(19) LIETUVOS RESPUBLIKA
VALSTYBINIS PATENTŲ BIURAS
V P B

(10) **LT 5403 B**

(12) **PATENTO APRAŠYMAS**

(11) Patento numeris: **5403**

(51) Int. Cl. (2006): **G06K 19/077**
G07C 9/00

(21) Paraiškos numeris: **2006 029**

(22) Paraiškos padavimo data: **2005 04 05**

(41) Paraiškos paskelbimo data: **2006 10 25**

(45) Patento paskelbimo data: **2007 02 26**

(62) Paraiškos, iš kurios dokumentas išskirtas, numeris: **2005 035**

(86) Tarptautinės paraiškos numeris: **PCT/US2003/028602**

(86) Tarptautinės paraiškos padavimo data: **2003 09 10**

(85) Nacionalinio PCT lygio procedūros pradžios data: **2005 04 05**

(30) Prioritetas: **20020409716P, 2002 09 10, US**
20020409715P, 2002 09 10, US
20020429919P, 2002 11 27, US
20020433254P, 2002 12 13, US
20030484692P, 2003 07 03, US

(72) Išradėjas:

Tamio SAITO, US
Takashi AIDA, US
Wayne DRIZIN, US

(73) Patento savininkas:

Ivi Smart Technologies, Inc., 1810 Old Oakland Road, Suite F, San Jose CA 95131, US

(74) Patentinis patikėtinis:

Reda ŽABOLIENĖ, Advokatės Redos Žabolienės kontora METIDA, Gedimino pr. 45-6, LT-01109 Vilnius, LT

(54) Pavadinimas:

Saugus biometrinis tapatybės verifikavimas

(57) Referatas:

Ypatingai saugi identifikavimo kortelė turi joje įrengtą atmintį biometrinių duomenų saugojimui ir jutiklį biometrinių duomenų nuskaitymui. Kortelės procesorius atlieka palyginimo operaciją įsitikinti, kad nuskaityti biometriniai duomenys sutampa su lokaliai saugomais biometriniais duomenimis. Tik esant teigiamam rezultatui

LT 5403 B

nuskaityti duomenys ar kortelės duomenys yra siunčiami papildomam patikrinimui ir/arba paskesniam apdorojimui. Optimaliu atveju kortelė yra ISO SmartCard suderinama kortelė. Pagal vieną iš realizavimo variantų ISO SmartCard kortelė veikia kaip užkarda, skirta apsaugoti apsaugos procesorių, naudojamą biometrinių duomenų saugojimui ir apsaugai nuo piktavališkų išorinių atakų per ISO SmartCard sąsają. Pagal kitą realizavimo variantą apsaugos procesorius yra įterptas tarp ISO SmartCard sąsajos ir nemodifikuoto ISO SmartCard procesoriaus ir blokuoja bet kokius išorinius ryšius, kol vartotojo pirštas nėra palygintas su anksčiau registruotu piršto atspaudu. Yra numatytas realaus laiko grįžtamasis ryšys, kol vartotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tokiu būdu palengvinant piršto padėties nustatymą virš jutiklio. Kortelė gali būti naudojama ryšiui su transakciniu tinklu užtikrinti ar fizinio įėjimo į saugią sritį leidimui gauti.

Visuotinis kompiuterizavimas ir ypač interneto technologijos suteikia lengvesnį priėjimą prie duomenų, įskaitant finansinius, medicininius, asmeninius duomenis, ir greitai atlikti finansines ir kitas transakcijas, kuriose yra atnaujinami konfidencialūs duomenys arba jais yra apsikeičiama.

Įprasta tokių duomenų konfidencialumą išsaugoti slaptažodžiais, tačiau dažniausiai slaptažodžiams naudojama gimimo data ar telefono numeris, kuriuos yra lengva atspėti, todėl tai nėra saugu. Be to, net ir sudėtingi atsitiktinai sukurti slaptažodžiai dažnai yra pavagiami. Tokiu būdu slaptažodinės duomenų sistemos nėra apsaugotos nuo kriminalinių įsilaužimų, kas sukelia pavojų pramonei ir ekonomikai ir net žmonių gyvybėms. Vadinasi, yra reikalingas patobulintas duomenų įslaptinimo ir apsaugos nuo nelegalaus priėjimo prie jų būdas.

Biometriniai duomenys gali apimti tikslias detales, kurias yra sunku paimti, bet lengva analizuoti (kaip, pavyzdžiui, pirštų atspaudų detales), arba visą raštą, kuri lengva paimti, bet sunku analizuoti (kaip, pavyzdžiui, atstumus tarp pirštų atspaudų gretimų spiralinių vijų).

Šiuo metu yra sukurti šifravimo algoritmai, kuriems reikalingas skaitmeninis raktas, kurį turi tik autorizuotas naudotojas. Be tinkamo rakto užšifruoti duomenys gali būti dešifruoti į tinkamą formatą tik sugaišus nemažai laiko ir jėgų, ir tai tik tuomet, kuomet yra žinomos (arba bent jau nuspėjamos) tam tikros neiššifruotų duomenų charakteristikos.

1985 metų vasario 15 dienos Tamio SAITO Japonijos patentinėje paraiškoje JP60-029868 aprašyta asmens tapatybės verifikavimo sistema, kuri naudoja tapatybės kortelę su integruota atmintimi užšifruotų biometrinių kortelės savininko duomenų registravimui. Biometriniai duomenys gali būti balsas, pirštų atspaudai, fizinė išvaizda ir/arba biologinės analizės duomenys. Kortelės duomenys naudojimo metu yra nuskaitomi ir dešifruojami palyginimui su atitinkamais duomenimis, paimtais iš kortelę pateikiančio asmens. Tokia sistema leidžia gana tiksliai identifikuoti registruotą individą. Tačiau, kadangi biometrinius duomenis nuskaito ir apdoroja išorinis įrenginys, yra sunku apsaugoti kortelėje saugomus duomenis nuo pakeitimo ir/arba vagystės.

Yra žinoma patobulinta tapatybės verifikavimo kortelė su duomenų valdoma multiprocesorine mikroschema, kuri suteikia apsauginę užkardą, užšifruojančią bei

izoliuojančią kortelėje saugomus biometrinius duomenis, tokiu būdu žymiai geriau apsaugant nuo neleistino kortelės duomenų pakeitimo. Tačiau tikrasis palyginimo procesas buvo atliktas tame pačiame išoriniame skaitytuvo terminale, kuris nuskaitė gyvus biometrinius duomenis ir kuris potencialiai nėra apsaugotas nuo piktavališkų išorinių veiksmų.

Aukšto saugumo identifikavimo kortelė, aprašyta pirmajame realizavimo variante, turi ne tik lokalią biometrinių duomenų saugojimo atmintį, bet taip pat lokalų jutiklį gyvų biometrinių duomenų nuskaitymui. Nutolusi autentiškumo nustatymo sistema turi saugią duomenų bazę su biometriniais duomenimis. Kortelės procesorius atlieka preliminarią patikrą, siekdamas patikrinti, ar nuskaityti biometriniai duomenys sutampa su kortelėje saugomais biometriniais duomenimis. Tik esant teigiamam rezultatui nuskaityti duomenys ar saugomi atmintyje duomenys yra siunčiami į nutolusią autentiškumo nustatymo sistemą papildomam palyginimui ir paskesniam apdorojimui. Siekiant apsisaugoti nuo piktavališkos atakos, kortelėje saugomi duomenys optimaliu atveju skiriasi nuo atokiai saugomų duomenų, ir tiek kortelėje, tiek nuotolinis duomenų palyginimas atliekamas, naudojant skirtingus palyginimo algoritmus. Todėl jei bus bandoma neleistinai įsibrauti į kortelę ar į vietinį terminalą, prie kurio kortelė yra prijungta, išlieka didelė tikimybė, kad nutolusi autentiškumo nustatymo sistema sugebės aptikti šį bandymą įsilaužti.

Kortelė, aprašyta antrajame realizavimo variante, taip pat turi lokalią atmintį biometrinių duomenų saugojimui, lokalų jutiklį gyvų biometrinių duomenų nuskaitymui ir lokalų procesorių. Tačiau šiame realizavimo variante visas palyginimo procesas atliekamas vietiniu procesoriumi ir tiek gyvai nuskaityti duomenys, tiek kita "privati" informacija, saugoma kortelės atmintyje, neprieinama jokiems išoriniams procesams. Šiuo atveju tik generuojamas patvirtinantis pranešimas, jei naujai nuskaityti biometriniai duomenys ir anksčiau nuskaityti biometriniai duomenys sutampa. Šis patvirtinimo pranešimas leidžia kortelei veikti panašiu kaip įprastoje ISO SmartCard kortelėje būdu; po sėkmingo/nesėkmingo įprasto asmeninio identifikavimo kodo (PIN) įvedimo, tačiau su papildoma apsauga, kurią suteikė saugesnis patikrinimo procesas. Bet kuriame iš šių realizavimo variantų kortelėje saugomi biometriniai duomenys ir bet koks susietas dešifravimo algoritmas ar raktas yra optimaliu atveju įrašytas į kortelę, išdavimo kortelės naudotojui metu tokiu būdu, kuris neleidžia pasiekti jų iš išorės, taip dar

labiau pagerinamas kortelėje saugomų biometrinių duomenų vientisumas ir visas patikrinimo procesas.

Viename iš realizavimo variantų ISO SmarCard kortelė veikia kaip užkarda, apsauganti apsaugos procesorių, naudojamą biometrinių duomenų saugojimui ir apdorojimui, nuo išorinio įsilaužimo per ISO SmartCard sąsają. Kitame variante saugumo procesorius yra įterptas tarp ISO SmarCard sąsajos ir nemodifikuoto SmartCard procesoriaus ir blokuoja bet kokį ryšį su išore tol, kol naudotojo piršto atspaudas nėra sutapdintas su anksčiau registruotu piršto atspaudu.

Pagal vieną aukšto saugumo identifikavimo kortelės su kortelėje numatyta pirštų atspaudų palyginimo ypatybe realizavimo variantą yra numatytas realaus laiko grįžtamasis ryšis, kuomet naudotojas manipuliuoja pirštu virš pirštų atspaudų jutiklio, tokiu būdu palengvinant optinį piršto nustatymą virš jutiklio. Šis grįžtamasis ryšys ne tik palengvina skaičiavimą, bet taip pat suteikia papildomas priemones, padedančias atskirti nepatyrusį naudotoją nuo nesąžiningo naudotojo ir, tokiu būdu, sumažina pirmojo ir/arba antrojo atvejų tikimybę. Kitame realizavimo variante pirštų atspaudų jutiklis yra įrengtas nešiklyje, suteikiančiame papildomo standumo.

Viename iš pateiktųjų variantų nuskaityti biometriniai duomenys ir/arba kortelės savininko tapatybė yra užšifruojami ir įvedami į operacinį tinklą, kurį sudaro finansinė institucija ir atskiras tapatybės nustatymo serveris, prieš suteikiant priėjimą prie konfidencialių duomenų ar bet kokio automatizuoto proceso, skirto atlikti saugią operaciją. Kitame pateiktajame variante kortelės išvestis naudojama, norint fiziškai įeiti į saugią zoną. Bet kuriame iš variantų sėkmingi ir nesėkmingi bandymai gali būti registruojami arba kortelėje, arba išoriniame apsauginiame serveryje, arba abiejuose.

Fig.1 pateiktas vienas SmarCard kortelės, nustatančios asmens tapatybę, realizavimo variantas.

Fig.2 pateikta diagrama, vaizduojanti procesą, padedantį naudotojui patalpinti pirštą virš pirštų atspaudų jutiklio.

Fig.3 yra funkcinė biometrinio verifikavimo sistemos, galinčios nustatyti asmens, pateikiančio identifikavimo kortelę, tapatybę tiek vietiniu, tiek nuotoliniu būdu, blokinė schema.

Fig.4 yra funkcinė biometrinio verifikavimo kortelės su skirtingais fizinių duomenų takais, skirtais panaudoti pirminio kortelės turėtojo biometrinių duomenų

nuskaitymo ir kortelės turėtojo asmens tapatybės patikrinimo duomenų persiuntimo nuotoliam apdorojimui metu, blokinė schema

Fig.5 pateiktas alternatyvus fig.4 biometrinio verifikavimo kortelės, kuri yra skirta naudojimui su nemodifikuotu ISO SmartCard procesoriumi, realizavimo variantas.

Fig.6 yra diagrama, parodanti ryšį tarp pavyzdinio panaudojimo ir pavyzdinės verifikavimo kortelės, kurioje atliekamas tik vietinis kortelės savininko tapatybės patikrinimas.

Fig.7 yra panaši į fig.6 diagrama, modifikuota panaudojimui su fig.5 pavaizduota biometrinio verifikavimo kortele.

Fig.8 pateiktas antrasis SmartCard kortelės su biometrinio verifikavimo funkcija realizavimo variantas, kuri gali būti prijungta prie vietinio terminalo arba bevieliu būdu, arba elektrine jungtimi.

Fig.9 yra fig.8 kortelės skerspjūvio vaizdas.

Fig.10 yra pirštų atspaudų jutiklio schema.

Fig.11 pateiktas fig.10 pavaizduoto jutiklio nešiklio vienas realizavimo variantas.

SmartCard kortelė

Čia naudojami terminai "smart card" ar "intelligent card" ("intelektuali kortelė") bendraja prasme reiškia bet kokį fizikinį objektą, kuris yra pakankamai mažas, kad būtų galima laikyti rankoje, nešioti, pasikabinus ant kaklo ar kitokiu būdu, ir kuris turi mikroprocesorių, galintį saugoti, apdoroti ir siųsti skaitmeniniu būdu užšifruotą informaciją, susijusią su konkrečiu kortelės savininku. Vienas tokios kortelės pavyzdys yra ISO (International Standarts Organization – tarptautinė standartų organizacija) SmartCard kortelė, kuri yra įprastos kredito kortelės dydžio ir formos, bet kuri turi impulsinę atmintį, naudotoją apibūdinančių duomenų saugojimui ir mikroprocesorių, kuris gali būti užprogramuotas galingu šifravimo algoritmu, kuris nurodo ar gautas iš terminalo PIN kodas (Personal Identification Number - asmens identifikavimo numeris) atitinka kortelėje įrašytą PIN kodą, tuo labiau užtikrinant, kad kortelę pateikiantis asmuo yra tikrasis kortelės savininkas, nei tai būtų įmanoma atlikti su verifikavimo sistema, kuri paprasčiausiai vizualiai patikrina parašų ir fizinės išvaizdos panašumą.

Fig.1 parodytas vienas SmartCard kortelės su joje įgyvendinta biometrinio verifikavimo funkcija realizavimo variantas. Kortelė 1 yra paprastai pagaminta iš plastinės medžiagos ir ji yra panaši į įprastą kredito kortelę, jos matmenys pagal ISO 7816 standartą yra maždaug 53,98 x 85.6 mm, o storis – maždaug 0,76 mm ar daugiau.

