SECURITATEA APLICAȚIILOR MOBILE BANKING

Mihai Ciobanu
Universitatea Tehnică a Moldovei
mihai.ciobanu@vb.md

Abstract. *Mobile banking is attractive because it is a convenient approach to perform remote banking, but there are security shortfalls in the present mobile banking implementations. This paper discusses some of these security shortfalls, such as security problems with GSM network, SMS/GPRS protocols and security problems with current banks mobile banking solutions. The results from these proposed solutions have proven to provide secure and economic communications between the mobile application and the bank servers. The proposed solutions allow the users to bank using secure SMS and GPRS.*

Cuvinte cheie: *Mobile Banking, protocol SMS, protocol GPRS, securitate, fiabilitate, standardizare*

I. Introducere

În ultimii ani numărul utilizatorilor bancari online a crescut continuu. Aceasta a determinat ca tot mai mulți dezvoltatori de software să identifice cele mai eficiente metode de a efectua tranzacții bancare la distanță. Actualmente băncile furnizează aplicații mobile prin două canale principale:

- WAP (Wireless Application Protocol) prin intermediul GPRS (General Packet Radio Service) şi
- SMS (Short Message Service) prin intermediul WIG (Wireless Internet Gateway).

În acest articol se investighează aspectele de securitate în implementările de mobile banking ce utilizează rețeaua GSM.

1.1. Arhitectura de securitate GSM şi GPRS

Global System for Mobile Communications (GSM) este cel mai popular standard pentru telefoane mobile. Figura 1 prezintă structura de bază a unui sistem GSM; GSM furnizează servicii SMS şi GPRS (General Packet Radio Service).

Rețeaua GPRS Core este o parte integrantă a rețelei GSM. GPRS utilizează câteva din elementele existente ale rețelei GSM: Base Station Subsystems (BSS), Mobile Switching Centers (MSC), Authentication Centers (AUC) şi Home Location Registers (HLR). Dintre elementele rețelei GPRS adăugate peste rețeaua GSM menționăm: nodurile de suport GPRS (GSN), protocolul de tunelare GPRS (GTP), punctele de acces şi (Packet Data Protocol) PDP Context.

1.2 Mecanismele de securitate în rețeaua GSM

Rețeaua GSM are câteva mecanisme de securitate cu rolul bine definit de a preveni activitatea de clonare a cartelei SIM şi de a stopa operarea manuală a comenzilor. GSM este prevăzută cu metode de autentificare şi de criptare a datelor vehiculate în rețea.

