(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 133582 A0**
(51) Int.Cl.
G06F 21/31 (2013.01);
H04W 12/06 (2009.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2018 00818**

(22) Data de depozit: **19/10/2018**

(41) Data publicării cererii:
30/08/2019 BOPI nr. **8/2019**

(71) Solicitant:
• **ONLINE SERVICES S.R.L.**, *STR. UNIRII BL. C1 AP. 29, BUZĂU, BZ, RO*

(72) Inventatori:
• **LUPU VIOREL**, *STR.UNIRII, BL.C8, AP.4, BUZĂU, BZ, RO*

(74) Mandatar:
CABINET DE PROPRIETATE INDUSTRIALĂ "LAZĂR ELENA",
B-DUL UNIRII, BL. 16C, AP. 12, OP 1, CP 52, BUZĂU, JUDEŢUL BUZĂU

(54) # METODĂ ŞI ARHITECTURĂ PENTRU ACORDAREA ACCESULUI AUTORIZAT LA O PLATFORMĂ DE SERVICII INTERNET

(57) **Rezumat:**

Invenţia se referă la o arhitectură şi la o metodă pentru acordarea accesului autorizat la o platformă de servicii Internet. Arhitectura conform invenţiei cuprinde un terminal (**T**) telefonic conectat la un sistem de telefonie (**Telco**) incluzând comunicaţii de telefonie mobilă şi fixă, un dispozitiv (**DS**) de securitate integrabil într-un set de căşti (**CA**) audio, destinat conversiei şi decriptării de semnale, un terminal (**Di**) de utilizator, ca un computer, ce poate exploata servicii de Internet şi este iniţiatorul cererii de autorizare a accesului, un server (**Da**) al platformei de servicii electronice căruia îi sunt transmise cererile de autorizare a accesului, un dispozitiv (**Dc**) de comunicaţie conectat la reţeaua privată a platformei şi la sistemul de telefonie (**Telco**). Metoda conform invenţiei constă în solicitarea autorizării la o platformă de servicii internet, iniţiată de un utilizator (**U**), prin intermediul terminalului (**Di**) utilizatorului ce transmite un mesaj către server (**Da**), mesajul conţinând un identificator al utilizatorului, verificarea utilizatorului de către server (**Da**), prin verificarea identificatorului utilizatorului în baza de date locală şi, dacă utilizatorul este cunoscut, generarea unei parole de unică utilizare, transformarea acesteia într-un set de pointeri ce desemnează sunete, respectiv, imagini corelate cu sunetele, şi transmiterea setului de pointeri la terminalul (**Di**) ce a iniţiat cererea de autorizare, şi la un dispozitiv (**Dc**) de comunicaţie ce asigură legătura cu terminalul (**T**) telefonic, în care dispozitivul (**Dc**) transformă setul de pointeri într-un sunet indescifrabil pentru urechea umană, sau într-un pachet de date criptat ce este transmis terminalului (**T**) telefonic şi, prin acesta, dispozitivului (**DS**) de securitate din căştile (**CA**)audio ce decriptează sunetul sau semnalul, şi afişează parola decriptată, sau produce sunetele necesare utilizatorului pentru identificarea parolei grafice şi, respectiv, a celei de acces.

Revendicări: 8
Figuri: 3

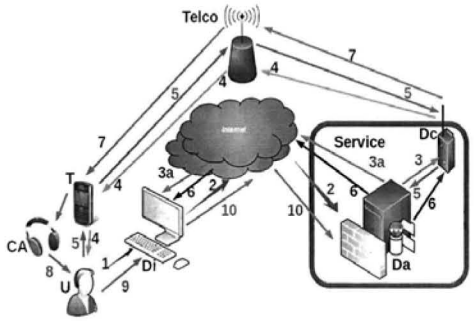


Fig. 1

RO 133582 A0

Metodă si arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet

Prezenta descriere de invenție se referă la un ansamblu constructiv și o metodă privind acordarea accesului autorizat la o platformă de servicii Internet care asigură protecția datelor personale și a bazelor de date exploatate de la distanță.

Ca stadiu cunoscut al tehnicii au fost identificate câteva soluții apropiate; astfel se cunosc:

US 6078908 Method for authorizing in data transmission systems

Patentul US 6078908 descrie un ansamblu și o procedură axată pe procesare text, în particular numere de tranzacție pe care utilizatorul le citește și le tastează în interacțiune cu computerul terminal. Nu sunt referințe despre validitatea în timp a mesajelor. Sunt identificate următoarele dezavantaje:

- Procedura este inițiată de către utilizator prin manevrarea tastaturii terminalului
- Sistemul nu poate fi exploatat de persoane cu dizabilități fără ajutor uman suplimentar
- Mesajele pot fi retransmise electronic (automat prin mijlocirea unor programe) într-o fereastră de timp necontrolabilă de către sistem astfel încât face posibilă exploatarea sistemului de către o altă persoană aflată la distanță. Riscul de securitate este redus, dar garanția prezenței utilizatorului în fața terminalului nu poate fi asigurată.

US 20070107050A1 Simple two-factor authentication

Patentul US 20070107050A1 descrie o procedură simplă realizată prin procesarea de coduri alfanumerice text, coduri pe care utilizatorul le citește de pe ecranul dispozitivul WAP/WML și le introduce în computer utilizând tastatura. Nu sunt referințe despre validitatea în timp a mesajelor. Sunt identificate următoarele dezavantaje:

- Procedura este inițiată de către utilizator prin manevrarea tastaturii terminalului
- Sistemul nu poate fi exploatat de persoane cu dizabilități fără ajutor uman suplimentar
- Mesajele pot fi retransmise electronic (automat prin mijlocirea unor programe) într-o fereastră de timp necontrolabilă de către sistem astfel încât face posibilă exploatarea sistemului de către o altă persoană aflată la distanță. Riscul de securitate este mai mic, dar garanția prezenței utilizatorului în fața terminalului nu poate fi asigurată.

US8917826B2 Detecting man-in-the-middle attacks in electronic transactions using prompts

Patentul US 8917826B2 descrie un sistem şi o metodă pentru eliminarea riscului de securitate "man in the middle". Sistemul conform patentului conţine un subsistem telefonic vocal interactiv IVR. Utilizatorul iniţiază procedura la terminal după care validează codul de acces în interacţiune cu sistemul IVR prin tastele telefonului. Sunt identificate următoarele dezavantaje:

- Procedura este iniţiată de către utilizator prin manevrarea tastaturii terminalului şi a tastaturii sistemului telefonic.
- Sistemul nu poate fi exploatat de persoane cu dizabilităţi fără ajutor uman suplimentar
- Sistemul rezultate este complex utilizând servicii telefonice interactive voce IVR.
- Este posibil cel puţin un scenariu în care utilizatorul care interacţionează cu sistemul telefonic nu se află în faţa computerului care afişează codul de acces.