Panašiai kaip ir įprasta kredito kortelė, kortelė 1 turi laisvą viršutinę sritį 2, nusidriekiančią per visą kortelės ilgį, skirtą magnetinei juostelei įrengti (kaip nurodyta ISO 7811-2 & 7811-6) kitoje kortelės pusėje, kurioje gali būti įrašyta įprasta raidinė-skaitmeninė informacija apie kortelės savininką ir bet kokią susietą sąskaitą, tuo užtikrinant, kad kortelė 1 galės būti nuskaityta įprastu magnetinės kortelės skaitytuvu. Tačiau, kadangi bet kokia informacija, įrašyta į magnetinę juostelę, gali būti lengvai pakeista, tokia magnetinė juostelė yra skirta ribotam naudojimui, kur grįžtamasis suderinamumas su senesniais magnetinių juostelių terminalais yra svarbiau už saugumą, kurio magnetinė juostelė negali suteikti sistemai.

Viršutinė sritis 2 taip pat gali būti panaudota įvairių apsauginių priemonių įrengimui, tokių kaip nesuklastojama spalvota kortelės savininko nuotrauka ir/arba kortelės eminento holografinis ženklas. Kortelės 1 apatinė sritis gali būti panaudota įprastu būdu informacijai, tokiai kaip kortelės savininko vardas, pavardė, sąskaitos (ar kortelės) numeris, galiojimo laikas, iškiliaisiais rašmenimis įrašyti (kaip nurodyta ISO 7811-1) tam, kad kortelę 1 galima būtų apdoroti įprastu kortelės spausdintuvu.

Viršutinė sritis 2 ir apatinė sritis 3 yra atskirtos vidurine sritimi 4, kurioje įrengta aštuonių matomų ISO SmartCard kontaktų 5 grupė, kurie užtikrina įprastą elektrinį ryšį tarp kortelės ir atitinkamo kortelės skaitytuvo kontaktų. Jų pagalba užtikrinamas ne tik duomenų, bet taip pat ir maitinimo, laiko ir valdymo signalų perdavimas tarp skaitytuvo ir kortelės, kaip nurodyta ISO 7816-3.

Srities 4 dešinėje pusėje matyti jutiklis 6, kuris naudojamas kortelės savininko piršto atspaudų nuskaitymui. Optimaliu atveju kortelei yra suteiktas unikalus ID kodas, kuris yra suderintas su jutikliu 6 ir kitais kortelėje įrengtais elektroniniais komponentais, pavyzdžiui, įprasto IP ir/arba MAC adreso formato kodas.

Taip pat fig.1 pavaizduotoje kortelėje yra įrengti keli papildomi elektroniniai komponentai, kurie kartu su kontaktų grupe 5 ir jutikliu 6 suteikia kortelei daugiau funkcionalumo ir ypač – saugumo, nei tai būtų įmanoma pasiekti kitokiu būdu.

Viename iš išradimo realizavimo variantų suderinamas su ISO SmartCard kortele procesorius 7 yra tiesiogiai sujungtas su kontaktų grupe 5, taip sudarant galimybę sujungti jį su neparodytu išoriniu ISO suderinamu kortelės skaitytuvu ne tik tam, kad tiektų srovę kortelės elektronikai, bet ir duomenų perdavimui tarp kortelės ir bet kokios išorinės ryšių programos, apsaugos programos, transakcijų programos ir/arba kitų taikomųjų programų, instaliuotų kortelės skaitytuve ar bet kuriuose kompiuteriniuose prietaisuose, susietuose su kortelės skaitytuvu.

Nors aprašytame realizavimo variante duomenų kelias tarp kortelės 1 ir išorinio kortelės skaitytuvo yra laidinis, naudojant ISO nurodytą SmartCard kortelės kontaktinę įrangą, yra akivaizdu, kad kituose realizavimo variantuose gali būti panaudotos kitos ryšių technologijos, tokios kaip USB ar RS 232C, ar SPI (serijinė) jungtys belaidžiais RF (radijo dažnių), mikrobangų ir/arba IR (infraraudonųjų spindulių) ryšių kanalais.

Be to, nors aprašytame realizavimo variante kortelė gauna maitinimą iš kortelės skaitytuvo, kitos kortelės gali turėti kortelėje įmontuotą energijos šaltinį, pavyzdžiui, saulės bateriją ar akumuliatorių. Toks kortelėje įrengtas energijos šaltinis yra naudingas tuomet, kuomet, pavyzdžiui, mechaninis ryšys tarp kortelės 1 ir konkrečios rūšies kortelės skaitytuvo yra toks, kad naudotojas negali pasiekti pirštų atspaudų jutiklio 6, kuomet kontaktai 5 yra prijungti prie atitinkamų jungčių kortelės skaitytuvo viduje, ir, tokiu būdu, naudotojo pirštų atspaudai turi būti nuskaityti, kuomet kortelė 1 nėra tiesiogiai sujungta su kortelės skaitytuvu.

Apsaugos procesorius

Kaip matyti figūroje, apsaugos procesorius (centrinis apdorojimo įrenginys - CPU) 8 yra prijungtas tarp ISO procesoriaus 7 (CPU) ir jutiklio 6 ir yra skirtas saugiam nuskaitytų duomenų apdorojimui ir saugojimui, o taip pat kaip užkarda, neleidžianti nesankcionuotai prieiti prie duomenų ir programų, įrašytų į jo dedikuotąją atmintį, per ISO procesorių 7, kaip bus aprašyta žemiau. Tokia užkarda gali būti skirta praleisti tik užšifruotus duomenis, naudojant šifravimo raktą, kurio pagrindą sudaro unikalus priskirtojo tinklo adresas ar kuris yra kitaip unikalus konkrečiai kortelei, kaip, pavyzdžiui, duomenys apie anksčiau išsaugotą

pirštų atspaudų raštą ar unikalus priskirto prietaiso numeris, pavyzdžiui, centrinio procesoriaus (CPU) ar pirštų atspaudų jutiklio numeris. Kitame realizavimo variante užkarda praleidžia tik duomenis, kurie turi ankstesnio perdavimo ar duomenų unikalius identifikavimo duomenis. Dar kituose realizavimo variantuose užkarda taiko skirtingus raktus skirtingoms operacijoms ir naudoja šiuos raktus nukreipti duomenis į atitinkamą skirtingą procesoriaus ar atminties skyrių.

Kitame nepavaizduotame realizavimo variante apsaugos procesorius 8 yra tiesiogiai prijungtas prie ISO kontaktų 5 ir veikia kaip apsauginis filtras tarp ISO procesoriaus 7 ir ISO kontaktų 5. Toks papildomas įrengimas suteikia papildomą apsaugą, kurią suteikia apsaugos procesorius 8 ir jutiklis 6, nepadarant žalos jokioms apsauginėms funkcijoms, kurios jau gali būti inkorporuotos į ISO procesorių 7.

Apsaugos procesorius 8 optimaliu atveju turi nelakią puslaidininkinę ar nepuslaidininkinę atmintį, tokią kaip FRAM, OTP, E^2PROM, MRAM, MROM, skirtą saugoti anksčiau nuskaitytus pirštų atspaudus ir/arba kitą biometrinę informaciją. Kituose realizavimo variantuose kai kurios arba visos apsaugos procesoriaus 8 funkcijos gali būti įdiegtos ISO procesoriuje 7 ir/arba kai kurios arba visos ISO procesoriaus 7 funkcijos gali būti įdiegtos apsaugos procesoriuje 8. Toks kombinuotas įdiegimas išsaugos užkardą tarp įvairių funkcijų, kurios būtų ypatingai naudingos, jei prietaise būtų įdiegtas procesas, kuris neleistų jokių paskesnių įrašytų programų modifikavimo. Alternatyviai abu procesoriai 7, 8 gali būti atskiri procesoriai viename daugiaprocesoriniame prietaise, skirti apsaugoti kiekvieną procesą nuo bet kokio kito proceso, vykstančio kitame procesoriuje, interferencijos. Vienas tokio daugiaprocesorinio prietaiso pavyzdys yra Sharp (Japonija) gamybos DDMP (Data Driven Multiple Processor – duomenų valdomas daugiaprocesorinis prietaisas) prietaisas.

Nors šie įvairūs jutikliai, kontaktai ir kiti elektroniniai komponentai, o taip pat spausdintinės schemos ar kitos elektrinės jungtys, kuriomis jie yra sujungti tarpusavyje, yra visiškai inkorporuoti kortelės 1 korpuso viduje tokiu būdu, kad būtų apsaugoti nuo susidėvėjimo ir išorinio užteršimo, optimali vieta vidutinės srities 4 ribose tarp viršutinės srities 2 ir apatinės srities 3 dar labiau apsaugo juos nuo galimo sugadinimo įprastais magnetinių juostų skaitikliais, štampavimo aparatais ir spausdinimo įrenginiais, kurie mechaniškai kontaktuoja su visomis šiomis sritimis.

Šviesos diodai

Šviesos diodai 9a, 9b yra valdomi apsaugos procesoriaus 8 ir suteikia naudotojui vizualią grįžtamąją informaciją. Šiame iliustruotame pavyzdyje jie yra išdėstyti apatinėje srityje 3 optimaliu atveju ties tuo kortelės kraštu, kuris yra toliausiai nuo kontaktų 5. Bet kuriuo atveju šviesos diodai 9a, 9b yra išdėstyti ten, kur jie nebus sugadinti štampavimo metu ir kur jie bus matomi, kuomet kortelė yra įkišta į įprastą ISO SmartCard skaitytuvą ir/arba kuomet naudotojo pirštas yra uždėtas ant pirštų atspaudų jutiklio 6. Pavyzdžiui:

Patikrinimo režime:

- mirksi RAUDONAS: laukia, kol bus uždėtas pirštas
- nustojo mirksėti: pirštas uždėtas ant jutiklio
- RAUDONAS mirkteli kartą: negali palyginti, galima pajudinti pirštą
- ŽALIAS mirkteli kartą: palyginta, OK, galima nuimti pirštą

Registravimo režime:

- ŽALIAS mirksi: laukia, kol bus uždėtas pirštas
- nustojo mirksėti: pirštas uždėtas ant jutiklio
- RAUDONAS mirkteli kartą: negali užregistruoti, galima pajudinti pirštą
- ŽALIAS mirkteli kartą: užregistruota, OK, galima nuimti pirštą

Ištrynimo režime:

- ŽALIAS ir RAUDONAS mirksi: pasiruošęs ištrinti
- ŽALIAS mirkteli kartą: ištrinta

Optimaliu atveju naudotojui leidžiama daug kartų uždėti pirštą ant jutiklio tam, kad būtų sėkmingai atliktas palyginimas ar užregistravimas, prieš perduodant neigiamą pranešimą. Viename iš realizavimo variantų neigiamas pranešimas išduodamas tik tuomet, jei naudotojas nuėmė pirštą, nesulaukęs žalio OK signalo, arba jei viršytas iš anksto nustatytas laiko limitas. Toks procesas ne tik išmoko naudotoją tinkamai uždėti pirštą virš jutiklio, kas ne tik supaprastina skaičiavimą, bet taip pat leidžia panaudoti labiau diferencijuotus slenksčius. Šis vizualus grįžtamasis ryšys leidžia psichologiškai atskirti nepatyrusį naudotoją (kuris dažniausiai bandys tiek kartų, kol tinkamai uždės pirštą virš jutiklio) nuo apgaviko (kuris dažniausiai nenori atkreipti dėmesį ir išeis, kol jo piktavališki ketinimai nėra

atskleisti). Galutinis rezultatas yra žymiai sumažintų klaidingų neigiamų ir/arba klaidingų teigiamų rezultatų tikimybė.

Fig.2 pateiktas pavyzdinis procesas, skirtas padėti naudotojui uždėti pirštą ant jutiklio 6. Padėtyje, kurioje yra blokas 10, raudonasis šviesos diodas 9b mirksi. Kuomet pirštas yra aptiktas (blokas 11), šviesos diodas nustoja mirksėjęs ir atliekamas (blokas 12) vaizdo kokybės testas (nustatomos pailgos sritys, atitinkančios piršto odos iškilimams ir įdubimams). Jei kokybė yra prasta (NE atšakoje 13), vienas raudono šviesos diodo 9b mirktelėjimas instruktuoja naudotoją perkelti savo pirštą į kitą padėtį (blokas 14); priešingu atveju (TAIP atšakoje 15) atliekamas antrasis testas (blokas 16), siekiant nustatyti, ar tas pats pirštas, kuris buvo panaudotas užregistruoti naudotoją, uždėtas toje pačioje vietoje taip, kad santykinai paprastas palyginimo algoritmas galėtų patikrinti, ar gyvi duomenys atitinka tam tikrose ribose įrašytus į atmintį duomenis, tokiu būti įsitikinant, kad gyvas pirštas yra tas pats pirštas, kuris ir buvo užregistruotas (TAIP atšakoje 17), ir aktyvuojamas žalias šviesos diodas 9a (blokas 18) laikotarpį (blokas 19), kurio pakanka įsitikinti, kad palyginimas buvo atliktas sėkmingai ir naudotojas dabar gali nuimti savo pirštą. Alternatyviai, jei palyginimas neatitiko nustatytų ribų (NE atšakoje 20), vienas raudono šviesos diodo 9b mirktelėjimas instruktuoja naudotoją perstatyti pirštą į kitą vietą, ir procesas pakartojamas.

Tinklo struktūrų pavyzdžiai

Fig.3 pavaizduotas vienas galimas biometrinės verifikavimo sistemos, galinčios atlikti tiek vietinį, tiek nuotolinį asmens, pateikiančio saugią identifikavimo kortelę, realizavimo variantas. Ji susideda iš trijų pagrindinių komponentų: kliento terminalo 21, programų serverio 22 ir autentiškumo nustatymo serverio 23. Kliento terminalas 21 gyvai nuskaito ir apdoroja naudotojo pirštų atspaudus, užšifravimo apdorotus duomenis ir saugiai, optimaliu atveju internetu, naudojant IP/TCP adresavimo schemą ir ryšio protokolą, susisiekia su taikomąja ir autentiškumo nustatymo serverio, apsaugotomis nuo nesankcionuoto priėjimo įprastomis IP užkardomis 24. Kituose realizavimo variantuose užkardos 24 gali turėti filtrus ir šifravimo/dešifravimo įrenginius, kurie užšifruoja patikrintus perduotus duomenis, paverčiant juos autorizuotais duomenimis, ir kurie dešifruoja priimtus duomenis prieš įsitikinant, ar tai iš tikrųjų yra autorizuoti duomenys, naudojant, pavyzdžiui, tokį šifravimo algoritmą, kaip DES128. Šiomis priemonėmis užkarda 26 gali atskirti

autorizuotus duomenis nuo galimai piktavališkų ne tik pagal pranešimo antraštę, bet taip pat ir pagal pranešimo turinį.