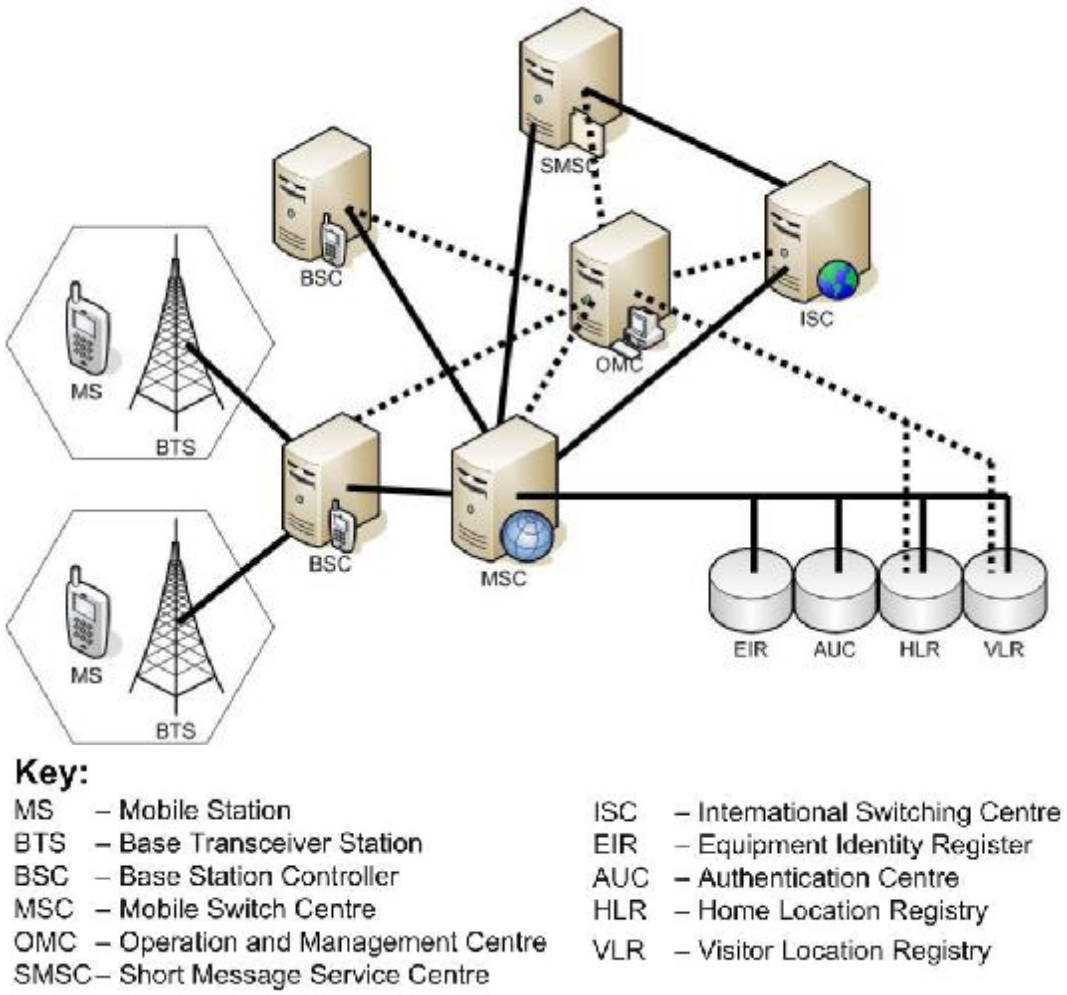

Fig. 1. Arhitectura GSM

1.2.1 Centrul de Autentificare GSM

Centrul de autentificare GSM este utilizat pentru a autentifica fiecare card SIM ce încearcă să se conecteze la rețeaua GSM. Autentificarea cartelei SIM are loc atunci cînd un dispozitiv mobil încearcă să se conecteze la rețea, adică atunci când un terminal este pornit. Dacă autentificarea eşuează, atunci nici un serviciu nu va fi oferit de rețeaua operatorului GSM, în caz contrar Nodul de Suport de Servicii GPRS (the Serving GPRS Support Node) SGSN şi HLR sunt specializate în managementul serviciilor asociate tipului concret de card SIM.

1.2.2 Procedura de autenticare

Autentificarea unui card SIM depinde de mecanismul de distribuire a cheilor secrete dintre cardul SIM şi AUC, denumit Ki. Această cheie secretă este introdusă în cardul SIM în procesul de personalizare a acestuia şi este de asemenea replicată securizat în AUC.

Când AUC autentifică un card SIM, se generează un număr aleator cunoscut ca RAND care este expediat către abonat. Ambele componente AUC şi SIM furnizează Ki şi valoarea RAND unui algoritm A3/A8 (sau algoritmului proprietar al operatorului GSM (COMP128)) iar un număr cunoscut ca Signed RESponse (SRES) este generat de către ambele părți. Dacă SIM SRES şi AUC SRES sunt aceleaşi, atunci cardul SIM este autentificat cu succes.

Ambele componente AUC şi SIM trebuie să calculeze o cheie secretă secundară denumită Kc prin transmiterea valorilor Ki şi RAND unui algoritm A5. Această cheie va fi folosită pentru criptarea şi decriptarea sesiunii de comunicare.