Problema tehnică pe care o rezolvă invenţia este realizarea unei arhitecturi constructive care permite printr-o metoda, autorizarea accesului şi a persoanelor, chiar si a persoanelor cu dizabilităţi precum: capacitate de memorare redusă, deficienţe motorii, respectiv incapacitatea de a utiliza tastaturi, deficienţe de vedere cu incapacitatea de a utiliza tastaturi, deficienţe de coordonare etc., la servicii de internet care asigura protectia datelor si a bazelor de date, exploatate de la distanta.

Astfel se verifică prezenţa persoanei desemnate prin interacţiunea cu apelul telefonic şi terminalul Internet în timp real prin confirmarea numărului de telefon, deţinerea dispozitivului audio inteligent simultan cu interacţiunea la terminalul Internet, persoana care solicită autorizarea cunoaşte semnificaţia sunetelor, interpretează corect semnificaţia lor şi acţionează în timp util asupra imaginilor afişate la terminalul internet, urmare a metodei de autentificare.

Terminalul recepţionează un apel telefonic, informaţia despre apel poate ajunge la unitatea centrală prin interfaţa cu terminalul telefonic. De exemplu dacă telefonul este un telefon mobil smartphone şi interfaţa este conectată cu telefonul prin bluetooth. CallerID poate fi transmis către unitatea centrala cu scopul identificării apelului veritabil de la serverul de autentificare preînregistrat în memorie, unitatea centrală poate comanda terminalului mobil (inteligent) să accepte apelul telefonic automat dacă de exemplu chemătorul este recunoscut ca server de autentificare conform metodei.

În cazul telefoniei analogice apelul va fi recunoscut de către utilizator, prin canalul audio stabilit prin conexiunea telefonică, serverul de autentificare transmite codurile audio care prin interfaţa sunt preluate de decodificator şi transmise unităţii centrale pentru decriptare. Serverul de autentificare poate transmite un şir de coduri DTMF care sunt recunoscute de decodificator şi recepţionate de unitatea centrală, sirul codurile recepţionate de unitatea centrală sunt decriptate, verificată integritatea, validată regula de formare, pentru a fi transformate în pointeri care desemnează sunete inteligibile uman echivalente, unitatea centrală va citi din memorie fişierele

corespunzătoare pointerilor identificați și va produce prin convertorul numeric analog DAC și interfața audio sunetele care sunt ascultate de către utilizator în casca audio, Utilizatorul va acționa asupra interfeței de autentificare conform sunetelor reproduse.

Terminalul telefonic poate fi decuplat de la Internet si metoda este compatibila cu telefonia fixă, pe fir, analogică dar și cu tehnologiile telefonice de tip VoIP securizate, un dispozitiv de securitate este imun la pierderea terminalului telefonic, redirectarea apelului telefonic sau clonarea cardului SIM al telefonului mobil. impune prezența simultană a utilizatorului în fața terminalului internet, la terminalul telefonic și să dețină dispozitivul audio inteligent descris. Metoda restrânge timpul de acțiune al utilizatorului astfel încât face imposibilă prezența unui intermediar și a breșelor de securitate Man-In-The-Middle.

Utilizatorul apropie cardul, primește apelul, alege imagini, procesul se desfășoară doar pe durata apelului telefonic, este posibil utilizarea de către persoane cu dizabilități cum sunt cele cu capacitate de memorare redusă, cu deficiențe motorii , respectiv incapacitatea de a utiliza tastaturi, cu deficiențe de vedere , incapacitatea de a utiliza ecrane, deficiențe de coordonare, se utilizeaza tehnologi avansate care pot transmite automat identificatorul utilizatorului.

Securitatea sporită este asigurata si de adăugarea factorului limba în forma vocală, configurabil pentru utilizatorul desemnat, prin posibilitatea utilizării indicațiilor vocale indirecte, a căror semnificație este cunoscută de un grup restrâns de utilizatori, prin posibilitatea adăugării unor imagini capcană sau sunete capcană a căror semnificație este cunoscută numai de către utilizatorii legitimi. Utilizatorii legitimi știu că imaginea jokerului nu va fi niciodată selectată chiar dacă este indicată vocal. Selectarea acestei imagini va determina anularea cererii de autentificare întotdeauna, prin aceea că pachetul de date care conține parola de unică utilizare criptată poate fi recepționată în timpul apelului prin canale de date alternative, prin posibilitatea de a compara datele după decriptare, recepționate de dispozitivul audio DA cu datele transmise de serviciul „Service" pentru autentificarea utilizatorului prin algoritmi avansați de criptare cu parametrii care pot cuprinde aria geografică în care este permisă decriptarea, numele rețelei curente a serviciului de date și voce GSM, oricare neconcordanță blochează la nivelul dispozitivului audio DA procesul de autentificare.

Sistemul este deschis pentru creșterea siguranței prin utilizarea unor dispozitive terminale noi cu facilități de siguranță sporite cum sunt telefoanele inteligente, tabletele sau computerele personale cu posibilitatea ștergerii tuturor datelor și aplicațiilor utilizatorului terminalului în cazul furtului sau abuzului, autentificare biometrică – amprentă tactilă, iris, facială, vocală, pentru creșterea gradului de confort al utilizatorului prin utilizarea sistemelor terminale care permit accesarea serviciilor internet prin comandă vocală, gesturi sau dispozitive auxiliare

Dispozitivul de securitate este integrabil, complet în casca audio, camuflabil complet, poate fi montat pe cablul telefonic pentru a recepționa eventual CallerID și a prelua semnalele audio direct din circuitul telefonic, este compatibil cu sistemele

Internet de tip VoIP, respectiv circuitul telefonic poate fi complet virtual, sistemul este în cască, funcționarea lui este complet automată, este integrabil si în dispozitive de tip cheie de securitate USB, conectabil la computer pentru integrarea cu alte sisteme de securitate.

Dispozitivul de securitate este compus si interconectat astfel: interfața cu terminalul telefonic , unitate centrală de calcul, decodificator analog-digital, convertor numeric-analog (DAC) audio, unitate de memorie, terminal telefonic, casca audio standard, difuzor, optional computer, Internet.

Avantajele inventiei sunt :

1. Protecția accesului internet la servicii web / web site applications particularizat pentru persoane chiar si cu diferite dizabilități sau vârstnice
2. Acces autorizat la contul bancar – internet banking
3. Domenii în care confidențialitatea datelor este importantă – de exemplu domeniile securitate personală, medical, asigurări etc.
4. Autorizarea accesului la registre private
5. Autorizarea accesului la registre fiscale etc.
6. Acționări autorizate la distanță;
7. Smart-home, accesul autorizat la sistemele de automatizare și monitorizare casnice;
8. Acordarea accesului diferențiat în spații protejate
9. Aplicații militare unde este necesară verificarea strictă a utilizatorului
10. Sistem alternativ pentru carduri de sanatate.
11. Accesul autorizat la cazier.
12. Acordarea serviciilor integrate.
13. Metoda este simpla si are prevazute o multitudine de sisteme de securitate imune la pierderea terminalului telefonic, redirectarea apelului telefonic sau clonarea cardului SIM al telefonului mobil.
14. Metoda restrânge timpul de acțiune al utilizatorului astfel încât face imposibilă prezența unui intermediar și a breșelor de securitate Man-In-The-Middle.
15. Securitate este sporită prin adăugarea factorului limbă în forma vocală, configurabil pentru utilizatorul desemnat. De exemplu utilizatorul dorește ca limba în care îi sunt indicate imaginile pentru formarea parolei să fie latina veche.
16. Securitate este sporită si prin posibilitatea utilizării indicațiilor vocale indirecte, a căror semnificație este cunoscută de un grup restrâns de utilizatori. De

exemplu sunetul pronunțat este "miroase bine" iar singura imagine care corespunde criteriului este *floare*.