Kliento terminalas 21 gali būti įgyvendintas kaip dedikuotasis tinklo įrenginys arba gali būti realizuotas programoje, instaliuotoje programuojamame stacionariame ar portatyviame kompiuteryje ar kitoje darbinėje stotyje ar asmeniniame kompiuteryje, turinčiame įprastas Windows XXX, OS X, Solaris XX, Linux ar Free BSD operacines sistemas. Optimaliu atveju kliento terminalas 21 turi naujausias "neigiamas" duomenų bazes (pavyzdžiui, sąrašą pamestų ar pavogtų kortelių, kortelės ar kortelių grupės suvaržymų sąrašą), kurios suteikia papildomas apsaugos priemones.

Programų serveris 22 atlieka transakcijas ar kitaip atsako į nutolusio naudotojo, esančio prie naudotojo terminalo 21, instrukcijas po to, kai autentifikavimo nustatymo serveris 23 patvirtino naudotojo tapatybę. Autentifikavimo serveris 23 saugiai susisiekia tiek su kliento terminalu 21, tiek su programų serveriu 22, autentiškų pirštų atspaudų duomenų ir kitos informacijos, susijusios su anksčiau registruotais naudotojais, įrašymui į atmintį, įrašytų į atmintį duomenų palyginimui su užšifruotais gyvais duomenimis, gautais iš kliento terminalo 21, ir programų serverio 22 informavimui apie tai, ar nurodyti pirštų atspaudai sutampa ar nesutampa su įrašytais į atmintį pirštų atspaudais.

Kalbant konkrečiau, kliento terminalas 21 papildomai turi du pagrindinius komponentus: fiksuotą kortelių skaitytuvą 25, turintį interneto naršyklės terminalą 26, kortelės skaitytuvo sąsają 5a (kuri gali būti paprastas USB kabelis, kurio gale įrengti elektros kontaktai, sudarantys jungtį sujungimui su ISO SmartCard kortelės kontaktais 5) ir portatyvų SmartCard kortelės komponentą 1'. Viename realizavimo variante portatyviu komponentu 1' gali būti anksčiau aprašytoji SmarCard kortelė 1, turinti pirštų atspaudų jutiklį 6, apsaugos procesorių 8 ir ISO SmartCard kortelės procesorių 7.

Programų serveris 22 dar turi interneto serverio sąsają, turinčią užkardą 24 ir interneto naršyklę 27, o taip pat transakcijų modulį 28 ir validavimo modulį 29. Tuo atveju, jei programų serveris ir programų modulis 28 yra prietaisai, kurie nėra skirti susisiekti išoriškai IP/TCP protokolu, užkarda 24 gali būti pakeista atitinkamu protokolo konverteriu, turinčiu validavimo modulį 29 ir fiksuotą IP adresą. Programų serveris gali būti valdomas, pavyzdžiui, trečiąja šalimi, kuri siekia pateikti paslaugą internetu įgaliotam naudotojui.

Autentifikavimo serveris 23 dar turi interneto serverio sąsają 30, apdorojimo modulį 31, turintį pirštų atspaudų palyginimo algoritmą 32, ir duomenų bazę 33 pirštų atspaudų ir kitos autentiškos informacijos, surinktos iš naudotojų jų užsiregistravimo sistemoje metu, saugojimui, duomenys skirti tik sistemos darbui. Saugumo sumetimais kiekvieno asmens duomenys nėra įrašyti programų serveryje kaip paprasta informacijos seka, bet kiekvienas įrašas yra įrašytas atskirai ir bet kokie reikalingi indeksai ar ryšiai, susiejantys šiuos įrašus, yra pasiekiami tik atitinkamu raktu, kuris sudaro dalį asmens privačių duomenų autentifikavimo serveryje.

Vieta

Tam tikruose realizavimo variantuose fiksuotas skaitytuvas 25 ir/arba portatyvi kortelė 1" gali turėti įrengtą integruotą pasaulinio padėties nustatymo palydovo (Global Positioning Satellite - GPS) imtuvą 34, kuris gali suteikti naudingos informacijos apie skaitytuvo ir kortelės dabartinę padėtį konkrečiu ar maždaug tuo metu, kai buvo atliktas konkretus veiksmas. Konkrečiai, padėties duomenys iš GPS imtuvo 34 gali būti panaudoti skaitytuvo ir/arba kortelės išjungimui (nuolatinai arba laikinai), jei kuris nors iš jų yra perkeltas į vietą, kurioje jų panaudojimas nėra autorizuotas. Taip pat padėtis gali būti automatiškai nustatyta kitomis nei GPS priemonėmis, pavyzdžiui, naudojant PHS (Japonijos mobilus telefonas) skambinančiojo vietos nustatymo technologiją, arba vietos nustatymo jutiklius, reaguojančius į vietinius žemės elektromagnetinių laukų pokyčius. Jei kortelė turi GPS imtuvą, įvairūs GPS komponentai, įskaitant anteną, signalo stiprintuvą, A/D konverterį ir skaitmeninį procesorių, skirtą apskaičiuoti padėtį, sudaro dalį vienos integrinės grandinės arba yra atskiri prietaisai, sumontuoti vienoje plokštėje, kuri yra padaryta išvien su kortelės korpusu, įmontuota jame arba laminuota kartu su juo.

ISO kortelės su įrengta joje palyginimo funkcija struktūra

ISO procesoriaus sąsajos

Fig.4 yra pavyzdinės suderinamos su ISO SmartCard kortele biometrinio verifikavimo kortelės 1 arba 1' su skirtingais fizinių duomenų takais, skirtais panaudoti pirminio kortelės turėtojo biometrinių duomenų nuskaitymo ir kortelės

turėtojo asmens tapatybės patikrinimo duomenų persiuntimo nuotoliam apdorojimui metu, funkcinė blokinė schema

Be jau anksčiau aprašytųjų ISO procesoriaus 7, apsaugos procesoriaus 8, pirštų atspaudų jutiklio 6, šviesos diodų 9a, 9b ir neprivalomo GPS imtuvo 34, kuomet tik ISO procesorius 7 yra tiesiogiai prijungtas prie kortelės skaitytuvo 25 ISO SmartCard kontaktais 5, čia yra parodytas atskiras įkrovimo terminalas 35 ir su juo susieta laikina jungtis 36, kuri suteikia tiesioginį ryšį su apsaugos procesoriumi 8 pirminės naudotojo registracijos metu. Reikia pastebėti, kad ISO procesorius 7 susisiekia su apsaugos procesoriumi 8 I/O prievadais 37, 38, tuo tarpu laikina įkrovimo jungtis 36 yra prijungta prie atskiro I/O prievado 39. Apsaugos procesorius optimaliu atveju yra užprogramuotas taip, kad bet kurie svarbūs ir susiję su apsauga duomenys ar programinė įranga yra pasiekiami tik iš prievado 39, bet ne iš prievadų 37 ir 38, tokiu būdu apsisaugant nuo bet kokių galimų piktavališkų bandymų pasiekti šiuos svarbius duomenis po to, kai yra atjungta jungtis 36.

Populiariausi ISO procesoriai turi mažiausiai du I/O prievadus, kai kurie turi mažiausiai tris. Tik vienas iš šių prievadų (I/O 1) yra skirtas įprastos SmartCard kortelės serijinių duomenų jungties 5 prijungimui prie išorinio ISO suderinamo kortelės skaitytuvo 25. Vienas arba du papildomi I/O prievadai optimaliu atveju suteikia dedikuotąjį laidinį ryšį tarp ISO procesoriaus 7 ir apsaugos procesoriaus 8, kuris veikia kaip aparatinė užtvara, skirta užblokuoti bet kokius piktavališkus bandymus perprogramuoti apsaugos procesorių 8 ar prieiti prie bet kokios svarbios informacijos, kuri galėjo būti anksčiau nuskaityta jutikliu 6 ar kitokiu būdu išsaugota procesoriuje 8. Šiuo konkrečiu atveju, kuomet ISO procesorius turi daugiau kaip dvi I/O linijas, yra galima pateikti daugiau nei du statinio statuso informacijos būvius dedikuotame ryšio take tarp ISO procesoriaus ir apsaugos procesoriaus, tokius kaip: 1) Pasiruošęs, 2) Užimtas 3) Klaida ir 4) Atlikta, net ir tuomet, kuomet apsaugos procesorius yra visiškai atjungtas nuo maitinimo. Žinoma, net jei yra tik vienas I/O prievadas, šios keturios sąlygos gali būti persiųstos dinamiškai kaip serijiniai duomenys.

Galimos komandos ir duomenys, kurie gali būti perduoti tarp ISO CPU ir apsaugos CPU ISO sąsajomis I/O2 ir I/O 3, yra šie:

- Komandos užregistruoti ar nustatyti naudotojo tapatybę, pagal kurias apsaugos CPU nusiųs užregistravimo ar autentifikavimo rezultatą vietiniam saugojimui ir/arba persiųs nuotoliniam pritaikymui.
- Pirštų atspaudų informacija kaip šablonas (nuoroda) gali būti išsiųsta iš apsaugos CPU į ISO CPU išsaugojimui ISO SmartCard kortelės atmintyje paskesniam perdavimui nuotoliniams panaudojimams.

Įkrovimo jungtis 36 suteikia tiesioginį ryšį su apsaugos CPU 8, kuris apeina bet kokią užkardą, suteiktą ISO jungčiai ir susietiems dedikuotiems I/O prievadams 37 ir 38, tuo pat metu palaikant ryšį tarp ISO CPU 7 ir ISO skaitytuvo 25 taip, kad maitinimą gaus ir apsaugos CPU 8. Tai pirmiausia yra naudojama pirminės kortelės priregistravimo konkrečiam naudotojui metu, ir turėtų apsaugoti nuo neleistino priėjimo.

Fig.5 parodytas alternatyvus fig.4 pavyzdinės biometrinio verifikavimo kortelės, kuri yra numatyta panaudojimui su nemodifikuotu ISO Smartcard kortelės CPU, realizavimo variantas. Konkrečiai, ISO CPU 7' daugiau nebeprivalo atlikti jokių tinklo sąsajos funkcijų tarp kortelės skaitytuvo 25 ir apsaugos CPU 8', tiek normalaus naudojimo ar įkrovimo metu, ir, tokiu būdu, jis gali būti bet kokia ISO patvirtinta mikroschema, jokiu būdu nemodifikuota ir naudojama tik būdu, kuris yra absoliučiai prieinamas tiek kortelės skaitytuvui 25, tiek bet kokiam išoriniam panaudojimui. Šiame realizavimo variante apsaugos CPU 8' veikia kaip vaiski užtvara tarp ISO CPU 7' ir bet kokio išorinio panaudojimo, jei nuskaityti pirštų atspaudai atitinka saugomus duomenis, ir blokuoja visus ryšius, jei nuskaityti pirštų atspaudų duomenys nesutampa su saugomais duomenimis.

Kortelės inicializavimas ir įrašytų duomenų apsauga

Pagal vieną realizavimo variantą originali kortelė turi išsikišantį spausdintinės schemos tęsinį, kuris leidžia ją tiesiogiai sujungti su apsaugos CPU, o taip pat su ISO sąsajų dalimis ir/arba su bet kokia atskira kortelės atmintimi. Ši tiesioginė sujungimo sąsaja yra naudojama tik kortelės testavimui ir pirštų atspaudų užregistravimui ir turi signalą, kuris leidžia atlikti registracijos procesą. Užbaigus registraciją, schemos tęsinys yra mechaniškai nukerpamas taip, kad nebūtų galima atlikti jokios paskesnės registracijos, ir apsaugos CPU atmintį

pasiekti galima tik per ISO CPU ir anksčiau minėtą užkardą tarp ISO CPU ir apsaugos CPU.

Saugiklis

Pagal kitą realizavimo variantą apsaugos CPU turi tokios rūšies atmintį, kuri, užregistravus pirštų atspaudus, tampa nebepasiekiama. Vienas tokios atminties pavyzdys yra vienkartinė PROM ("OTP") atmintis, kurios konstrukcija yra panaši į EEPROM atmintį, bet yra nepralaidi UV spinduliams ir todėl negali būti ištrinta. Kitas pavyzdys yra Flash ROM atmintis, kuri po registracijos procedūros padaroma skirta tik nuskaitymui, paduodant, pavyzdžiui, pakankamai srovės į teisės suteikimo, adreso ar duomenų signalo taką, suformuojant fizinį pertrūkį ("saugiklį") šiame signalo take.

Autentifikavimo proceso pavyzdys

Pagal vieną išradimo realizavimo variantą autentifikavimo procesas apima pirštų atspaudų fizinių duomenų nuskaitymą, naudojant, pavyzdžiui, optinį, slėgio, laidumo, talpumo, akustines, elastines ar fotografines technologijas kliento terminale, kuriuo naudojasi asmuo, siekiantis susisiekti su programų serveriu, kurie yra vėliau nusiunčiami (optimaliu atveju – užšifruotos formos) į atskirą pirštų atspaudų autentifikavimo serverį. Pirštų atspaudų autentifikavimo serveris palygina nuskaitytus pirštų atspaudų duomenis su rinkmenoje esančiais užregistruotais naudotojo pirštų atspaudų duomenimis, naudojant autentifikavimo programinę įrangą, ir, jei duomenys sutampa, autentifikavimo serveris nusiunčia instrukcijas, leidžiančias atlikti veiksmą, į programų serverį.

Pagal kitą realizavimo variantą naudotojas pasiekia saugią pirštų atspaudų autentifikavimo serverio tinklo naršyklę, kurioje yra pirštų atspaudų duomenų rinkmenos, kur visi pirštų atspaudai yra iš anksto užregistruoti kartu su asmens duomenimis, tokiais, kaip vardas, pavardė, adresas ir gimimo data. Po to saugus pirštų atspaudų autentifikavimo serveris, kurią naudotojas pasiekia saugiu protokolu, tokiu, kaip HTTPS formatas, nusiunčia į kliento terminalą instrukcijas nuskaityti naudotojo pirštų atspaudus. Atsiliepdamas į kliento terminalo naršyklės atvaizduotas instrukcijas, naudotojas uždeda pasirinktą pirštą ant pirštų atspaudų jutiklio, ir pirštų atspaudų nuskaitymo programa, esanti kliento terminale, nuskaito

pirštų atspaudus skaitmeniu būdu, pavyzdžiui, kaip 25-70 mikronų pikselių 12,5-25 mm^2 plote 8 bitų pilko atspalvio vaizdą.