După autentificarea SIM, componentele SGSN sau HLR solicită identificarea dispozitivului mobil pentru a se asigura că stația mobilă nu este folosită de către un utilizator aflat in lista neagră. Statia mobilă furnizează codul IMEI (International Mobile Equipment Identity); acest număr este transmis către EIR (Equipment Identity Register). Codul EIR authorizează abonatul care recepționează prin SIM statutul său: dacă stația mobilă este autorizată, atunci SGSN informează HLR şi PDP Context că activarea a avut loc.

1.3. Wireless Application Protocol (WAP)

WAP este un standard deschis internațional pentru aplicații ce utilizează comunicațiile fără fir. Ca principală aplicație este capacitatea de a accesa sisteme prin intermediul Internetului de pe un telefon mobil sau PDA. Telefoanele mobile sau terminalele pot accesa Internetul utilizând navigatoare WAP;

Navigatoarele WAP pot accesa numai site-uri WAP. În loc de tradiționalele HTML, XML sau XHTML, site-urile WAP sunt scrise în WML (Wireless Markup Language). Protocolul WAP este persistent de la client către poarta WAP, conexiunea de la Poarta WAP la Serverul Bancar este securizată prin unul din protocoalele SSL sau TLS. Figura 2 ilustrează această arhitectură.

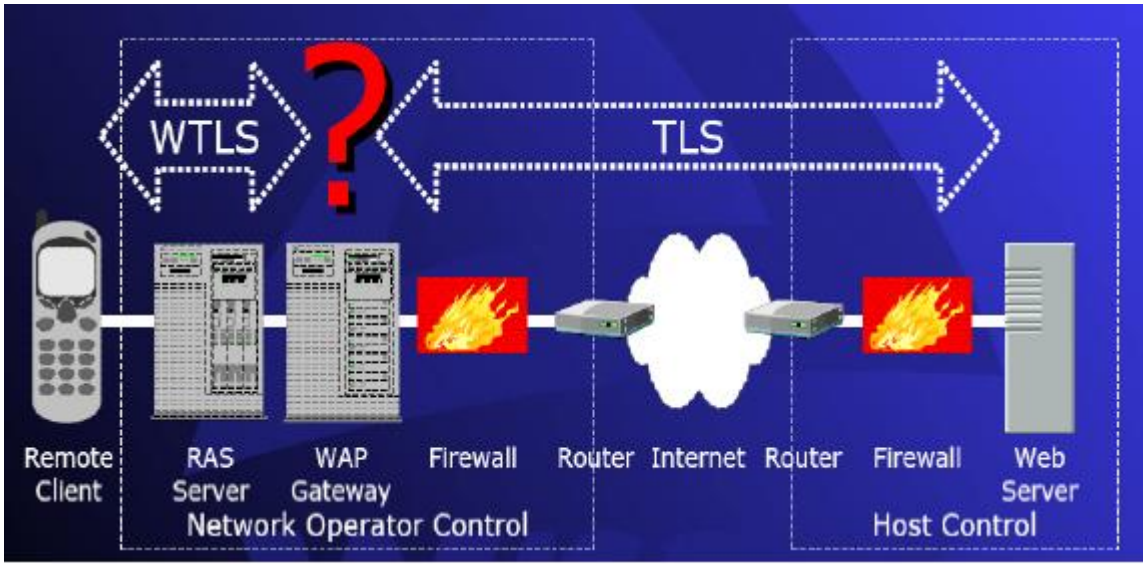

Fig. 2. Protocolul WAP în raport cu rețeaua externă

WAP este responsabil de securizarea comunicației utilizând protocolul WTLS (WAP Transport Layer Security) şi modulul WIM (WAP Identity Module). WTLS generează o cheie publică bazată pe un mecanism de securitate similar cu TLS şi WIM memorează cheile secrete. În scopul asigurării interoperabilității echipamentelor WAP cu programele specifice tehnologiilor diferitor dezvoltatori, WAP utilizează suita de protocoale WAP. Figura 3 ilustrează diferitele nivele ale protocolului WAP.

