomości PReM do adresata i odpowiedzialny za zarządzanie przychodzącymi wiadomościami. Jest on także odpowiedzialny za zarządzanie własna domeną. Nadawca wiadomości PReM identyfikuje adresata po jego nazwie lub adresie. Kopia bazy adresowej znajduje się na serwerze adresów każdego operatora.

Zarówno wiadomości PReM jak i ewidencja przeprowadzonych operacji jest archiwizowana w bazach operatorów nadawcy i adresata. Rezerwowa kopia ewidencji jest przechowywana w bazie autoryzowanej organizacji niezależnej od operatora.



Rys 2. Model koncepcyjny rejestrowanej poczty elektronicznej
Źródło: UPU S52-1 [2].

System powinien zapewnić przesyłanie wiadomości zarówno w przypadku, gdy obaj korespondenci są obsługiwani przez tego samego

wyznaczonego operatora jak i przez różnych operatorów. Przyjmuje się, że korespondenci będą korzystać z powszechnie stosowanych aplikacji pocztowych takich jak Microsoft Outlook, Microsoft Outlook Express, Mozilla ThunderBird i inne, a także z opcji logowania do serwera pocztowego przez stronę WWW. Szyfrowanie połączenia z serwerem realizują dodatkowo instalowane wtyczki.

Format przesyłanych wiadomości jest zgodny ze specyfikacją [4, 5]. Norma także definiuje kody zdarzeń, wraz z poziomem ich ważności, określające poszczególne etapy i problemy rejestrowane w ewidencji podczas przesyłania wiadomości PReM.

4. Zarządzanie tożsamością i procedury identyfikacji

Zasadniczą cechą systemu PReM jest rejestracja zdarzeń dotyczących operacji przesyłania wiadomości. W celu udokumentowania nadania i doręczenia wiadomości niezbędna jest identyfikacja nadawcy i adresata. Wybór procedury identyfikacji użytkowników zależy od strategii bezpieczeństwa domeny. Procedury te zostały opisane poniżej.

- **Identyfikacja hasłem**. Standardowa identyfikacja przez login i hasło. Podwyższony poziom bezpieczeństwa zapewniają nam hasła jednorazowe, należy jednak zapewnić bezpieczną procedurę ich dostarczania.
- **Podpis elektroniczny z zastosowaniem elektronicznego certyfikatu.** Zarządzanie tożsamością dotyczy w tym przypadku nie tylko nadawcy i adresata, ale również wyznaczonych operatorów. Format i zasady certyfikacji powinny spełniać wymagania RFC 5280 [8] i Dyrektywy 1999/93/WE [9].
- **Kwalifikowany podpis elektroniczny z certyfikatem kwalifikowanym**. Procedura ta jest uważana za najwyższy poziom zarządzania tożsamością i uwierzytelniania, przewidziane dla PReM. Procedura identyfikacji powinna przebiegać zgodnie z RFC 3739 [10], ETSI TS 101 862 [11] i Dyrektywą 1999/93/WE [9].

Wybór stosowanych procedur identyfikacji jest w gestii wyznaczonego operatora. Należy jednak zauważyć, że będzie to miało znaczący wpływ na poziom zaufania do operatora.

Podsumowanie

Potrzeba stosowania poczty elektronicznej o podwyższonym poziomie bezpieczeństwa jest niepodważalna. Tego typu systemy stosowane są w bankach, administracji rządowej itp. Powinny być stosowane wszędzie tam, gdzie wymagana jest wysoka wiarygodność nadawcy wiadomości oraz wysoki poziom bezpieczeństwa przekazywanych wiadomości i dokumentów.

Opisane rozwiązanie rejestrowanej poczty elektronicznej jest dedykowane jako usługa dostępna na całym świecie. Wymaga to wprowadzenia procedur gwarantujących wiarygodność, i to na odpowiednim poziomie, poszczególnych użytkowników i operatorów świadczących tę usługę. Norma [2] definiuję tę usługę, jako usługę o wysokim poziomie zaufania, świadczoną przez operatorów pocztowych certyfikowanych i akredytowanych przez uznaną międzynarodową organizację pocztową.

Równoważną usługę definiuje specyfikacja ETSI [1, 4, 5, 6, 7]. Oba rozwiązania stosują ten sam format przesyłania wiadomości, a stosowane rozwiązania są podobne. Wydaje się, że będzie istnieć możliwość komunikacji pomiędzy użytkownikami obu systemów przy zachowaniu podwyższonego poziomu wiarygodności. Wdrożenie światowego systemu PReM będzie wymagało skoordynowania wielu działań organizacyjnych.

Literatura

1. UPU-S43 *“Secured electronic postal services (SePS) interface specification; Part A: Concepts, schemas and operations; Part B: EPCM Service”*
2. UPU: S52-1 *“Postal Services – Hybrid Mail - Functional Specification for postal registered electronic mail”*
3. ETSI TS 102 640-1: *"Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 1: Architecture"*.
4. ETSI TS 102 640-2: *"Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 2: Data Requirements and Formats for Signed. Evidences for REM"*.
5. ETSI TS 102 640-3. *“Technical Specification Electronic Signatures and Infrastructures (ESI);Registered Electronic Mail (REM);Architecture, Formats*

and Policies; Part 3: Information Security Policy Requirements for REM Management Domains"

6. ETSI TS 102 640-4 "*Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM);Part 4: REM-MD Conformance Profiles"*
7. ETSI TS 102 640-5 „*Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles"*.
8. RFC5280. "*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*." http://www.ietf.org/rfc/rfc5280.txt
9. Dyrektywa 1999/93/WE *Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego*
10. RFC3739. "*Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*." http://www.ietf.org/rfc/rfc3739.txt
11. ETSI TS 101862 *'Qualified certificate profile"*
12. Kobus R. *Systemy informatyczne i elektroniczne w nowoczesnych usługach pocztowych.* Uniwersytet Szczeciński. Zeszyty Naukowe NT 544. Ekonomiczne problemy usług nr 35. Rynki przesyłu i przetwarzania informacji – stan obecny i perspektywy rozwoju.Część I
13. Kobus R. *Narzędzia Regulatora do kontroli jakości usług pocztowych w warunkach zliberalizowanego rynku*. Uniwersytet Szczeciński. Zeszyty Naukowe NT 544. Ekonomiczne problemy usług nr 35. Rynki przesyłu i przetwarzania informacji – stan obecny i perspektywy rozwoju. Część II
14. Materiały CEN/TC331 Postal services i UPU.

ELECTRONIC POSTAL SERVICES

Sumary

This paper presents the registered e-mail worldwide. The system ensures a high level of security of messages sent with full tracking of sending events. The service is delivered only by selected, trusted operators, and can be sending only by a verified sender. The basis of the solution is standard UPU S52-1.

Translated by Ryszard Kobus