Saugus pirštų atspaudų autentifikavimo serveris priima pirštų atspaudų duomenis kartu su naudotojo ID, o taip pat interneto IP adresu ir/arba pirštų atspaudų jutiklio individualiu kodu (MAC adresu), ir/arba "slapuku", ir/arba unikaliu kodu ar kita informacija, identifikuojančia atskirą asmenį ar terminalą (pavyzdžiui, detales iš ankstesnio pokalbio tarp kliento terminalo ir saugaus pirštų atspaudų autentifikavimo serverio), po ko ji palygina priimtus pirštų atspaudų duomenis su pirštų atspaudais, esančiais rinkmenoje, kuri yra iš anksto užregistruoti pirštų atspaudų duomenys kartu su naudotojo ID, asmens informacija, tokia, kaip vardas, pavardė, adresas, gimimo data, žinios apie teistumą, vairuotojo pažymėjimas, socialinio draudimo pažymėjimo numeris, t.t., naudojant autentifikavimo programą, tai gali būti detalusis ar greitasis Fourier transformacijos palyginimas.

Autentifikavimo proceso pradžioje tinklo serveris 27 instruktuoja naudotoją vaizdu ar garsu uždėti savo pirštą ant pirštų atspaudų nuskaitymo jutiklio 6 ir nuspausti pelės ar klaviatūros mygtuką tam, kad būtų inicijuota pirštų atspaudų nuskaitymo programa apsaugos procesoriuje 8. Tuomet nuskaityti naudotojo pirštų duomenys yra nusiunčiami užšifruotame formate (pavyzdžiui, naudojant saugų RSA užšifruotą perdavimo protokolą HTTPS) į pirštų atspaudų autentifikavimo serverio 23 tinklo serverį 30 per kliento terminalo 21 ISO procesorių 7 ir tinklo naršyklę 26. Jei nuskaityti duomenys sutampa su atitinkamais duomenimis duomenų bazėje 33, pirštų atspaudų autentifikavimo serveris 23 suteikia naudotojui prieigą prie kliento terminalo 21 ir programų serverio 22.

Optimalaus realizavimo varianto, naudojant trijų pakopų autentifikavimo protokolą ir vienkartinį slaptažodį kaip atsitiktinių ženklų šifravimo seką, pavyzdys bus dabar aprašytas su nuoroda į fig.3:

- Kliento terminalo 21 tinklo naršyklė 26 nukreipia į atitinkamą programų serverio 22 tinklo sąsają 27 prašymą pasiekti taikomąjį procesą (modulį) 28.
- Atsakydama programų serverio 22 tinklo sąsaja 27 pateikia LOG-IN (užsiregistravimo) informaciją ir atitinkamas taikomojo proceso 28 atlikimo instrukcijas.
- Kliento terminalas 21 instruktuoja ISO procesorių 7 aktyvuoti apsaugos procesorių 8.

- ISO procesorius 7 aktyvuoja apsaugos procesorių 8.
- Apsaugos procesorius 8 laukia pirštų atspaudų duomenų iš pirštų atspaudų jutiklio 6, ir kuomet yra gauti tinkami duomenys, pateikia skaitmeninį pirštų atspaudų raštą, kuris yra persiunčiamas į tinklo naršyklę 26 per ISO procesorių 7.
- Tinklo naršyklė 26 nusiunčia užšifruotą pateiktų pirštų atspaudų rašto versiją į autentifikavimo serverį 23 kartu su informacija, susijusią su panaudota kortele 1' ir kortelės skaitytuvu 25, tokia, kaip naudotojo ID, kliento terminalo 21 adresas ir/arba jutiklio 6 ID kodas (MAC adresas).
- Autentifikavimo serverio 23 tinklo sąsaja 30, gavusi pateiktą pirštų atspaudų raštą kartu su kita kliento terminalo 21 informacija, persiunčia šią informaciją pirštų atspaudų palyginimo procesoriui 31.
- Pirštų atspaudų palyginimo procesorius 31, valdomas palyginimo programos 32, naudoja gautą naudotojo ID ar kitą naudotoją apibūdinančią informaciją, siekiant surasti atitinkamą pirštų atspaudų raštą duomenų bazėje 33, ir palygina nuskaitytą pirštų atspaudų raštą su konkrečiu pirštų atspaudų raštu.
- Rezultatas (sutapęs ar nesutapęs) yra išsaugojamas priėjimų archyve kartu su kita informacija, identifikuojančia terminalą 21, naudotojo ID, kortelę 1' ir užklausiusįjį taikomąjį procesą 28, o atsakymas yra grąžinamas autentifikavimo serverio tinklo sąsajai 30.
- Jei rezultatas sutapo, autentifikavimo serverio tinklo sąsaja 30 generuoja vienkartinį ženklų sekos pavidalo užklausos slaptažodį, kuris yra perduodamas į kliento terminalą 21, ir naudoja šią užklausos ženklų seką kaip atsitiktinių ženklų kodą susijusios informacijos užšifravimui, kurią ji išsaugo kaip atitinkamą atsakymą į užklausą galimiems būsimiems veiksmams.
- Kliento terminalas 21 naudoja priimtą užklausos ženklų seką kaip atsitiktinių ženklų kodą anksčiau išsaugotos susijusios informacijos neužšifruotos kopijos užšifravimui, kurią jis po to persiunčia į programų serverio 22 tinklo sąsają 27 kaip dalį savo atsakymo į Log-In (užsiregistravimo) procesą.
- Programų serverio 22 tinklo sąsaja 27, gavusi konvertuotą į atsitiktinius ženklus susijusią informaciją, persiunčia ją į taikomąjį procesą 28, kuris susieja ją su bandymu užsiregistruoti iš kliento serverio, o sutapusio rezultato patvirtinimui persiunčia gautą susijusią informaciją, kuri buvo kliento terminalu paversta

atsitiktiniais ženklais, naudojant užklausos seką, pateiktą autentiškumo nustatymo serverio kaip atsakymas į užklausą.

- Autentiškumo nustatymo serverio 23 tinklo sąsaja 30, gavusi atsakymą į užklausą iš programų serverio, persiunčia jį autentifikavimo procesui 31, kuris palygina jį su anksčiau išsaugota tikėtino atsakymo į užklausa kopija, siekiant nustatyti, ar naudotojas yra faktiškai identifikuotas.
- Bet kokia identifikuota naudotojo informacija, gauta iš šio palyginimo, yra po to gražinama taikomajam procesui 28 per autentifikavimo serverio tinklo sąsają 30 ir programų serverio 22 validavimo modulį 29.
- Validavimo modulis 29 naudoja autentifikavimą naudotojo tapatumui, nustatytam pradiniame bandyme užsiregistruoti, patvirtinti.
- Patvirtinus naudotojo tapatumą, taikomasis procesas 28 susisiekia tiesiogiai su kliento terminalo 21 tinklo naršykle 26 per programų serverio 22 tinklo sąsają 27.

Fig.6 pateiktas alternatyvus autentifikavimo proceso variantas, kuriame palyginimas yra apsaugos CPU atliekamas ISO suderinamoje kortelėje, pavaizduotoje fig.4, ir nenaudojamas joks išorinis autentifikavimo serveris 23. Kairė fig.6 pusė rodo funkcijas, kurias atlieka programų serveris 22, o dešinė pusė rodo funkcijas, kurias atlieka ISO SmartCard kortelė 1.

Kuomet SmartCard kortelė yra įdėta į kortelės skaitytuvą 25, pirminės padėties nustatymo signalas RST yra nusiunčiamas iš kortelės skaitytuvo ir į ISO CPU (START blokas 40), ir į apsaugos CPU 8 (pirštų atspaudų verifikavimo blokas 41), ir abu gauna maitinimą VCC iš kortelės skaitytuvo 25. Po to ISO CPU atsako ATR (Answer-to-Reset - atsakymas į pirminės padėties nustatymo signalą) pranešimu ir susisiekia su PPS (Protocol and Parameters Selection - protokolo ir parametrų pasirinkimas), jei reikia (blokas 42). Tuo pat metu apsaugos CPU pereina į laukimo būvį ir laukia pirštų atspaudų duomenų, ir, kuomet duomenys yra gauti iš jutiklio 6, atlieka autentifikavimo procesą (blokas 43).

Kuomet taikomasis procesas 28 išsiunčia pirminį prašymą į ISO CPU 7 (blokas 44), ISO CPU užklausia (blokas 45) apsaugos procesorių apie autentifikavimo statusą. Jei atsakymas yra teigiamas, ISO CPU reaguoja į taikomojo modulio prašymą, vykdydamas komandą (blokas 46). Priešingu atveju

(gavęs klaidos pranešimą arba negavęs jokio atsakymo iš apsaugos CPU 8), jis nereaguoja, bet laukia naujo pirminio prašymo (blokas 44b).

Jei pirštų atspaudai buvo verifikuoti, o pirmasis atsakymas buvo gautas laiku ir nustatyta, kad taikomasis modulis 28 turi į jį reaguoti (blokas 47), atsakymo į prašymą procesas tęsiamas (blokai 48, 49, 50) tol, kol bus viršyta iš anksto nustatyta verifikavimo pertrauka, kurios metu jokių prašymų nebuvo gauta iš taikomojo modulio (blokas 51) ar taikomasis modulis negavo laukiamo atsakymo (blokas 52).

Fig.7 yra diagrama, panaši į fig.6, bet modifikuota naudojimui su biometrinio verifikavimo kortele, pavaizduota fig.5. Kairioji fig.7 pusė rodo funkcijas, kurias atlieka programų serveris 22, sekantis stulpelis reiškia skaitytuvą 25, kitas stulpelis vaizduoja ISO kontaktus 5, kitas stulpelis rodo funkcijas, kurias atlieka apsaugos CPU 8, o dešinioji pusė rodo funkcijas, kurias atlieka nemodifikuotas ISO SmartCard kortelės CPU 7:

- Kuomet SmartCard kortelė yra įdėta į kortelės skaitytuvą arba taikomoji programa aktyvuoja kortelės skaitymo prietaisą, pirminės padėties nustatymo signalas 53 iš kortelės skaitytuvo 25 yra nusiunčiamas į apsaugos CPU 8.
- Iš karto po to, kai apsaugos CPU gauna pirminės padėties nustatymo signalą 53, jis nusiunčia atitinkamą pirminės padėties nustatymo signalą 54 į ISO CPU 7. Tuo pačiu metu apsaugos CPU laukia pirštų atspaudų duomenų iš pirštų atspaudų jutiklio.
- Gavęs pirminės padėties nustatymo signalą 54, ISO CPU paruošia ATR (atsakymą į pirminės padėties nustatymo signalą) atsakymą 55 ir po to susisiekia su PPS (protokolo ir parametrų pasirinkimas), jei reikia.
- Kai apsaugos CPU 8 gauna ATR (atsakymą į pirminės padėties nustatymo signalą) signalą iš ISO CPU, jis perduoda jį kortelės skaitytuvui (blokas 56), įskaitant bet kokas susijusias komandas.
- Tuo pat metu, jei apsaugos CPU gauna pirštų atspaudų duomenis, jis pradeda vykdyti anksčiau aprašytą autentifikavimo procesą. Jei autentifikavimo testo rezultatas yra teigiamas (PASS), šis statusas yra išlaikomas tam tikrą laikotarpį. Jei rezultatas yra neigiamas (FAIL), - apsaugos CPU 8 laukia naujų pirštų atspaudų duomenų.

- Pradėjus vykdyti komandą, komanda 57 nusiunčiama į apsaugos CPU, kuris nusiunčia komandą 58 į ISO CPU ir taip pat nusiunčia jo tikslų atsakymą 59 į kortelės skaitytuvą tik tuomet, jei apsaugos CPU statusas vis dar yra teigiamas (PASS) arba jei paskutinis teisingas atsakymas turėjo didesnį duomenų bitų rinkinį (testavimo blokas 60).
- Priešingu atveju (nėra atšakos 61) apsaugos CPU generuoja netikrą užklausą 62 ir nusiunčia ją į ISO CPU ir taip pat nusiunčia gautąjį ERR atsakymą 63 į taikomąjį procesą 28 per kortelės skaitytuvą 208, tokiu būdu palaikant tinkamą sinchronizaciją tarp sekos numerių užklausose ir atsakymuose.

Šifravimas ir apsauga

Prieš persiunčiant duomenis bet kokiu išoriniu tinklu, visi svarbūs duomenys ir/arba autentifikavimo rezultatai yra užšifruojami, jei įmanoma, - naudojant DES ar TwoFish šifravimą. Šifravimo raktas yra pagrįstas nuskaitytais ar išsaugotais pirštų atspaudų duomenimis, naudotojo ID kodu, jutikliui priskirtu unikaliu kodu, atminties adresu, gretimais duomenimis atmintyje, kitais funkciškai susijusiais duomenimis, ankstesne konversija (transakcija), IP adresu, terminalo kodu arba suteiktu slaptažodžiu. Arba, alternatyviai, svarbūs duomenys gali būti persiųsti internetu, naudojant saugų HTTPS protokolą.

Siekiant užtikrinti geresnį saugumą, virtuali privati tinklų sąsaja, tokia kaip aparatinis DES užšifravimas ir dešifravimas, gali būti įterptas tarp saugaus pirštų atspaudų autentifikavimo serverio ir prisijungimo prie tinklo vietos, ir atitinkamai tarp programų serverio ir prisijungimo prie tinklo vietos. Naudojat tokią virtualią tinklo sąsają ar virtualų privatų tinklą VPN (Virtual Private Network), svarbūs duomenys yra papildomai apsaugoti papildomu šifro sluoksniu, pavyzdžiui, ir DES 128 (paprastai naudojamu virtualiame privačiame tinkle VPN), ir RSA (kurį naudoja HTTPS).

Ypač saugiems atvejams visi ryšiai gali būti apvynioti papildomais apsaugos sluoksniais. Konkrečiai, pranešimų antraštės apatiniame sluoksnyje gali būti užšifruotos viršutiniame sluoksnyje.

Belaidis ryšis

Kituose realizavimo variantuose gali būti numatyta dviguba sąsaja darbui tiek kontaktiniu (ISO 7816), tiek belaidžiu (ISO 1443 A arba B) būdu, ir optimaliu atveju ji turi daugiasąsajinį maitinimo įtaisą, kuri užtikrina veikimą tarp ISO 7816 kontaktinės, ISO 1443 A, ISO 1443 B, ISO 15693 ir HID belaidžių sistemų (tarp kitų) vienoje kortelėje. Taip pat kortelėje gali būti numatyta galimybė kitų belaidžio ryšio technologijų, tokių kaip Bluetooth (trumpo diapazono) ar mobilaus ryšio (vidutinio diapazono), ar mikrobangų (ilgo diapazono), panaudojimui.