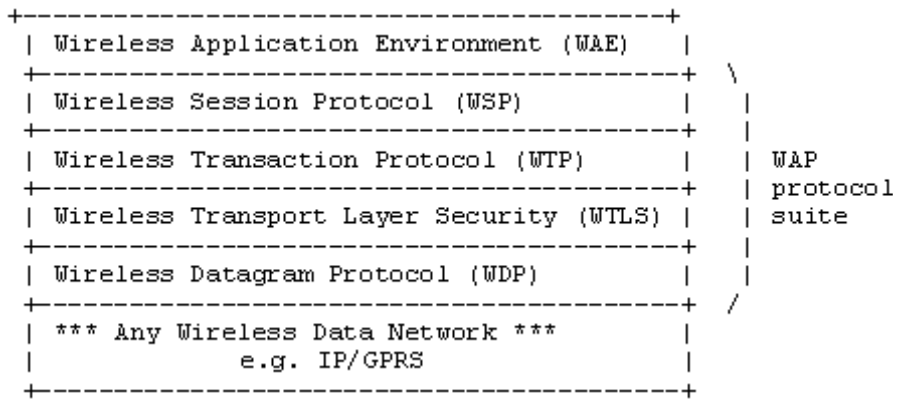

Fig. 3. Suita de protocoale WAP

1.4 Problemele de securitate în implementările GPRS curente

1.4.1 Aspecte de securitate legate de utilizarea protocolului WAP

Implementările bancare curente ce utilizează protocolul WAP s-au dovedit foarte sigure dar există câteva semne de întrebare ce pot pune la îndoială securitatea comunicațiilor.

În primul rând nu există o criptare cap la cap (end-to-end) între client şi serverul bancar. Există criptare end-to-end între client şi Gateway şi între Gateway şi Serverul Bancar. Pentru a rezolva acest aspect, serverul bancar ar trebui să aibe propriul Access Point Name (APN) în orice rețea GPRS. Acest APN va putea servi ca WAP Gateway pentru bancă. Prin urmare clientul se va putea conecta direct la bancă fără o a treia parte utilzând doar mijloacele de comunicații specifice.

Un alt aspect se referă la lungimile cheilor criptosistemului oferite de către standardul WTLS care nu sunt suficient de mari pentru a satisface cerințele actuale ale aplicațiilor de securitate WAP. Aceste chei au fost restricționate ca lungime din cauza puterii de procesare scazute ale dispozitivelor mobile.

Suita de schimburi de chei anonime oferită de către negocierea WTLS nu sunt considerate securizate. Banciile trebuie să furnizeze funcționalități care să nu permită optiunea de negociere.

1.4.2 Aspecte de securitate derivate din utilizarea rețelei GPRS

Rețeaua GPRS Core este prea generală şi nu este orientată către cerințele bancare de securitate: lipsa contului deținătorului de card SIM sau a autentificării bancare. Banca poate furniza un cod unic APN pentru accesul Serverului Bancar, dar fără aceasta sau a altui mecanism de autentificare, oricine poate fura identitatea altcuiva față de Bancă.

II. Soluții SMS de securitate

Solutia propusă se referă la protocolul de securizare a mesajului SMS integrat în sistemul de mobile banking pentru creşterea securității serviciului SMS banking.

Pentru exemplificare au fost simulate trei tipuri de tranzacții în acest articol. Aceste tranzacții sunt cele mai populare şi se referă la: verificarea soldului din cont, transferul de bani şi încărcarea contului.

2.1 Protocolul de securitate SMS

2.1.1 Structura Mesajului

Mesajul securizat SMS este divizat în câmpuri multiple pentru a fi acomodat diferitor cerințe de securitate ale protocolului. Figura 4 ilustrează structura unui mesaj SMS securizat. Numerele de

deasupra câmpurilor reprezintă numărul minim de bytes necesari. Numărul de bytes a fiecărui câmp poate fi crescut în funcție de cerințele de implementare.