17. Securitate este sporită si prin posibilitatea adăugării unor imagini capcană sau sunete capcană a căror semnificație este cunoscută numai de către utilizatorii legitimi. De exemplu utilizatorii legitimi știu că imaginea jokerului nu va fi niciodată selectată chiar dacă este indicată vocal. Selectarea acestei imagini va determina anularea cererii de autentificare întotdeauna.

Se dă în continuare un exemplu de realizare al invenției în legătură cu figurile 1-6, care reprezintă:

fig. 1 – ansamblu constructiv

fig. 2 – diagrama metodei

fig. 3 – etapa 1 metodă imagine afișaj -1

fig. 4 – etapa II metodă imagine afișaj - 2

fig. 5 – etapa III metodă afișaj – 3

fig.6 – schema dispozitiv de securitate.

Invenția conform propunerii cuprinde servicii internet, baze de date și servicii de telecomunicații mobile vocale cu scopul de a simplifica efortul utilizatorilor și de a permite validarea identității utilizatorilor în timp real inclusiv al utilizatorilor cu anumite dizabilități.

Descrierea figurii 1, 6 – ansamblu functional si a figurii 2 – diagrama metoda.

U – Utilizator al serviciilor (Service) prin internet și abonat al unui serviciu de telefonie (mobilă GSM sau fixă). Utilizatorul poate fi o persoană cu deficiențe sau cu capacitatea redusă de vedere (persoană cu vârstă înaintată) sau cu memorie redusă. Utilizatorul poate fi în egală măsură o persoană normală care dorește acces sigur și rapid fără memorarea unor parole lungi, complexe care sunt schimbate relativ des așa cum recomandă practicile curente de securitatea IT. Utilizatorul are preînregistrate în sistem (Service) datele personale și numărul de telefon încă de la abonarea la serviciile platformei. Cu ocazia abonării la serviciu poate primi și cardul de acces, de exemplu în tehnologie NFC.

T – Terminal telefonic vocal cu funcția de monitor. Terminalul telefonic este conectat și accesibil prin sistemul telefonic (telefonie fixă sau mobil GSM sau alte sisteme de telefonie, de exemplu Internet). Terminalul telefonic (M) poate oferi sisteme de protecție suplimentară cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, prin sau gesturi.

Telco – Sistemul de telefonie internațional care include comunicația telefonică mobilă și fixă inclusiv comunicațiile telefonice prin Internet (VoIP – voice over IP).

CA – Terminal inteligent audio pentru conversia și decriptarea semnalelor recepționate de terminalul telefonic și transmiterea lor utilizatorului.

Di – Terminal internet (computer, tabletă, telefon mobil inteligent, e-reader etc.) care poate exploata serviciile internet ale platformei Service. Terminalul internet are funcția de inițiator al cererii de autorizare acces. Terminalul internet (Di) poate oferi sisteme de protecție suplimentare pentru accesul utilizatorilor (U) cum sunt cele implementate în sistemele Android, Windows sau IOS, respectiv autentificare biometrică, cu parolă, pin sau gesturi. Terminalul internet (Di) poate avea în configurație subsisteme pentru citirea automată a cardurilor, recunoașterea imaginii codurilor QR, recunoaștere vocală, etc.

Da - Server internet al platformei de servicii electronice Service căruia îi sunt transmise cererile de autorizare acces. Serverul de autorizare are acces prin rețeaua protejată privată a platformei la servicii de baze de date, dispozitive de comunicație etc. Rețeaua privată a platformei este protejată prin servere de securitate numite în literatura de specialitate și zid de protecție sau firewall.

Dc – Dispozitiv de comunicație conectat la rețeaua privată a platformei și la serviciul telefonic (GSM mobil sau rețeaua de telefonie fixă). Dispozitivului de comunicație Dc implementează tehnologia modemului voce.

Săgețile numerotate reprezintă interacțiunile dintre componentele sistemului în ordinea apariției evenimentelor astfel:

Utilizatorul (U) inițiază (1) procedura de solicitare a autorizării prin manevrarea dispozitivului (Di) prin care solicită autorizarea, astfel încât dispozitivul (Di) să determine identificatorul electronic unic al utilizatorului. Identificarea se poate realiza prin metode alternative cum sunt amprenta sau vocea etc., sau prin citirea automată (de către Di) a unui dispozitiv (NFC, RFiD, QR, audio) capabil să comunice identificatorul electronic al utilizatorului (U). În situații excepționale, utilizatorul poate iniția procedura prin tastarea numelui de utilizator și a unei parole.

Dispozitivul (Di) care solicită autorizarea transmite (2) un mesaj către dispozitivul care autorizează (Da) care conține identificatorul utilizatorului în baza de date locală. Transmisia este realizată prin canalul de comunicație (internet) prin care se va desfășura ulterior exploatarea serviciilor solicitate de utilizator (U).

Dispozitivul care autorizează (Da) verifică identificatorul utilizatorului în baza de date (locală). În cazul unui identificator necunoscut, transmite dispozitivului (Di) refuzul autorizării și procedura se încheie. În cazul în care identificatorul utilizatorului este cunoscut, serverul (Da) generează automat și aleatoriu o parolă de unică utilizare pe care o transformă într-un set de pointeri care desemnează sunete, respectiv imagini (corelate cu sunetele ce urmează a fi generate). Setul de pointeri este transmis simultan atât dispozitivului care a inițiat cererea de autorizare (Di) cât și unui dispozitiv de comunicație (Dc) care asigură legătura cu utilizatorul prin terminalul telefonic (T). Starea este reprezentată în Fig.1 prin 3 și 3a.

Dispozitivul de comunicație (Dc) la recepția setului de pointeri (3) va iniția un apel voce (4) către numărul telefonului (T) asociat în baza de date locală cu numele utilizatorului. Sistemul de telefonie (Telco) va informa (5) dispozitivul de comunicație (Dc), respectiv dispozitivul care acordă autorizarea (Dc) despre starea rețelei și starea apelului. Evenimentele detectate de dispozitivul de comunicații (Dc) pot fi linie telefonică ocupată, apel rejectat, răspuns la apel, lipsă răspuns la apel, număr inexistent, etc.