Fig.8 pavaizduota biometrinio verifikavimo SmartCard kortelė, kuri gali būti prijungta prie vietinio terminalo belaidžiu būdu arba elektrine jungtimi. Didžiąja dalimi jos struktūra ir konstrukcija yra panaši į anksčiau aprašytąją kortelę, pavaizduotą fig.1, ir panašūs elementai pažymėti tais pačiais skaitmenimis. ISO CPU 7 yra įrengtas kitoje vietoje po kontaktais 5, bet atlieka panašią anksčiau aprašytą funkciją.

ISO antena 64 turi dvi kilpas, paprastai įrengtas ties kortelės 1 periferiniu kraštu, ir užtikrina ISO suderinamą belaidį ryšį su ISO CPU 7 duomenų perdavimui ir maitinimo padavimui, panašiai kaip ir elektrinė jungtis 5. Be to, apsaugos antena 130 (įrengta, aprašytame pavyzdyje, antenos 64 viduje ir sudaryta tik iš vienos kilpos), sudaro atskirą apsaugos CPU 8 maitinimo šaltinį per DC-DC įtampos reguliatorių 66. Kadangi šiuo atveju nėra tiesioginės belaidės jungties, išskyrus ISO CPU 7, nėra pavojaus apsaugos CPU 8 saugomų svarbių duomenų iškraipymui belaide sąsaja. Alternatyviai, kaip minėta anksčiau, kalbant apie realizavimo variantus, turinčius tik laidines jungtis su išoriniu skaitytuvu ir išoriniu tinklu, dviejų procesorių veikimas gali būti apjungtas arba išorinis ryšys gali būti užtikrintas per apsaugos CPU 8, o ne ISO CPU 7, šiuo atveju atitinkamos belaidės apsaugos priemonės turi būti inkorporuotos į tokiu būdu modifikuotą kortelės struktūrą.

Fig.9 yra fig.8 pavaizduotos kortelės skerspjūvio vaizdas. Didžioji dalis aprašytųjų komponentų yra įrengta centrinėje šerdyje 67, ir tik kontaktai 5 išlenda pro viršutinį apsauginį sluoksnį 68. Jutiklio 6 funkcinis paviršius pasiekiamas pro viršutinį langą viršutiniame sluoksnyje 68 ir apatinį langą, esantį PCB 69, kuris yra įrengtas tarp viršutinio sluoksnio 68 ir centrinės šerdies 67 ir kuris užtikrina elektrinį sujungimą tarp įvairių elektroninių komponentų ir elektrostatinės iškrovos kontakto, dengiančio jutiklio 6 aktyvią sritį.

Taip pat yra matomi apatinis sluoksnis 70 ir magnetinė juostelė 71.

Pirštų atspaudų jutiklis

Fig.10 pateikta jutiklio 6 schema, kurioje jutiklio elementų 73 matrica 72 yra suformuota iš eilučių 74 ir stulpelių 75. Kaip pavaizduota fig.10, kiekvienas elementas 73 turi aktyvų įėjimą 76 ir keitiklį 77. Pirštų atspaudai suformuojami piršto odos iškilimais ir įdubimais. Kiekvienas jutiklio elemento keitiklis 77 yra veikiamas mechaniškai ir/arba elektriškai, kuomet vienas iš šių piršto odos iškilimų betarpiškai liečia matricos 72 elementą 73, šis poveikis sukuria pirštų atspaudų vaizdą pagal mikroslėgių, kuriuos sudaro iškilimai ir įdubimai piršto gale, pokyčius skersai jutiklio paviršiaus. Nors kiekvienas keitiklis 77 yra pavaizduotas kaip atskiras kintamo talpumo kondensatorius, čia yra įrengta įvairių rūšių keitiklių, kurie gali reaguoti į vieną žmogaus odos iškilimą. Šiame konkrečiame spaudimui jautriame plonasluoksniame pjezokeitiklyje plėvelė yra deformuojama betarpiškai greta elemento ir generuoja krūvį, kuris yra išsaugomas kondensatoriuje, prijungtame prie šio elemento. Kondensatoriaus įtampa yra mechaninės įtampos, suformuotos pjezomedžiagos deformavimu, funkcija, kuri, savo ruožtu, yra funkcija, priklausanti nuo to, kas yra virš elemento: iškilimas ar įdubimas. Kuomet signalas iš susieto stulpelio tvarkykles 78 rodo, kad elemento įėjimas 76 yra aktyvuotas (ON), o susieta eilės tvarkyklė 79 yra įžeminta, išėjimo linijos 80 gale atsiranda įtampa, kuri yra konvertuojama į 8 bitų skaitmeninį signalą išėjimo tvarkyklėje 81. Siekiant padidinti pjezomedžiagos deformacijų aptikimą, pjezoelektrinė medžiaga gali būti suformuota ant elastinės medžiagos, tokios kaip poliimidas, arba gali paprasčiausiai būti poliimido pjezoelektrinė medžiaga. Kitos analoginės keitiklio technologijos, kurios gali būti įgyvendintos panašioje struktūroje, apima kintamas varžas ir kintamas talpines varžas. Alternatyviai, kiekvienas elementas gali būti sudarytas iš vieno skaitmeninio jungiklio, kuris suteikia tik vieną informacijos bitą. Šiuo atveju papildomi informacijos bitai gali būti generuoti, įrengiant daugiau elementų tame pačiame plote arba atrenkant kiekvieną elementą didesniu dažniu. Tokiame alternatyviame realizavimo variante nereikia jokių A/D konverterių.

Pateiktame realizavimo variante jutiklis yra tik 0,33 mm storio ir yra pakankamai atsparus susidėvėjimui, kad galėtų būti įrengtas SmartCard kortelėje, jo neveikia statinė elektra, naudotojo odos elementai ar sąlygos (drėgmė,

sausumas, šiluma, šaltis). Tipinis jutiklio 6 elemento ilgis yra nuo 25 iki 70 mikronų ir tipinis plotis - nuo 25 iki 70 mm. Šiame pavyzdyje pateikto jutiklio nuskaitymo sritis yra nuo 12,5x25 mm dydžio ir turi 8 bitų lygio jautrumą. Toks jutiklis gali būti pagamintas kaip TFT (plonasluoksnio tranzistoriaus) ir slėgiui jautraus kondensatoriaus matrica, suformuota, pavyzdžiui, iš plonasluoksnės pjezomedžiagos, tokios kaip titano bario oksidas ar stroncio bario oksidas, ir turi viršutinį elektrodą, kuris dengia ir apsaugo visą nuskaitymo sritį. Jei taikomas mechaninis poveikis, atitinkamas krūvis yra generuojamas ir išsaugomas plonasluoksniame pjezokondensatoriuje. Alternatyviai, slėgiui jautrus jutiklis gali būti pagamintas kaip TFT (plonasluoksnio tranzistoriaus), plonasluoksnio kondensatoriaus, slėgiui jautraus kondensatoriaus, suformuoto, pavyzdžiui, iš slėgiui laidžios medžiagos lakšto, tokios kaip gumos lakštas, disperguotas anglies pluoštu, metalu (tokiu kaip varis, alavas ar sidabras) padengtas anglies pluoštas ar stiklo pluoštas popieriaus pagrindu, ar elastinė medžiaga (tokia kaip silikonas), disperguota metalu, ir viršutinio elektrodo lakšto, kuris padengia visą nuskaitymo sritį, matrica.

Eilučių ir stulpelių tvarkyklėmis 79, 78 konkretus pirštų atspaudų jutiklio elementas 73 perduoda elektrinius duomenis į išvesties schemą 81, tokiu būdu konvertuodamas fizinę naudotojo pirštų atspaudų įvestį į analoginius elektrinius duomenis. Po to A/D konverteris išvesties schemoje 81 konvertuoja analoginį elektrinį signalą į skaitmeninį elektrinį signalą. Kiekvienas plonasluoksnis tranzistorius pasirinktinai sujungia bendrą eilučių tarpusavio jungtį su įtampa susietame su ja kondensatoriuje, tokiu būdu kiekvieno kondensatoriaus įtampa gali būti nuskaityta ir kiekvieno elemento deformacija gali būti išmatuota. Optimaliu atveju vienu metu yra sujungiamas visas plonasluoksnių tranzistorių stulpelis, ir tokiu būdu keli elementai (pavyzdžiui, 8) viename pasirinktame stulpelyje gali būti nuskaityti lygiagrečiai skirtingose eilučių tarpusavio jungtyse. Daugybės eilučių ir stulpelių sujungimas sumažina jungčių skaičių, o lygiagretus daugybės elementų iš skirtingų to paties stulpelio eilučių nuskaitymas sumažina visos matricos nuskaitymo laiką. Jutiklio išvesties įtampa gali būti sustiprinta kitu stiprintuvu. Tokio stiprintuvo išvestis gali būti panaudota analoginio signalo konversijai į skaitmeninį (A/D konverteryje).

Substratu gali būti stiklas (toks kaip nešarminis stiklas), nerūdijantis plienas, aliuminis, keramika (tokia kaip aliuminio oksidas), popierius, stiklo-epoksidinės

dervos kompozitas, bet tinkamiausias yra plonasluoksnis kristalinis silikonas. Plonasluoksnis puslaidininkis gali būti pagamintas iš amorfinio silikono, polisilikono, deimanto ar bet kokios kitos plonasluoksnės pulaidininkinės medžiagos. Pjezoelektrinė medžiaga gali būti pjezoelektrinė keramika, tokia kaip švino-cirkonato-titanato (PZT) plėvelės, kurių storis optimaliu atveju siekia nuo 0,1 iki 50,0 mikronų, arba plonasluoksnis polimerinis pjezoelektrinis poliimidas. Tarpusavio sujungimams gali būti panaudotos Ti/Ni/Cu, Al, Cr/Bi/Au, Ti/Ni/Au, Al/Au, W/Cu, W/Au, W/Au medžiagos.

Fig.11 pavaizduota jutiklio, suformuoto ant kristalinio silikono, nešiklio konstrukcija. Kristalinis silikonas pasižymi puikiomis elektrinėmis savybėmis ir palengvina reikalingų tvarkyklių ir išvesties schemų integravimą į jutiklio matricą, tačiau sąlyginai didelis ir plonas silikono lakštas susilenks ir įtruks, kuomet jo paviršius bus spaudžiamas. Pavaizduotasis nešiklis suteikia konstrukcijai daugiau standumo, nei suteiktų to paties storio silikono lakštas.

Kaip parodyta, monolitinis silikono lakštas 82 yra maždaug 0,1 mm storio ir yra apjuostas vienodo storio stiklo-epoksidinės dervos rėmu 83, kuris yra sumontuotas ant pagrindo plokštės 84, taip pat pagamintos ant 0,05 mm storio stiklo-epoksidinės dervos konstrukcijos. Rėmas 83 ir pagrindas 84 gali būti lengvai pagaminti, naudojant įprastą spausdintinių plokščių (PCB) technologiją. Konkrečiai, pagrindo 84 viršutinis ir apatinis paviršiai yra padengiami plonu vario sluoksniu 85, perskirtu stiklo-epoksidinės dervos šerdimi. Rėmas 83 periferijoje turi eilę lydmetalio taškų 86, skirtų sujungimui su apsaugos procesoriumi 8. Plonas silikono lakštas 82 yra priklijuotas epoksidine derva prie rėmo 83 ir pagrindo 84, o aktyvios sritys yra elektriškai prijungtos prie atitinkamų elektrinių takų rėme 82 įprastu sujungimu laidais 87 ties atviromis silikono 82, juosiančio apsauginį viršutinį elektrodą 88, išorinio krašto dalimis 89.

Palyginimo algoritmai

Vietiniam apdorojimui kortelėje, kur apdorojimas yra ribotas ir kur atliekamas tik paprastas 1:1 palyginimas su vieninteliu pavyzdžiu, pirštų atspaudų palyginimo programa gali būti paremta santykinai paprastu detalių, gautų iš dviejų raštų, palyginimu. Pavyzdžiui, pilkos spalvos pirštų atspaudų vaizdas gali būti sumažintas iki dviejų reikšmių – baltos ir juodos – ir erdviniai iškilimai yra konvertuojami į dviejų matmenų plonas linijas (vektorius). Būdo tikslumas

priklauso tarp kitų problemų nuo vaizdo susiliejimo, sulipimo, iškraipymo, dalinio linijos segmentų stygiaus ir kitų efektų. Nors detalių nuskaitymo būdas yra iš principo nelabai tikslus, jam reikalingi mažesni skaičiavimo resursai ir jis yra suderinamas su daugeliu egzistuojančių duomenų bazių.

Apdorojimui nutolusiame autentifikavimo serveryje, kur apdorojimo galia yra didesnė, gali prireikti ir tikslesnio vertinimo, pavyzdžiui, "POC" ("Phase Only Correlattion" - fazinė koreliacija) palyginimo algoritmo. POC yra identifikavimo algoritmas, pagrįstas makroskopiniu pilnų vaizdų palyginimu. POC, priešingai, palygina plataus diapazono struktūrinę informaciją – nuo detalių iki pilno vaizdo. Taigi, POC gali suteikti daugiau tikslumo įvairių trukdžių, tokių kaip sulipimas ir daliniai pertrūkiai, atžvilgiu. Iš principo POC būdui neturi įtakos tokie faktoriai, kaip perstūmimai, nustatant piršto padėtį, ir ryškumo skirtumai, jis yra greitas (autonominis palyginimas trunka apie 0,1 sekundės) ir labai tikslus. Pavyzdžiui, POC programa gali atlikti dviejų pirštų atspaudų raštų erdvės dažnio palyginimą, naudojant plokštuminį pirmąjį Fourier transformavimą ("2DFFT"). 2DFFT konvertuoja skaitmeninių duomenų, išreiškiančių pirštų atspaudo fizikinį plokštuminį pasiskirstymą, matricą į dažnių erdvę, kitais žodžiais – atvirkštinį erdvės pasiskirstymą, kur tankesnis raštas turi didesnį erdvės dažnį. Pasukamoji transformacija gali būti panaudota palyginti dažnių erdvės raštą. POC rašto palyginimas turi kitą privalumą – detalių vektorių palyginimą, nes jo neklaidina bendri įrašyto pirštų atspaudo rašto defektai, kuriuos POC priima kaip trukdžius, bet detalių analizė juos interpretuoja kaip prasmingus duomenis.

Ypatingais atvejais hibridinis būdas gali suteikti daugiau tikslumo ir saugumo, nei bet kuris atskiras būdas. Pavyzdžiui, detalių metodologija gali būti panaudota nuskaitymo vietoje, o POC metodologija gali būti panaudota nutolusiame serveryje. Kitu atveju palyginimo procesas gali analizuoti ir detales, ir tarpelius, siekiant gauti kombinuotą rezultatą, kuris apima abu rezultatus.