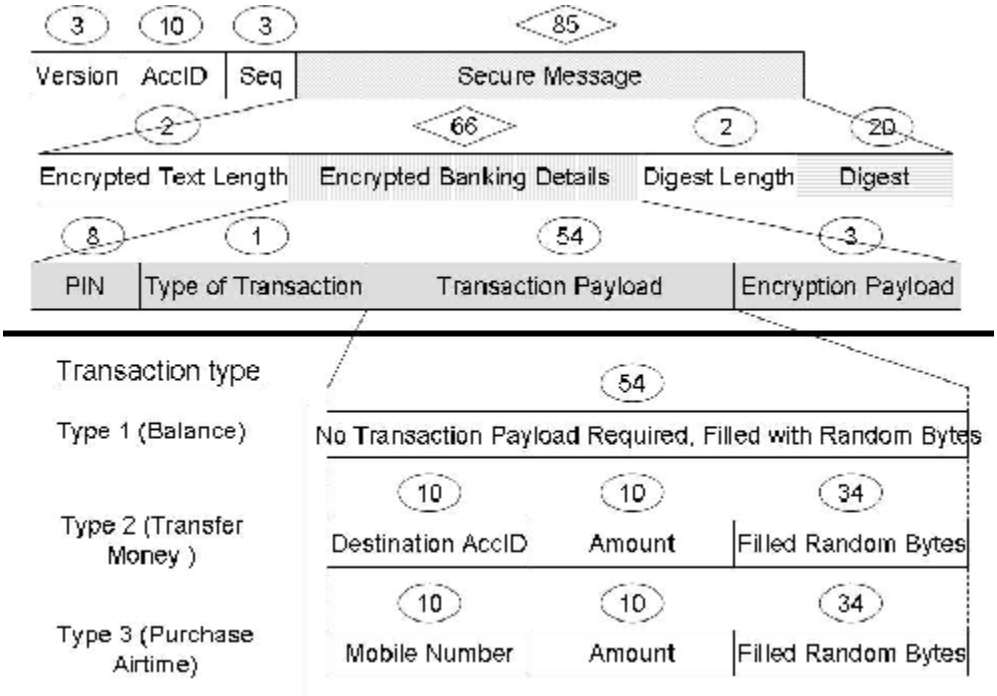

Fig. 4. Structura unui mesaj SMS securizat

Utilizarea fiecărui câmp este explicată mai jos:

Version reprezintă numărul versiunii aplicației mobile. Beneficiarul trebuie să verifice dacă primii trei bytes ale mesajului SMS recepționat sunt valizi pentru aplicația bancară. Acest număr este foarte important pentru eliminarea nesajelor eronate.

AccID contine identificatorul bancar al contului utilizatorului.

Seq este numărul secvential curent al utilizatorului pentru parola de o singură dată (one-time password).

Encrypted Text Length conține numărul următorilor bytes reprezentați de mesajul cifrat.

Digest Length conține numărul următorilor bytes conținuți în rezumatul mesajului.

Digest conține valoarea calculată a rezumatului mesajului şi este utilizată de server pentru calcularea integrității mesajului. În cadrul protocolului bancar SMS securizat se calculează rezumatul unic al următoarelor câmpuri: *Version*, *AccID*, *Seq*, *PIN*, *Type of Transaction* and *Transaction Payload*.

Conținutul următoarelor câmpuri este criptat utilizând cheile de sesiune generate.

PIN conține parola predefinită a utilizatorului care este utilizată de către beneficiarul aplicației în autentificarea utilizatorului.

Type of Transaction este utilizată de către aplicația de pe serverul bancar pentru a identifica tipul tranzacției ce urmează a fi efectuată.

Transaction Payload este o data neordinară utilizată de catre o tranzacție şi care nu are nici o justificare de securitate.

2.1.2 Protocol Sequences

În rețelele GSM mesajele SMS sunt expediate asincron către beneficiari, motiv pentru care protocolul de securitate SMS este asincron. Figura 5 prezintă desfăşurarea acțiunilor protocolului securizat SMS.