Dispozitivul care a inițiat cererea de autorizare (Di) pe baza setului de pointeri recepționat (3a) va pregăti pentru afișare un set de imagini corespunzător. Acest set de imagini conține imagini alese aleatoriu completate cu imaginile desemnate de pointerii primiți de la dispozitivul care acordă autorizarea (Da). Portofoliul de imagini care formează baza alegerii în dispozitivul care inițiază cererea de autorizare (Di) pot fi stocate local sau recepționate dinamic de la platforma care furnizează serviciile (Service).

Dispozitivul care autorizează (Da) este informat de rețeaua telefonică (Telco) prin dispozitivul de comunicații (Dc) de starea apelului (5). În situația în care apelul eșuează (rețea congestionată, lipsă semnal, apel respins etc.), dispozitivul care autorizează (Da) închide procedura prin refuzul autorizării și informează dispozitivul care a inițiat cererea (Di), respectiv utilizatorul (U) despre refuz. În situația în care utilizatorul (U) răspunde la apel prin terminalul telefonic (T) evenimentul este preluat (5) de rețeaua telefonică (Telco) prin dispozitivul de comunicații (Dc) respectiv de dispozitivul care autorizează (Da). Dispozitivul care autorizează (Da) informează (6) dispozitivul care a inițiat cererea (Di) pentru a afișa setul de imagini pregătit. Simultan, prin acțiunea 6, dispozitivul de comunicații (Dc) este informat asupra faptului că sistemul poate transmite (criptată) parola utilizatorului.

Dispozitivul de comunicație (Dc) transformă setul de pointeri primit de la dispozitivul care autorizează (Da) într-un sunet indescifrabil pentru urechea umană (sau un pachet de date criptat) care este transmis (7) terminalului telefonic (T) și prin acesta dispozitivului audio inteligent (CA) în timpul apelului. Dispozitivul audio inteligent (CA) decriptează semnalul audio recepționat telefonic (7) sau decriptează pachetul de date recepționat din sursa alternativă. Imediat ce procesul de decriptare a fost încheiat, dispozitivul audio inteligent (CA) va afișa parola decriptată (dacă deține un afișaj) sau va produce sunetele necesare pentru identificarea parolei grafice (8).

Utilizatorul (U) urmare a faptului că a răspuns apelului vocal, aude în dispozitivul audio (CA) desemnarea imaginilor (8) și selectează între imaginile afișate de către dispozitivul prin care a solicitat cererea de autorizare (Di) acele imagini desemnate (9). Acțiunile utilizatorului (9) asupra imaginilor afișate sunt transmise în timp real (10) către serverul (Da) pentru a fi asamblată parola.

În situația în care utilizatorul (U) nu deține terminalul telefonic (T) cu numărul de telefon înregistrat în baza de date a serviciului, la apel va răspunde o persoană care nu cunoaște rostul apelului pentru că nu ea a inițiat cererea de autorizare, iar pe de altă parte va auzi un sunet a cărui utilitate nu o cunoaște și care poate fi tradus în

informație utilă doar de dispozitivul audio (CA). Astfel apelul va fi închis și va determina respingerea autorizării.

Acțiunile (9) utilizatorului (U) determinate de apelul vocal în desfășurare sunt preluate de dispozitivul care solicită autorizarea (Di) generând un set de pointeri echivalenți care sunt transmiși în timp real (10) serverului (Da). Dacă setul de pointeri generat de acțiunile utilizatorului (10) este identic cu setul generat pe baza parolei de unică utilizare (3), autorizarea poate fi acordată de către dispozitivului (Da). În toate celelalte situații cererea de autorizare este respinsă.

Dispozitivul care autorizează (Da) verifică (11) dacă acțiunile utilizatorului (U) sau desfășurat în timpul dictării instrucțiunilor prin dispozitivul de comunicație (Dc), terminalul telefonic (T) și respectiv dispozitivul audio (CA). Dacă aceste condiții sunt respectate, autorizarea este acordată și transmisă dispozitivului care a solicitat autorizarea (Di) pentru a continua sesiunea solicitată de utilizator (U).

Dispozitivul de securitate (DS) este compus si interconectat astfel

1 = interfața cu terminalul telefonic;

2 = unitate centrală de calcul;

3 = decodificator analog-digital (de exemplu decodificator din standardul telefonic DTMF - Dual Tone Multi Frequency);

4 = convertor numeric-analog (DAC) audio;

5 = unitate de memorie

M = Terminal telefonic (inteligent sau clasic analogic)

CA = Casca audio standard, difuzor

C = Computer Internet (opțional)

Dispozitivul de securitate (DS) este integrabil, complet în casca audio (CA), camuflabil complet. În tehnologia actuală ar putea fi ca o cască bluetooth normal. Poate fi montat pe cablul telefonic pentru a recepționa eventual CallerID și a prelua semnalele audio direct din circuitul telefonic.

Este compatibil cu sistemele Internet de tip VoIP (Skype, WhatsUp etc.). Repsectiv circuitul telefonic poate fi complet virtual, sistemul este în cască. Asigură funcționare transparentă, fără intervenția utilizatorului pentru apelurile telefonice normale. Funcționarea lui este complet automată.

Este Integrabil si în dispozitive de tip cheie de securitate USB, conectabil la computer (C) pentru integrarea cu alte sisteme de securitate. De exemplu DS poate fi integrat cu o cheie USB de tip certificat digital sau semnătură electronică și poate primi informații prin canalul USB simultan cu apelul telefonic pentru validări suplimentare.

Funcționalitate:

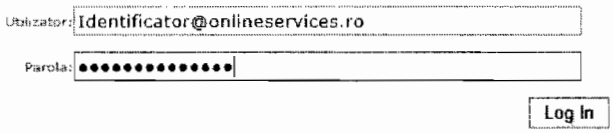
- Urmare a metodei de autentificare, terminalul (M) recepționează un apel telefonic;
- Informația despre apel (cine este chemătorul) poate ajunge la unitatea centrală (2) prin interfața cu terminalul telefonic (1). De exemplu dacă telefonul este un telefon mobil smartphone și interfața este conectată cu telefonul prin bluetooth. CallerID poate fi transmis către unitatea centrală (2) cu scopul identificării apelului veritabil de la serverul de autentificare preînregistrat în memorie (5);
- Unitatea centrală (2) poate comanda terminalului mobil (inteligent) să accepte apelul telefonic automat dacă de exemplu chemătorul este recunoscut ca server de autentificare conform metodei. În cazul telefoniei analogice apelul va fi recunoscut de către utilizator.
- Prin canalul audio stabilit prin conexiunea telefonică, serverul de autentificare transmite codurile audio care prin interfața (1) sunt preluate de decodificatorul (3) și transmise unității centrale (2) pentru decriptare. De exemplu serverul de autentificare transmite un șir de coduri DTMF care sunt recunoscute de decodificator și recepționate de unitatea centrală (2).
- Șirul codurile recepționate de unitatea centrală (2) sunt decriptate, verificată integritatea, validată regula de formare etc. pentru a fi transformate în pointeri care desemnează sunete inteligibile uman echivalente. De exemplu șirul codurilor DTMF 5317294 poate însemna identificarea fișierelor cu pointerii 5, 3, 1, 7, 2, 9 respectiv fișierele care conțin pronunția cuvintelor în limba Română șoricel, oaie, pisică, fluture, vacă, avion.
- Unitatea centrală (2) va citi din memoria (5) fișierele corespunzătoare pointerilor identificați și va produce prin convertorul numeric analog DAC (4) și interfața audio sunetele care sunt ascultate de către utilizatorul (U) în casca audio (A).
- Utilizatorul (U) va acționa asupra interfeței de autentificare conform sunetelor reproduse.