Pritaikymas

Aukščiau aprašytoji technologija užtikrina aukštą saugumą įvairioms panaudojimo funkcijoms, tiek komercinėms, tiek vyriausybinėms, atlikti. Priklausomai nuo poreikio, kelios saugios panaudojimo funkcijos gali koegzistuoti ir veikti toje pačioje kortelėje ir/arba tame pačiame serveryje. Pagal vieną realizavimo variantą viena kortelė gali turėti iki 24 nepriklausomų ir saugių

panaudojimo funkcijų. Pavyzdžiui, technologija suteiks/draus priėjimą (fizinį ir/arba loginį), nustatys tikslią asmens vietą ir/arba judėjimą, tuo pat metu atlikdama kitas saugias funkcijas, visiškai ir saugiai atskirtas viena nuo kitos.

Tarp numatytų panaudojimo funkcijų ir vietų yra šios:

- Oro uosto ID/įėjimas
- Pastato apsauga
- Įėjimas į viešbučio kambarį ir sąskaitos apmokėjimas
- Ligoninė
- Tiesioginiai (online) žaidimai
- Parsisiųsdintos pramogos
- Gimimo liudijimas
- Priėjimas prie kompiuterio
- Vairuotojo pažymėjimas – TWIC
- Elektroninė piniginė
- Skubi medicinos informacija
- Leidimas dirbti su sprogmenimis
- Leidimas įeiti į vyriausybinius ir karinius objektus
- HAZMAT licencija
- Medicinos priežiūros ir nuolaidų kortelė
- Parkingas
- Pasas
- Piloto licencija
- Uosto ID/įėjimas
- Draudimo polisas
- Socialinio draudimo pažymėjimas
- Patikimo keliautojo kortelė
- Viza arba leidimas įvažiuoti/išvažiuoti
- Balsuotojo registracijos kortelė
- Pašalpos ir maisto kortelė

Daugelyje iš išvardintų atvejų kortelės atmintis taip pat suteikia saugią apsaugą įvairios rūšies privačiai informacijai, kurią registruotas kortelės savininkas gali pasiekti, kuomet įrodo savo tapatybę. Tokia privati informacija yra:

- Administracinė informacija, tokia kaip vardas, pavardė, adresas, gimimo data ir vieta, tautybė, religija, priklausomybė organizacijoms, socialinio draudimo numeris ir imigracijos informacija, tokia kaip vizos rūšis, galiojimas, pilietybė, t.t.
- Finansinė informacija, tokia kaip elektroninė piniginė, Visa, MasterCard, American Express ir t.t. kredito kortelių informacija, banko informacija, tokia kaip banko pavadinimas, banko balansas, pinigų pervedimo informacija, IRS numeris, įrašai apie bankrotą, t.t.
- Fiziologinė ir sveikatos informacija, tokia kaip asmens biometrinė informacija, tokia kaip ūgis, svoris, pirštų atspaudai, rainelės informacija, tinklainės informacija, rankos dydis, kaulų struktūra, balsas, DNA, kraujo grupė, medicininio patikrinimo rezultatai, medicininė istorija, prirašyti vaistai, draudimo informacija, psichologiniai ir fiziologiniai atsakai į tam tikrus veiksnius, t.t.
- Kriminalinė informacija, tokia kaip nusikaltimai, nusižengimai, taisyklių pažeidimai.
- Kritinė informacija, tokia kaip kapinės, giminių ir kita kontaktinė informacija, advokatas, religinė informacija.
- Išsilavinimas, darbo istorija, įskaitant baigtas mokslo įstaigas, laipsnį, darbovietes.
- Priėjimo prie duomenų istorija (saugo įrašus apie priėjimą prie kortelėje ir ne kortelėje esančių duomenų).
- ID informacija, tokia kaip pirštų atspaudai, apdoroti pirštų atspaudai, pirštų atspaudų apdorojimo rezultatai.
- Slaptažodžiai, tokie kaip nuolatinis slaptažodis, laikinas slaptažodis ir/arba vienkartinis slaptažodis.
- Šifravimo raktai, tokie kaip viešasis raktas, asmeninis raktas ir/arba viekartinis raktas.

Dabar bus aprašytas kortelės užregistravimo sistemos pavyzdys.

Pareiškėjas užpildo prašymą ir pateikia jį kartu su nuotrauka ir pirštų atspaudais. Siekiant nustatyti asmens tikrą tapatybę, atliekamas jo pateiktų dokumentų ir informacijos sutikrinimas su informacija valstybinėse ir komercinėse duomenų bazėse.

Patvirtinus tapatybę, pareiškėjas eina į išdavimo stotį, kur kortelės savininko informacija, kuri gali būti reikalinga, yra įrašoma į kortelę. Pareiškėjas uždeda pirštą ant kortelės jutiklio. Kuomet pirštas yra tinkamai uždėtas ant jutiklio ir piršto atspaudas yra įrašytas į kortelę, kortelės tęsinys gauna elektros krūvį, kuris sudegina tam tikrus saugiklius ir niekas kitas jau nieko nebegali įrašyti į šią sritį. Po to tęsinys yra nupjaunamas/nukerpamas (panašiai kaip bambagyslė). Dabar kortelė gali būti nuskaityta ar įrašyta tik per ISO kontaktinį skaitytuvą ar ISO belaidę sistemą.

Naudojant tinklinį autentifikavo serverį, kai kurie ar visi įrašyti į kortelę duomenys yra perduodami užšifruotos formos į nutolusį serverį kartu su papildomais duomenimis, kurie normaliai nėra saugomi kortelėje, bet kurių gali prireikti tam tikrais aukšto saugumo reikalaujančiais panaudojimo atvejais.

IŠRADIMO APIBRĖŽTIS

1. Intelektuali identifikavimo kortelė, turinti:
   joje įrengtą atmintį informacinių duomenų saugojimui;
   joje įrengtą jutiklį gyvų biometrinių duomenų nuskaitymui;
   joje įrengtą mikroprocesorių, nuskaitytų biometrinių duomenų palyginimui iš anksto nustatyto slenksčio ribose su atitinkamais atmintyje išsaugotais informaciniais duomenimis ir verifikavimo pranešimo generavimui tik tuomet, jei duomenys sutampa iš anksto nustatyto slenksčio ribose; ir
   priemonę verifikavimo pranešimo persiuntimui į išorinį tinklą, besiskirianti tuo, kad verifikavimo pranešimas turi mažiausiai ištraukas iš nuskaitytų biometrinių duomenų.

2. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad verifikavimo pranešimas yra perduodamas į nutolusią autentifikavimo sistemą papildomam verifikavimui.

3. Identifikavimo kortelė pagal 2 punktą, besiskirianti tuo, kad nutolusi autentifikavimo sistema turi atokiai saugomus informacinius duomenis, kurie skiriasi nuo lokaliai saugomų informacinių duomenų.

4. Identifikavimo kortelė pagal 2 punktą, besiskirianti tuo, kad kortelės mikroprocesorius naudoja skirtingą palyginimo algoritmą nei tas, kurį naudoja nutolusi autentifikavimo sistema.

5. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad kortelė yra suderinama su ISO SmartCard.

6. Identifikavimo kortelė pagal 5 punktą, besiskirianti tuo, kad joje esantis procesorius yra apsaugos procesorius, naudojamas apsaugotų biometrinių duomenų saugojimui ir apdorojimui ir tuo, kad dar turi ISO SmartCard procesorių.

7. Identifikavimo kortelė pagal 6 punktą, besiskirianti tuo, kad apsaugos procesorius yra funkciškai atskirtas užkarda nuo ISO SmartCard procesoriaus.

8. Identifikavimo kortelė pagal 6 punktą, besiskirianti tuo, kad visi išoriniai duomenys į ir iš apsaugos procesoriaus praeina per ISO SmartCard procesorių.

9. Identifikavimo kortelė pagal 6 punktą, besiskirianti tuo, kad visi išoriniai duomenys į ir iš ISO SmartCard procesoriaus praeina per apsaugos procesorių.

10. Identifikavimo kortelė pagal 6 punktą, besiskirianti tuo, kad apsaugos procesorius turi pirmąją jungtį, naudojamą duomenų įvedimui duomenų įvedimo proceso metu, ir antrąją jungtį, prijungtą prie išorinio tinklo.

11. Identifikavimo kortelė pagal 10 punktą, besiskirianti tuo, kad pirmoji jungtis yra nuolatinai atjungiama užbaigus duomenų įvedimo procesą.

12. Identifikavimo kortelė pagal 6 punktą, besiskirianti tuo, kad:
kortelė turi viršutinę magnetinės juostelės sritį ir apatinę reljefišką sritį;
biometrinis jutiklis yra pirštų atspaudų jutiklis; ir
apsaugos procesorius, ISO SmartCard procesorius ir pirštų atspaudų jutiklis yra įrengti vidurinėje srityje tarp viršutinės srities ir apatinės srities.

13. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad į biometrinių duomenų sudėtį įeina pirštų antspaudų duomenys, o jutiklis yra pirštų atspaudų jutiklis, kuris nuskaito duomenis nuo naudotojo piršto, uždėto ant jutiklio.

14. Identifikavimo kortelė pagal 13 punktą, dar turinti:

indikatorių piršto padėties realaus laiko grįžtamojo ryšio tiekimui, kol naudotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tuo būdu palengvinant optimalų piršto nustatymą virš jutiklio.

15. Identifikavimo kortelė pagal 13 punktą, besiskirianti tuo, kad palyginimo procesas naudoja hibridinį palyginimo algoritmą, kuris atsižvelgia tiek į atskiras detales, tiek į bendrą erdvinį nuskaitytų biometrinių duomenų vaizdą.

16. Identifikavimo kortelė pagal 13 punktą, besiskirianti tuo, kad pirštų atspaudų jutiklis turi kristalinio silicio sluoksnelį, uždėtą ant pagrindo plokštės.

17. Identifikavimo kortelė pagal 16 punktą, besiskirianti tuo, kad pagrindo plokštė turi stiklo epoksido dervos sluoksnį, įterptą tarp dviejų metalo sluoksnių.

18. Identifikavimo kortelė pagal 16 punktą, besiskirianti tuo, kad pagrindo plokštė yra sustiprinta nešiklio rėmu, juosiančiu silicio sluoksnelį.

19. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad kortelė dar turi apribojimo priemonę, leidžiančią kortelę naudoti iš anksto nustatytoje vietoje.

20. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad mažiausiai kai kurie nuskaityti biometriniai ir informaciniai duomenys yra perduodami į atskirą autentifikavimo serverį saugiam naudotojo tapatybės verifikavimui prieš suteikiant tiesioginį priėjimą prie programų serverio saugių finansinių transakcijų šio naudotojo vardu atlikimui.

21. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad atsakant į palyginimo užklausą, susijusią su konkrečiu bandymu

užsiregistruoti konkrečiame programų serveryje, kuris išduoda teigiamą palyginimo rezultatą autentifikavimo serveryje, aktyvuojamas saugus trijų pakopų autentifikavimo protokolas, kuriame užklausos ženklų seka yra išsiunčiama iš autentifikavimo serverio į identifikavimo kortelę, tuomet identifikavimo kortelė naudoja užklausos ženklų seką ir palyginimo užklausą atsakymo generavimui, kurį ji po to persiunčia į programų serverį, tuomet programų serveris persiunčia atsakymą į užklausą į autentifikavimo serverį, kuris patikrina, ar atsakymas į užklausą yra galiojantis.

22. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad kortelės išvestis yra panaudojama gauti fiziniam priėmimui į saugią sritį.

23. Identifikavimo kortelė pagal 22 punktą, besiskirianti tuo, kad įrašai apie sėkmingus ir nesėkmingus bandymus prisijungti yra aptarnaujami kortelės.

24. Identifikavimo kortelė pagal 1 punktą, besiskirianti tuo, kad ši priemonė turi mažiausiai vieną:
elektrinio kontakto sąsajos įtaisą; ir
belaidę persiuntimo sąsajos įtaisą.

25. Intelektuali identifikavimo kortelė, turinti:
joje įrengtą jutiklį gyvų biometrinių duomenų nuskaitymui;
joje įrengtą pirmą procesorių, kuris yra sujungtas su joje įrengtu minėtu jutikliu, joje įrengtą minėtą pirmą procesorių, turintį atmintį informacinių duomenų saugojimui, joje įrengtą minėtą pirmą procesorių, nuskaitytų biometrinių duomenų palyginimui iš anksto nustatyto slenksčio ribose su atitinkamais atmintyje išsaugotais informaciniais duomenimis, ir verifikavimo pranešimo generavimui tik tuomet, jei duomenys sutampa iš anksto nustatyto slenksčio ribose;

antrą joje įrengtą procesorių, sujungtą su joje įrengtu minėtu pirmu procesoriumi, identifikavimo kortelės funkcijų vykdymui, verifikavimo pranešimas įjungiantis minėtą antrą joje esantį procesorių; ir

bendravimui su išoriniu tinklu sąsają, sujungtą su vienu iš joje įrengtu minėtu pirmu procesoriumi arba joje įrengtu minėtu antru procesoriumi.

26. Identifikavimo kortelė pagal 25 punktą, besiskirianti tuo, kad joje įrengtas minėtas antras procesorius yra ISO SmartCard procesorius.

27. Identifikavimo kortelė pagal 26 punktą, besiskirianti tuo, kad joje įrengtas pirmas procesorius yra funkciškai atskirtas užkarda nuo ISO SmartCard procesoriaus.

28. Identifikavimo kortelė pagal 26 punktą, besiskirianti tuo, kad visi išoriniai duomenys į ir iš joje įrengto pirmo procesoriaus pereina per ISO SmartCard procesorių.

29. Identifikavimo kortelė pagal 26 punktą, besiskirianti tuo, kad visi išoriniai duomenys į ir iš ISO SmartCard procesoriaus pereina per joje esantį pirmą procesorių.

30. Identifikavimo kortelė pagal 29 punktą, besiskirianti tuo, kad joje įrengtas pirmas procesorius turi pirmąją jungtį, naudojamą duomenų įvedimui įvedimo proceso metu, ir antrąją jungtį, prijungtą prie išorinio tinklo.

31. Identifikavimo kortelė pagal 25 punktą, dar turinti:

joje įrengtą lokacijos detektorių, identifikavimo kortelės esamai lokacijai nustatyti; ir

prietaisą, priklausomai nuo detektuotos lokacijos, apribojantį kortelės naudojimą.

32. Identifikavimo kortelė pagal 31 punktą, besiskirianti tuo, kad joje įrengtas minėtas lokacijos detektorius turi:

globalinio padėties nustatymo palydovo (GPS) signalų imtuvą.

33. Intelektuali identifikavimo kortelė pagal 25 punktą, dar turinti:
indikatorių piršto padėties realaus laiko grįžtamojo ryšio tiekimui, kol naudotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tuo būdu palengvinant optimalų piršto nustatymą virš jutiklio.

34. Identifikavimo kortelė pagal 25 punktą, besiskirianti tuo, kad minėta sąsaja turi mažiausiai vieną:
belaidę sąsają, sujungtą su joje įrengtu minėtu antru procesoriumi; ir
laidinę elektrinę sąsają, sujungtą su joje įrengtu minėtu antru procesoriumi.