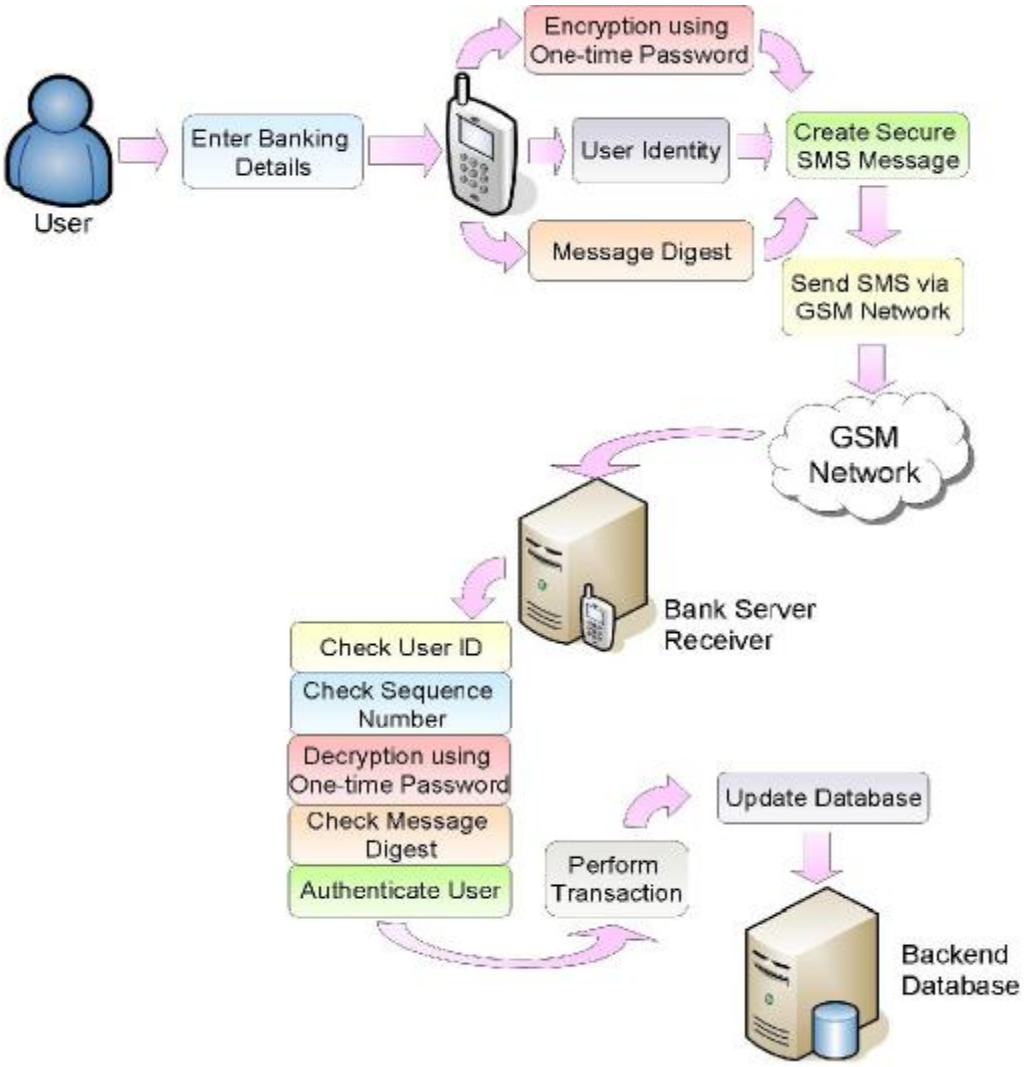

Fig. 5. Descrierea protocoluluii

Putem considera ca protocolul securizat SMS poate fi divizat în două părți. În prima parte are loc generarea mesajului. Telefonul mobil generează mesajul şi îl expediază către server. În a doua parte are loc verificarea securității mesajului. Serverul citeşte mesajul recepționat, decodează conținutul şi efectuează verificările de securitate.