În cazul apelurilor telefonice normale de voce, urmare a faptului că numerele telefonice apelante nu sunt recunoscute sau utilizatorul nu activează dispozitivul de securitate, casca audio funcționează tradițional, respectiv dispozitivul de securitate este transparent.

Exemplu:

1. Utilizatorul (U) tastează adresa internet a platformei de servicii web (Service) la terminalul internet (Di). Alternativ, utilizatorul (U) apropie de terminalul (Di) un

card Near Near Communication (NFC) care este programat cu un link și deschide automat bowser-ul și o nouă sesiune web cu platforma de servicii (Service). Dacă utilizatorul (U) a inițiat cererea prin apropierea unu card pasul curent este ignorat, se trece direct la faza 2. Imaginea ecran a terminalului (Di) poate fi:



2. Serverul (Da) platformei (Service) verifică identificatorul utilizatorului (U) în baza de date și găsește numărul de telefon (T) al utilizatorului (U). Serverul (Da) generează aleatoriu un setul de pointeri care îi transmite simultan către dispozitivul de comunicație (Dc) al (3) platformei de servicii (Service) și către (3a) terminalul internet (Di):

   a. dispozitivul de comunicații (Dc) apelează telefonic-voce (4) numărul de telefon (T) al utilizatorului (U).
   b. terminalul utilizatorului (Di) generează imaginile pe baza setului de pointeri recepționat

În acest timp terminalul (Di) va afișa:

3. În momentul în care utilizatorul (U) răspunde la telefon (evenimentele 5, 6, 6a, 7), va auzi un mesaj de salut și un sunet indescifrabil, de exemplu o succesiune de sunete DTMF (standard telefonic pentru transmisia în banda audio a acționării tastelor telefoanelor). Dacă utilizatorul utilizează dispozitivul audio inteligent (CA) conectat la terminalul telefonic, atunci va auzi (8) sunetele care identifică imaginile pe care trebuie să le selecteze.

4. Utilizatorul (U) selectează (9) în ordine imaginile afişate în browser de către terminal (Di) conform sunetelor (instrucțiunilor vocale) produse de dispozitivul audio (CA). De exemplu pe ecran sunt afişate 10 (zece) imagini cum sunt: calculator, bicicletă, pisică, ceas, avion, floare, etc. În dispozitivul audio (CA) conectat la telefon (T) aude: avion, bicicletă etc.
5. Dacă utilizatorul (U) selectează (9) imaginile conform cu instrucțiunilor şi în timpul apelului, atunci primeşte accesul la serviciile platformei (Service). Orice abatere anulează accesul, respectiv comunicația este întreruptă la inițiativa serverului de autentificare (Da). Metoda şi arhitectura propusă verifică prezența persoanei desemnate prin interacțiunea cu apelul telefonic şi terminalul Internet în timp real prin confirmarea numărului de telefon, deținerea dispozitivului audio inteligent simultan cu interacțiunea la terminalul Internet. Persoana care solicită autorizarea cunoaşte semnificația sunetelor, interpretează corect semnificația lor şi acționează în timp util asupra imaginilor afişate la terminalul internet.

Metodă de autentificare Internet multi-factor în care terminalul telefonic poate fi decuplat de la Internet, compatibilă cu telefonia fixă, pe fir, analogică dar şi cu tehnologiile telefonice de tip VoIP securizate.

Sistem de securitate imun la pierderea terminalului telefonic, redirectarea apelului telefonic sau clonarea cardului SIM al telefonului mobil. Metodă şi arhitectură sistem care impune prezența simultană a utilizatorului în fața terminalului internet, la terminalul telefonic şi să dețină dispozitivul audio inteligent descris. Metoda restrânge timpul de acțiune al utilizatorului astfel încât face imposibilă prezența unui intermediar şi a breşelor de securitate Man-In-The-Middle.

Securitate sporită prin adăugarea factorului limbă în forma vocală, configurabil pentru utilizatorul desemnat. De exemplu utilizatorul doreşte ca limba în care îi sunt indicate imaginile pentru formarea parolei să fie latina veche.

Securitate sporită prin posibilitatea utilizării indicațiilor vocale indirecte, a căror semnificație este cunoscută de un grup restrâns de utilizatori. De exemplu sunetul pronunțat este "miroase bine" iar singura imagine care corespunde criteriului este *floare*.

Securitate sporită prin posibilitatea adăugării unor imagini capcană sau sunete capcană a căror semnificație este cunoscută numai de către utilizatorii legitimi. De exemplu utilizatorii legitimi știu că imaginea jokerului nu va fi niciodată selectată chiar dacă este indicată vocal. Selectarea acestei imagini va determina anularea cererii de autentificare întotdeauna.

Securitate sporită conform metodei prin aceea că pachetul de date care conține parola de unică utilizare criptată poate fi recepționată în timpul apelului prin canale de date alternative. De exemplu dacă utilizatorul răspunde la apelul telefonic, atunci sistemul poate transmite pachetul de date criptat necesar producerii sunetelor prin SMS sau o aplicație dedicată pate extrage o serie de date necesare decriptării dintr-o secvență audio sau nu a unui film disponibil Internet, sau a unui canal radio public. Se poate ca sistemul central să transmită o serie de date (parametrii) care se schimbă zilnic prin radio, pentru a marca teritorial posibilitatea utilizării sistemului.

Securitate sporită prin posibilitatea de a compara datele după decriptare, recepționate de dispozitivul audio DA cu datele transmise de serviciul (Service) pentru autentificarea utilizatorului prin algoritmi avansați de criptare cu parametrii care pot cuprinde aria geografică în care este permisă decriptarea, numele rețelei curente a serviciului de date și voce GSM etc. Oricare neconcordanță blochează la nivelul dispozitivului audio DA procesul de autentificare. De exemplu dacă numele rețelei GSM primită de la server nu corespunde cu numele rețelei GSM în care este utilizat terminalul (ex. este în roaming) atunci DA va bloca procesul, respectiv nu va produce sunetele corecte ci poate produce sunete pentru inducerea în eroare. Autentificarea nu va mai avea loc.