35. Identifikavimo kortelė pagal 34 punktą, besiskirianti tuo, kad minėta belaidė sąsaja yra suderinama su ISO antena, naudojama tiek duomenims, tiek energijai perduoti.

36. Identifikavimo kortelė pagal 34 punktą, besiskirianti tuo, kad minėta sąsaja dar turi:
apsaugos anteną, kuri per galios grandinę yra sujungta su joje įrengtu minėtu pirmu procesoriumi, ši apsaugos antena tik tiekia energiją joje įrengtam minėtam pirmam procesoriui.

37. Identifikavimo kortelė pagal 36 punktą, besiskirianti tuo, kad minėta apsaugos antena per galios grandinę taip pat tiekia energiją joje įrengtam minėtam jutikliui.

38. Intelektualios identifikavimo kortelės naudotojo identifikavimo būdas, intelektuali identifikavimo kortelė turinti joje įrengtą atmintį informaciniams duomenims saugoti ir joje įrengtą biometrinį jutiklį, šis būdas, turintis:
gyvų biometrinių duomenų nuskaitymą panaudojant joje įrengtą jutiklį;

nuskaitytų biometrinių duomenų palyginimą nustatyto slenksčio ribose su atitinkamais informaciniais duomenimis, išsaugotais joje įrengtoje atmintyje;

verifikavimo pranešimo generavimą tik tuo atveju, jei yra sutapimas nustatyto slenksčio ribose; ir

verifikavimo pranešimo perdavimą į išorinį tinklą,

besiskiriantis tuo, kad verifikavimo pranešimas turi mažiausiai ištraukas iš nuskaitytų biometrinių duomenų.

39. Būdas pagal punktą 38, dar turintis:

verifikavimo pranešimo perdavimą į nutolusią autentifikavimo sistemą papildomam verifikavimui.

40. Būdas pagal punktą 39, dar turintis:

informacinių duomenų saugojimą nutolusioje autentifikavimo sistemoje, kurie yra skirtingi nuo informacinių duomenų, išsaugotų identifikavimo kortelėje.

41. Būdas pagal punktą 39, besiskiriantis tuo, kad palyginimo algoritmas, naudojamas identifikavimo kortelėje yra skirtingas nei palyginimo algoritmas, naudojamas nutolusioje autentifikavimo sistemoje.

42. Būdas pagal punktą 38, dar turi:

mažiausiai kai kurių nuskaitytų biometrinių duomenų ir informacinių duomenų perdavimą į atskirą autentifikavimo serverį, saugiam varotojo tapatybės verifikavimui prieš suteikiant tiesioginį priėmimą prie programų serverio, saugioms finansinėms transakcijoms šio naudotojo vardu atlikimui.

43. Būdas pagal punktą 38, dar turintis:

palyginimo užklausos, susijusios su konkrečiu bandymu užsiregistruoti konkrečiame programų serveryje, priėmimą; ir

saugų trijų pakopų autentifikavimo protokolo paleidimą, jei teigiamas palyginimo rezultatas į palyginimo užklausos atsaką yra išduodamas, autentifikavimo protokolas, turintis:

užklausos ženklų sekos išsiuntimą iš autentifikavimo serverio į identifikavimo kortelę;

užklausos atsakymo, paremto užklausos ženklų seka ir palyginimo užklausa, identifikavimo kortelėje generavimą;

užklausos atsakymo persiuntimą į programų serverį;

užklausos atsakymo persiuntimą iš programų serverio į autentifikavimo serverį; ir

patikrinimą, autentifikavimo serveryje, ar užklausos atsakymas yra galiojantis.

44. Intelektualios identifikavimo kortelės naudotojo identifikavimo būdas, intelektuali identifikavimo kortelė, turinti joje įrengtą atmintį informacinių duomenų saugojimui, joje įrengtą biometrinį jutiklį, apsaugos procesorių ir ISO kortelės procesorių, šis būdas turintis:

gyvų biometrinių duomenų nuskaitymą, panaudojant joje įrengtą jutiklį;

nuskaitytų biometrinių duomenų palyginimą, panaudojant apsaugos procesorių, su atitinkamais informaciniais duomenimis, išsaugotais joje įrengtoje atmintyje, nustatyto slenksčio ribose;

verifikavimo pranešimo generavimą, panaudojant apsaugos procesorių, tik tuo atveju, jei yra sutapimas nustatyto slenksčio ribose, ISO kortelės procesorių aktyvuojantį verifikavimo pranešimą; ir

ISO kortelės procesoriaus aktyvavimą, jei naudotojo identiškumas yra patvirtintas.

45. Būdas pagal punktą 44, dar turintis:

duomenų įvedimą įvedimo proceso metu per pirmąją jungtį į apsaugos procesorių; ir

pirmos jungties nuolatinį atjungimą, užbaigus duomenų įvedimo procesą.

46. Būdas pagal punktą 44, besiskiriantis tuo, kad visi išoriniai duomenys į ir iš ISO kortelės praeina per apsaugos procesoriaus antrą jungtį.

47. Būdas pagal punktą 44, besiskiriantis tuo, kad visi išoriniai duomenys į ir iš apsaugos procesoriaus praeina per ISO kortelės procesorių.

48. Būdas pagal punktą 44, besiskiriantis tuo, kad į biometrinių duomenų sudėtį įeina pirštų antspaudų duomenys, o jutiklis yra pirštų atspaudų jutiklis, kuris nuskaito duomenis nuo naudotojo piršto, uždėto ant jutiklio.

49. Būdas pagal punktą 48, dar turintis:
piršto padėties realaus laiko grįžtamojo ryšio tiekimą, kol naudotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tuo būdu palengvinant optimalų piršto nustatymą virš jutiklio.

50. Būdas pagal punktą 44, besiskiriantis tuo, kad palyginimo procesas naudoja hibridinį palyginimo algoritmą, kuris atsižvelgia tiek į atskiras detales, tiek į bendrą erdvinį nuskaitytų biometrinių duomenų vaizdą.

51. Būdas pagal punktą 44, dar turintis:
piršto padėties realaus laiko grįžtamojo ryšio tiekimą, kol naudotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tuo būdu palengvinant optimalų piršto nustatymą virš jutiklio.

52. Būdas pagal punktą 44, besiskiriantis tuo, kad minėtas verifikavimo pranešimo perdavimas turi mažiausiai vieną:
perdavimą per belaidę sąsają, sujungtą su ISO kortelės procesoriumi; ir

perdavimą per laidinę elektrinę sąsają, sujungtą su ISO kortelės procesoriumi.

53. Būdas pagal punktą 52, besiskiriantis tuo, kad minėta belaidė sąsaja yra suderinama su ISO antena, naudojama tiek duomenų, tiek energijos perdavimams.

54. Būdas pagal punktą 52, dar turintis:
energijos tiekimą apsaugos procesoriui per apsaugos anteną ir galios grandinę, sujungtą su apsaugos procesoriumi, kortelė aprūpinama apsaugos antena ir galios grandine.

55. Būdas pagal punktą 54, dar turintis:
energijos perdavimą į joje įrengtą biometrinį jutiklį per apsaugos anteną ir galios grandinę.

56. Intelektualios identifikavimo kortelės naudotojo identifikavimo aparatas, intelektuali identifikavimo kortelė, turinti joje įrengtą atmintį informacinių duomenų saugojimui ir joje įrengtą biometrinį jutiklį, šis aparatas, turintis:
prietaisą gyvų biometrinių duomenų nuskaitymui, panaudojant joje įrengtą jutiklį;
prietaisą nuskaitytų biometrinių duomenų palyginimui iš anksto nustatyto slenksčio ribose su atitinkamais joje įrengtoje atmintyje išsaugotais informaciniais duomenimis;
prietaisą verifikavimo pranešimo generavimui tik tuomet, jei duomenys sutampa iš anksto nustatyto slenksčio ribose; ir
prietaisą verifikavimo pranešimui perduoti į išorinį tinklą,
besiskiriantis tuo, kad verifikavimo pranešimas turi mažiausiai ištraukas iš nuskaitytų biometrinių duomenų.

57. Intelektualios identifikavimo kortelės naudotojo identifikavimo aparatas, intelektuali identifikavimo kortelė, turinti joje įrengtą atmintį informacinių

duomenų saugojimui, joje įrengtą biometrinį jutiklį, apsaugos procesorių ir ISO kortelės procesorių, šis aparatas, turintis:

prietaisą gyvų biometrinių duomenų nuskaitymui, panaudojant joje įrengtą jutiklį;

prietaisą nuskaitytų biometrinių duomenų palyginimui, panaudojant apsaugos procesorių, iš anksto nustatyto slenksčio ribose su atitinkamais joje įrengtoje atmintyje išsaugotais informaciniais duomenimis;

prietaisą verifikavimo pranešimo generavimui, panaudojant apsaugos procesorių, tik tuomet, jei duomenys sutampa iš anksto nustatyto slenksčio ribose, verifikavimo pranešimas aktyvuojantis ISO kortelės procesorių; ir

prietaisą aktyvuojantį ISO kortelės procesorių, jei naudotojo identiškumas yra patvirtintas.

58. Aparatas pagal punktą 57, dar turintis:

indikatorių piršto padėties realaus laiko grįžtamojo ryšio tiekimui, kol naudotojas manipuliuoja savo pirštu virš pirštų atspaudų jutiklio, tuo būdu palengvinant optimalų piršto nustatymą virš jutiklio.