2.2. Soluții de securizare GPRS

Pentru a acorda băncii controlul deplin asupra protocolului WTLS, această soluție permite clienților băncii să se conecteze la rețeaua lor bancară prin intermediul unui gateway WAP personalizat care nu permite următoarele opțiuni considerate suspecte: negociere abreviată, server autentificat prin negociere deplină si suite de schimb de chei anonime.

Figura 6 redă locația ideală a unui gateway WAP pentru mobile banking.

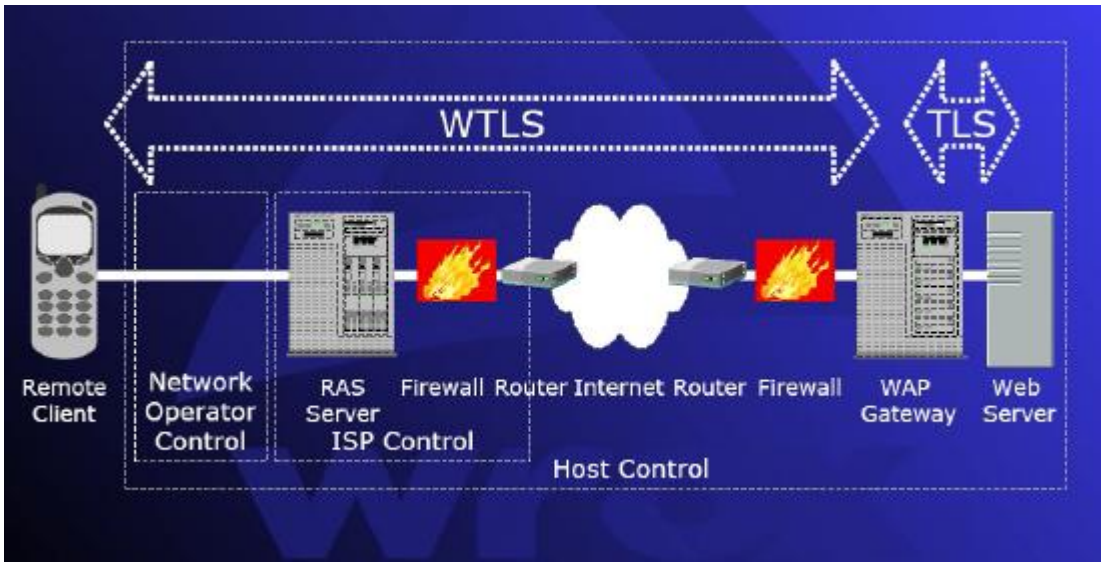

Fig. 2. Setarea ideală pentru Gateway WAP al unui server bancar

III. Concluzii

Dorința de a utiliza sisteme deschise, sigure şi fără o multitudine de proceduri de autentificare „single sign-on", forțează adoptarea unor sisteme securizate pentru managementul identității. Integrarea tehnologiilor smart card în astfel de abordări, asigură creşterea gradului de securitate şi fiabilitate în sistemele pentru managementul identității.

IV. Referințe

1. Camelia Lungu, Plățile mobile la răspântie, iulie 2007, http://www.comunic.ro
2. http://europa.nvc.cs.vt.edu/~ctlu/Publication/M-Payment-Solutions.pdf
3. www.hec.unil.ch/yp/Pub/03-ICEIS.PDF
4. J. Markendahl, P. Andersson, "Analysis of ecosystem for mobile ticketing and payment services and implications for NFC based mobile services", in Proceedings of 8th Biennial and Silver Anniversary ITS Conference, Tokyo, Iunie 2010.
5. M. Smith, J. Markendahl, P. Andersson, "Analysis of roles and position of mobile network operators in mobile payment infrastructure", in Proceedings of 21st European Regional ITS Conference, Copenhagen, 13-15 Septembrie 2010
6. D. Katsianis et al., "The financial perspective of the mobile networks in Europe", IEEE Personal Communications Magazine, Vol. 8, No. 6, pp 58-64, Decembrie 2001.