Metodă de autorizare simplă, rapidă cu verificarea identității multi-factor. Utilizatorul apropie cardul, primește apelul, alege imagini. Procesul se desfășoară doar pe durata apelului telefonic. (Alegerea poate fi realizată pe ecran tactil utilizând degetul – reduce efortul de coordonare și utilizarea altor obiecte). Browser-ele moderne permit mărirea imaginilor după confortul utilizatorului (combate deficiența vederii).

Metoda și arhitectura propusă permite utilizarea de către persoane cu dizabilități cum sunt cele cu capacitate de memorare redusă, cu deficiențe motorii – respectiv incapacitatea de a utiliza tastaturi, cu deficiențe de vedere – incapacitatea de a utiliza ecrane, deficiențe de coordonare etc. Metoda se bazează pe utilizarea tehnologiilor avansate care pot transmite automat identificatorul utilizatorului. De exemplu tehnologiile de recunoaștere vocală sau biometrice, NFC, respectiv carduri de proximitate sau alte dispozitive similare (inele, brățări, ceasuri de mână, etc.) care pot transmite terminalului internet (Di) identificatorul utilizatorului. Interacțiunea cu sistemul de telefonie este practic eliminată, utilizatorul doar răspunde la apel (poate fi selectat răspunsul automat în funcție de caracteristicile tehnice alte telefonului (T).

Complexitatea sistemului redusă determină costuri mici ale implementării. Este eliminat sistemul de interacțiune vocală IVR și multe din validările de adrese internet (IP) reducând astfel necesarul de putere de calcul, crescând fiabilitatea și scăzând

costurile. Deoarece durata convorbiri telefonice este redusă la minim, nefiind necesară interacțiunea IVR cu utilizatorul, necesarul de timp de comunicație, respectiv intensitatea utilizării liniilor telefonice scade, micșorând la implementare numărul de linii telefonice necesare, numărul de echipamente de telecomunicații și costurile cu exploatarea.

Metoda și sistemul propus este exploatabilă direct și în situații extreme cum sunt pierderea cardului sau imposibilitatea citirii electronice automate a identificatorului unic al utilizatorului (U) din diferite cauze tehnice – defect, incompatibilitate etc... În aceste situații este necesară utilizarea numelui utilizatorului și parola în pagina Internet specifică serviciului.

Sistem deschis pentru creșterea siguranței prin utilizarea unor dispozitive terminale noi cu facilități de siguranță sporite cum sunt telefoanele inteligente, tabletele sau computerele personale cu posibilitatea ștergerii tuturor datelor și aplicațiilor utilizatorului (inițializării) terminalului în cazul furtului sau abuzului, autentificare biometrică – amprentă tactilă, iris, facială, vocală etc.

Sistem deschis pentru creșterea gradului de confort al utilizatorului (cu dizabilități) prin utilizarea sistemelor terminale care permit accesarea serviciilor internet prin comandă vocală, gesturi sau dispozitive auxiliare (carduri, inele etc). Sistemul conform metodei este sigur și imun la greșelile produse prin comenzi vocale eronate sau gesturi interpretate greșit deoarece apelul telefonic (faza 4) poate fi rejectat.

Metodă care permite virtualizarea dispozitivului audio inteligent în terminale telefonice inteligente cu putere de calcul corespunzătoare și sisteme sporite de securitate (inițializare la inițiativa sistemului de securitate, autodistrugerea datelor și aplicațiilor în caz de abuz, furt sau pierdere, certificate digitale, enclave digitale pentru securitatea datelor, etc.)

Metodă și arhitectură sistem care permite implementarea în sisteme cu putere de calcul reduse, compatibile cu clasa de echipamente Internet of Things (IoT). Întreaga arhitectură propusă, respectiv terminalul Di, serverul Da și echipamentul de telecomunicații Dc pot fi implementate într-un singur echipament.

Revendicări:

1. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, caracterizata prin accea ca, se verifică prezența persoanei desemnate prin interacțiunea cu apelul telefonic și terminalul Internet în timp real prin confirmarea numărului de telefon, deținerea dispozitivului audio inteligent simultan cu interacțiunea la terminalul Internet, persoana care solicită autorizarea cunoaște semnificația sunetelor, interpretează corect semnificația lor și acționează în timp util asupra imaginilor afișate la terminalul internet, urmare a metodei de autentificare, un terminal (M) recepționează un apel telefonic, informația despre apel, poate ajunge la o unitate centrală (2) prin interfața cu terminalul telefonic (1), dacă telefonul este un telefon mobil smartphone și interfața este conectată cu telefonul prin bluetooth, CallerID poate fi transmis către o unitate centrală (2) cu scopul identificării apelului veritabil de la serverul de autentificare preînregistrat în memoria (5), unitatea centrală (2) poate comanda terminalului mobil inteligent să accepte apelul telefonic automat dacă de chemătorul este recunoscut ca server de autentificare conform metodei, in cazul telefoniei analogice apelul va fi recunoscut de către utilizator, prin canalul audio stabilit prin conexiunea telefonică, serverul de autentificare transmite codurile audio care printr-o interfața (1) sunt preluate de un decodificator (3) și transmise unității centrale (2) pentru decriptare, serverul de autentificare transmite un șir de coduri DTMF care sunt recunoscute de decodificatorul (3) și recepționate de unitatea centrală (2), sirul codurile recepționate de unitatea centrală (2) sunt decriptate, verificată integritatea, validată regula de formare, pentru a fi transformate în pointeri care desemnează sunete inteligibile uman echivalente, unitatea centrală (2) va citi din memoria (5) fișierele corespunzătoare pointerilor identificați și va produce printr-un convertor numeric analog DAC (4) și interfața audio sunetele care sunt ascultate de către utilizatorul (U) în casca audio (A), Utilizatorul (U) va acționa asupra interfeței de autentificare conform sunetelor reproduse.

2. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1, caracterizata prin accea ca, terminalul telefonic poate fi decuplat de la Internet, este compatibilă cu telefonia fixă, pe fir, analogică dar și cu tehnologiile telefonice de tip VoIP securizate, un dispozitiv de securitate (DS) este imun la pierderea terminalului telefonic (T), redirectarea apelului telefonic sau clonarea cardului SIM al telefonului mobil.

3. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1 si 2, caracterizata prin accea ca, se impune prezența simultană a utilizatorului în fața terminalului internet, la terminalul telefonic și să dețină dispozitivul audio inteligent descris. Metoda restrânge timpul de acțiune al utilizatorului astfel încât face imposibilă prezența unui intermediar și a breșelor de securitate Man-In-The-Middle.

4. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1, 2 si 3, caracterizata prin accea ca, securitatea sporită este asigurata si de adăugarea factorului limbă în forma vocală, configurabil pentru utilizatorul desemnat, prin posibilitatea utilizării indicațiilor vocale indirecte, a căror semnificație este cunoscută de un grup restrâns de utilizatori, prin posibilitatea adăugării unor imagini capcană sau sunete capcană a căror semnificație este cunoscută numai de către utilizatorii legitimi, utilizatorii legitimi știu că imaginea jokerului nu va fi niciodată selectată chiar dacă este indicată vocal, selectarea acestei imagini va determina anularea cererii de autentificare întotdeauna, prin aceea că pachetul de date care conține parola de unică utilizare criptată poate fi recepționată în timpul apelului prin canale de date alternative, prin posibilitatea de a compara datele după decriptare, recepționate de dispozitivul audio (DA) cu datele transmise de serviciul „Service" pentru autentificarea utilizatorului prin algoritmi avansați de criptare cu parametrii care pot cuprinde aria geografică în care este permisă decriptarea, numele rețelei curente a serviciului de date și voce GSM, oricare neconcordanță blochează la nivelul dispozitivului audio (DA) procesul de autentificare.

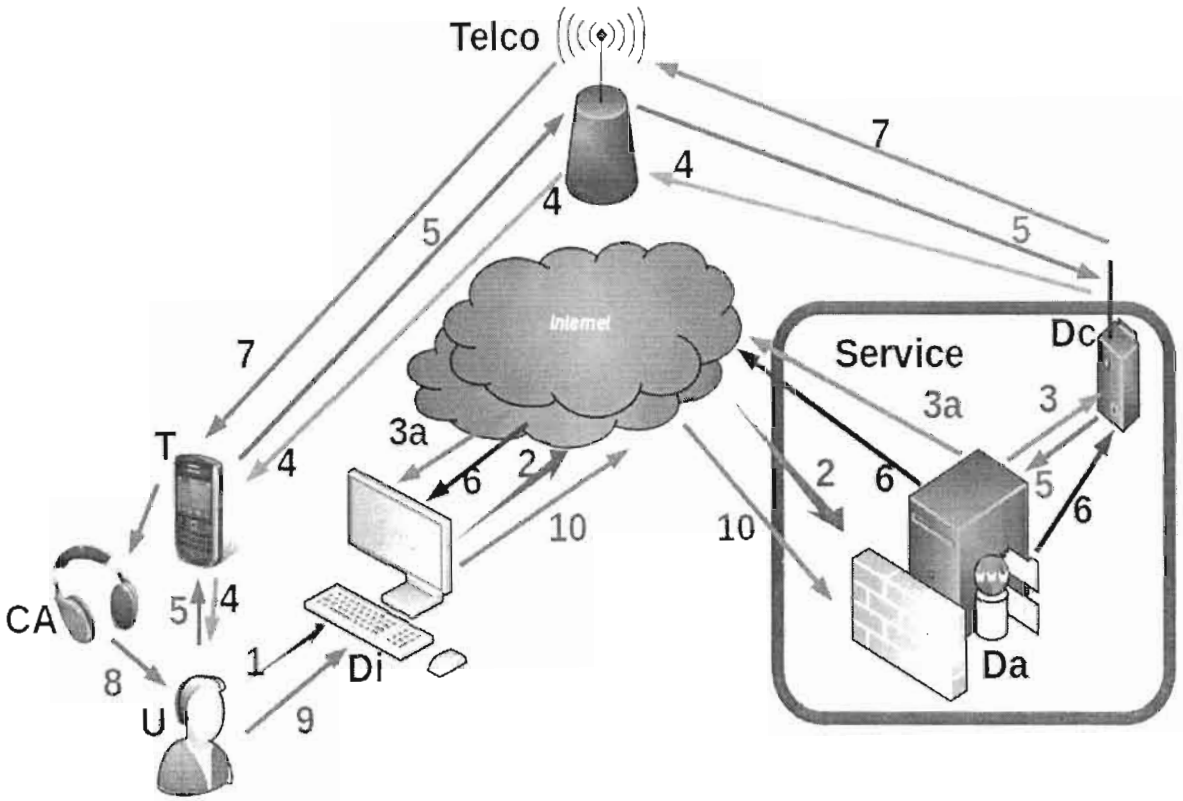
5. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1, 2, 3 si 4, caracterizata prin accea ca, utilizatorul apropie cardul, primește apelul, alege imagini, procesul se desfășoară doar pe durata apelului telefonic, este posibil utilizarea de către persoane cu dizabilități cum sunt cele cu capacitate de memorare redusă, cu deficiențe motorii , respectiv incapacitatea de a utiliza tastaturi, cu deficiențe de vedere – incapacitatea de a utiliza ecrane, deficiențe de coordonare, se utilizeaza tehnologi avansate care pot transmite automat identificatorul utilizatorului.

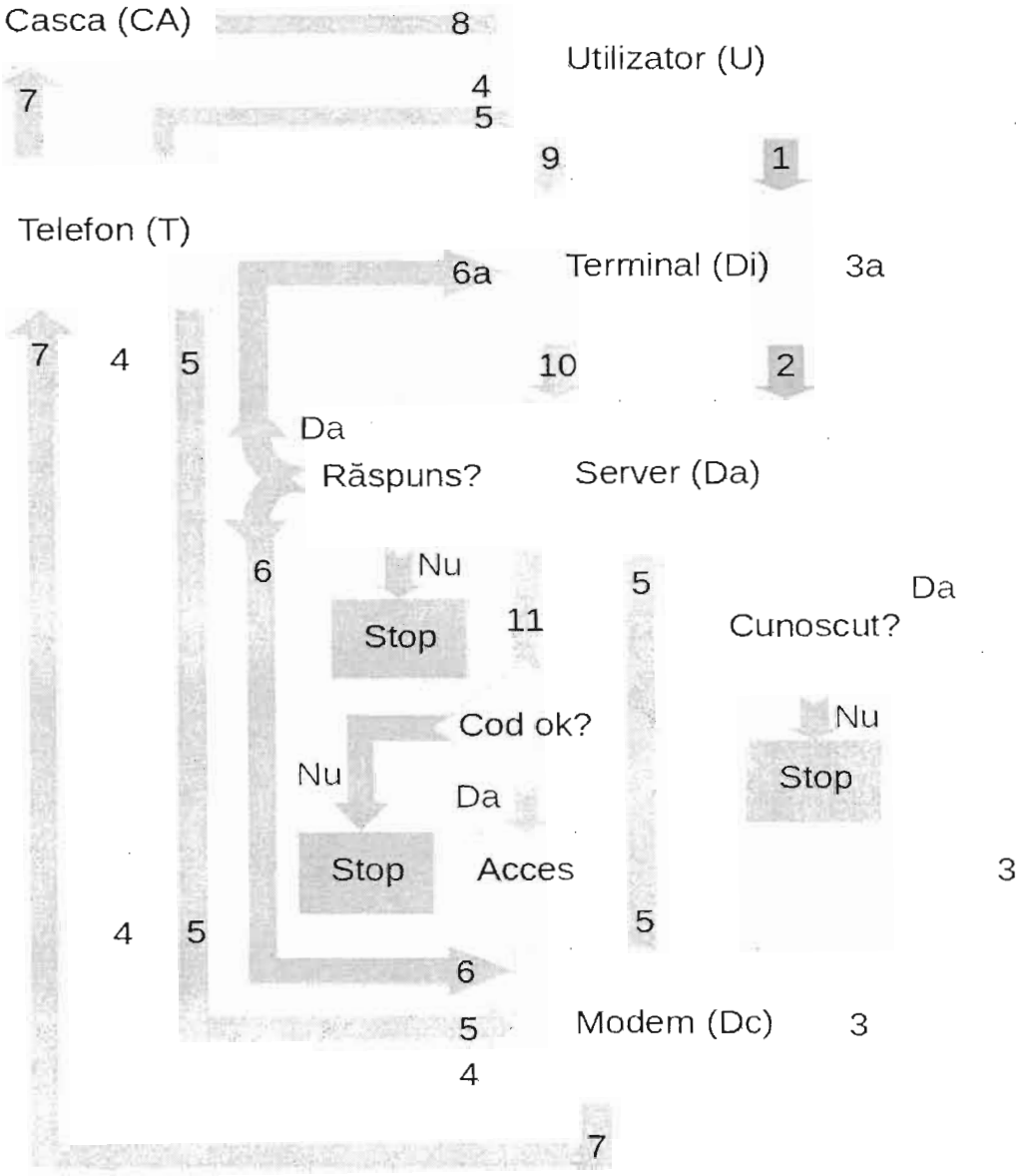
6. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1, 2, 3, 4 si 5, caracterizata prin accea ca, sistemul este deschis pentru creșterea siguranței prin utilizarea unor dispozitive terminale noi cu facilități de siguranță sporite cum sunt telefoanele inteligente, tabletele sau computerele personale cu posibilitatea ștergerii tuturor datelor și aplicațiilor utilizatorului terminalului în cazul furtului sau abuzului, autentificare biometrică – amprentă tactilă, iris, facială, vocală, pentru creșterea gradului de confort al utilizatorului prin utilizarea sistemelor terminale care permit accesarea serviciilor internet prin comandă vocală, gesturi sau dispozitive auxiliare

7. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1, 2, 3, 4, 5 si 6, caracterizata prin accea ca, dispozitivul de securitate (DS) este integrabil, complet în casca audio (CA), camuflabil complet, poate fi montat pe cablul telefonic pentru a recepționa eventual CallerID și a prelua semnalele audio direct din circuitul telefonic, este compatibil cu sistemele Internet de tip VoIP, respectiv circuitul telefonic poate fi complet virtual, sistemul este în cască, funcționarea lui este complet automată, este integrabil si în dispozitive de tip cheie de securitate USB, conectabil la computer (C) pentru integrarea cu alte sisteme de securitate.

8. Metoda și arhitectura pentru acordarea accesului autorizat la o platformă de servicii internet, conform cu revendicarea 1-6 si 7, caracterizata prin accea ca, dispozitivul de securitate (DS) este compus si interconectat astfel: interfața cu terminalul telefonic (1), unitate centrală de calcul (2,) decodificator analog-digital (3), convertor numeric-analog (DAC) audio (4), unitate de memorie (4), terminal telefonic (M), Casca audio standard, difuzor (CA), optional computer Internet (C).

Fig 1


Telco
7
4
4
5
5
7
Internet
Service
Dc
3a
3
T
4
3a
6
2
2
6
5
6
10
10
CA
5
4
1
Di
8
U
9
Da


Casca (CA)
8
Utilizator (U)
7
4
5
9
1
Telefon (T)
6a
Terminal (Di)
3a
7
4
5
10
2
Da
Răspuns?
Server (Da)
6
Nu
5
Da
Stop
11
Cunoscut?
Cod ok?
Nu
Nu
Da
Stop
Acces
3
4
5
5
6
5
Modem (Dc)
3
4
7

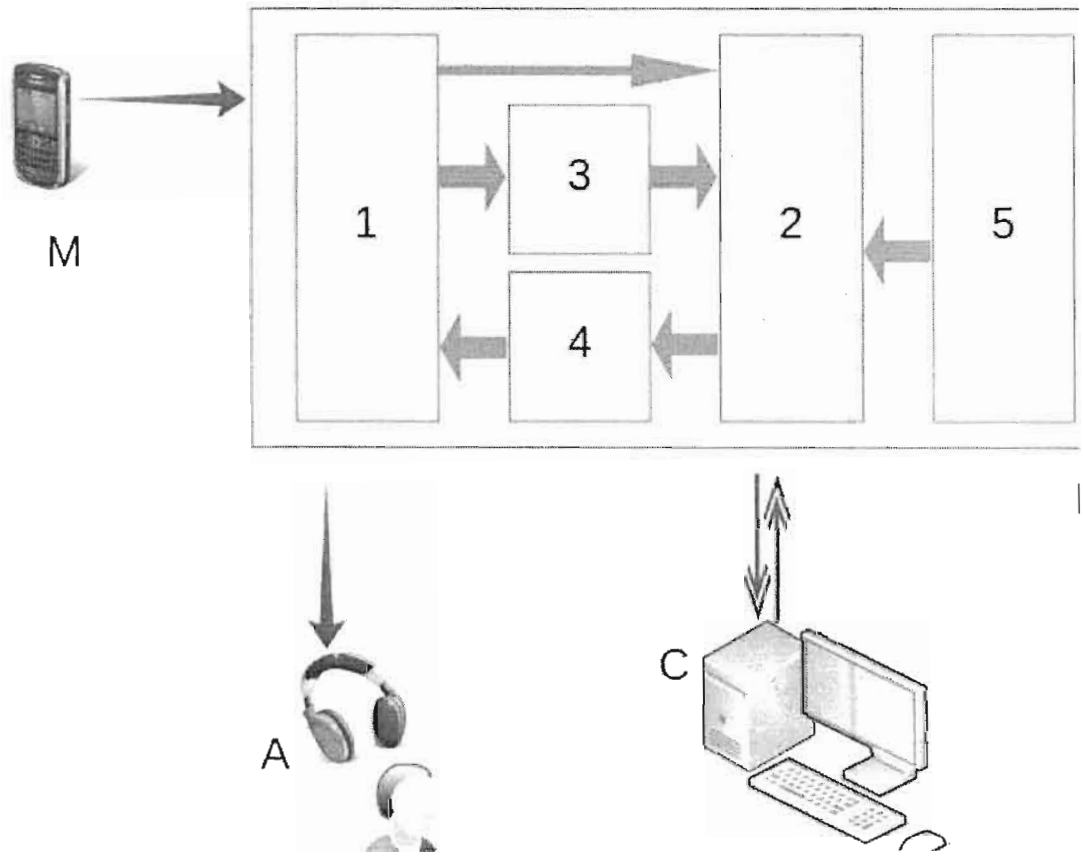


fig.6