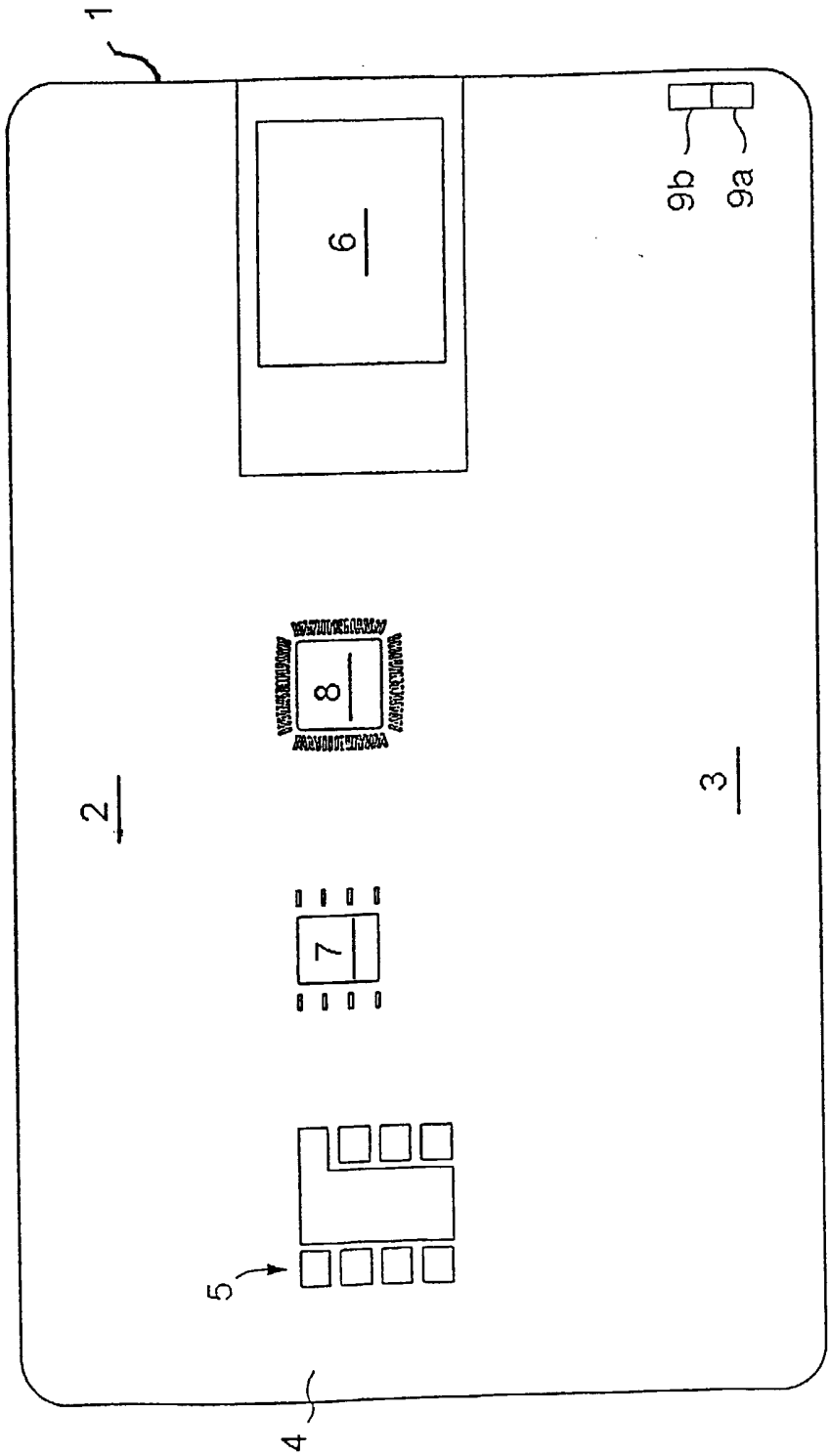


Fig. 1

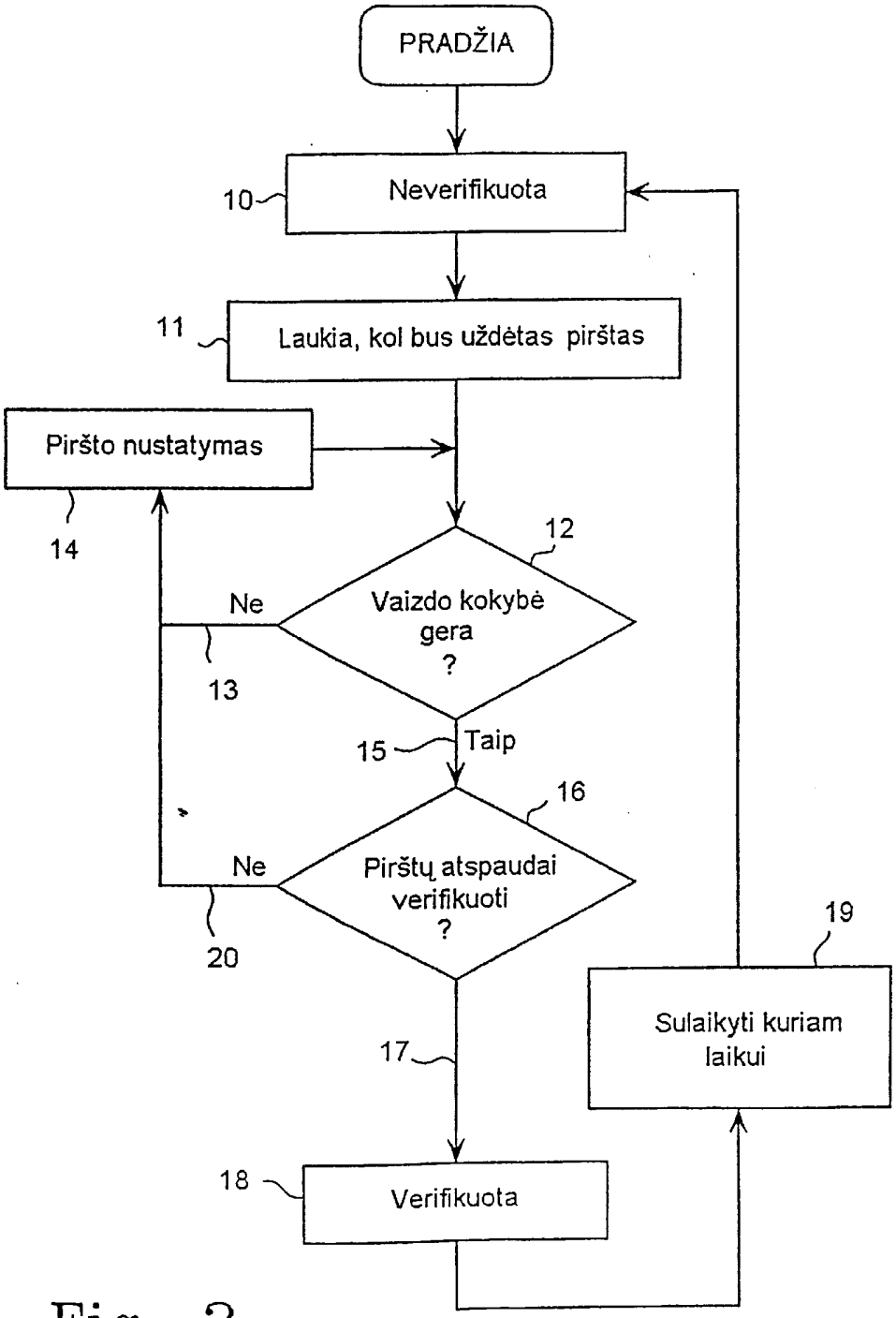

PRADŽIA
10
Neverifikuota
11
Laukia, kol bus uždėtas pirštas
Piršto nustatymas
14
12
Ne
Vaizdo kokybė gera ?
13
15
Taip
16
Ne
Pirštų atspaudai verifikuoti ?
20
19
Sulaikyti kuriam laikui
17
18
Verifikuota

Fig. 2

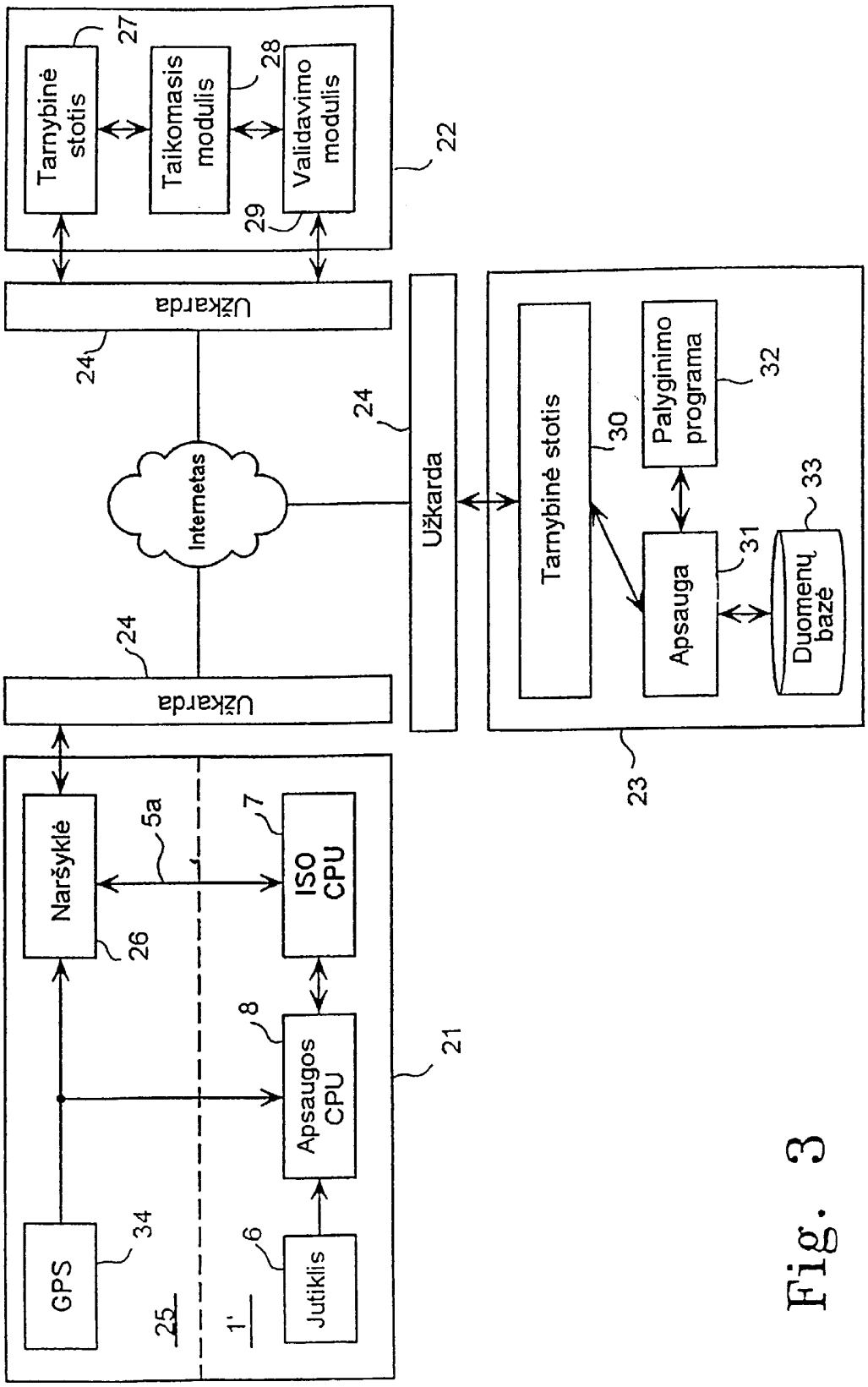

Tarnybinė stotis
27
Taikomasis modulis
28
Validavimo modulis
29
22
Užkarda
24
Internetas
24
Užkarda
24
Užkarda
Tarnybinė stotis
30
Palyginimo programa
32
Apsauga
31
Duomenų bazė
33
23
Naršyklė
5a
7
ISO CPU
26
8
Apsaugos CPU
21
GPS
34
25
1'
Jutiklis
6

Fig. 3

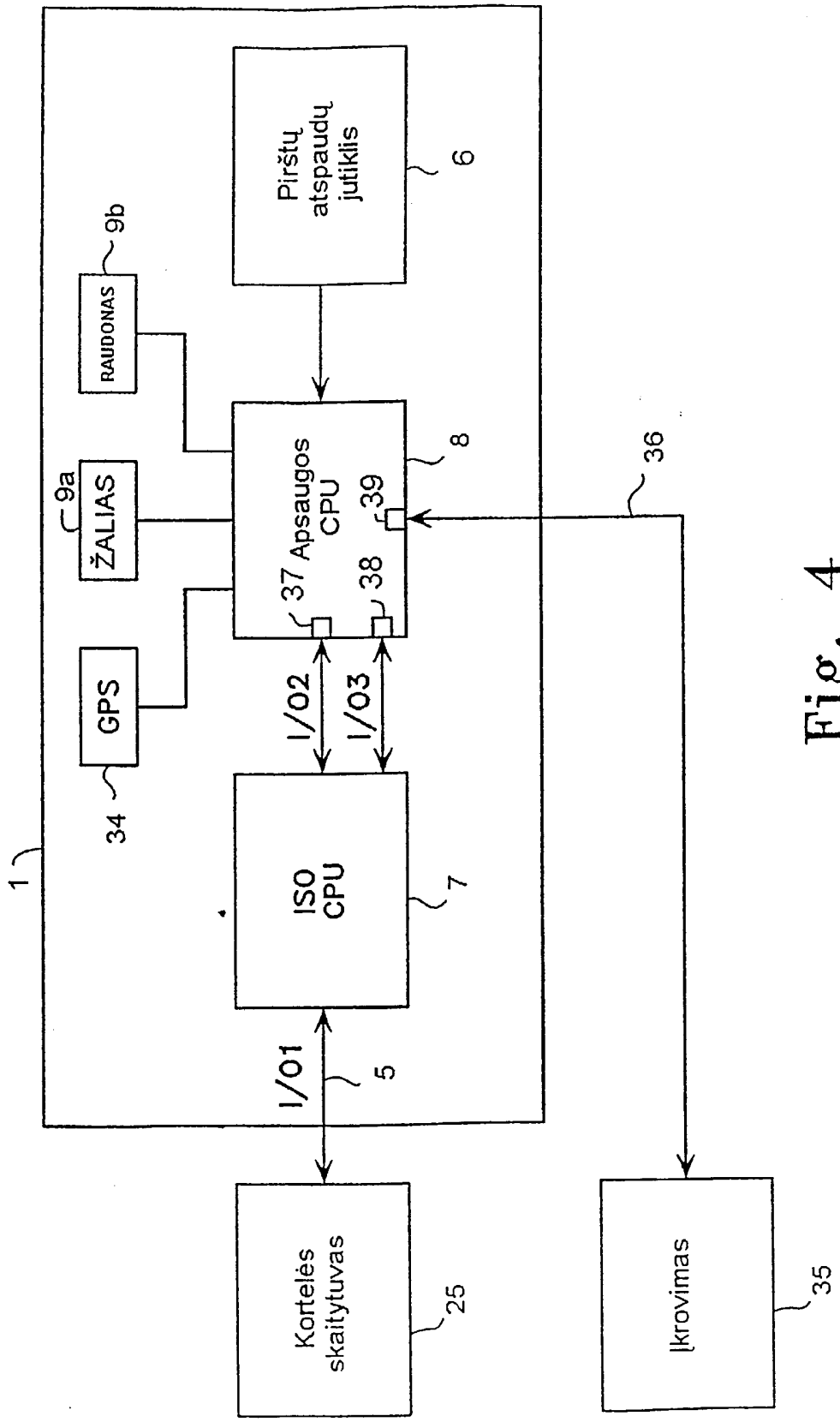

Pirštų atspaudų jutiklis
6
9b
RAUDONAS
9a
ŽALIAS
GPS
34
Apsaugos CPU
8
37
38
39
36
I/02
I/03
ISO CPU
7
1
I/01
5
Kortelės skaitytuvas
25
Įkrovimas
35

Fig. 4

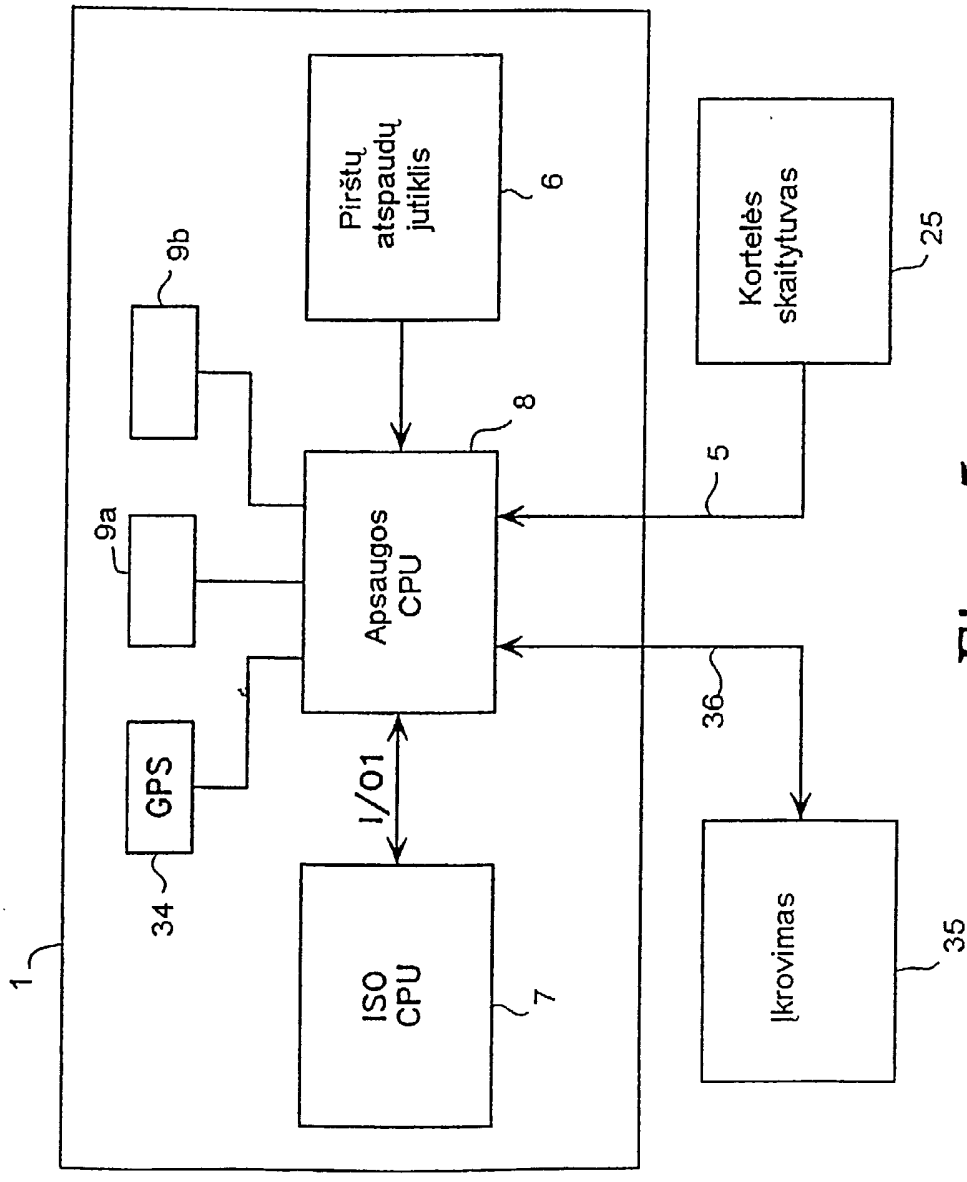

Pirštų atspaudų jutiklis
6
Kortelės skaitytuvas
25
9b
8
5
9a
Apsaugos CPU
GPS
34
I/O1
36
ISO CPU
7
Įkrovimas
35
1

Fig. 5

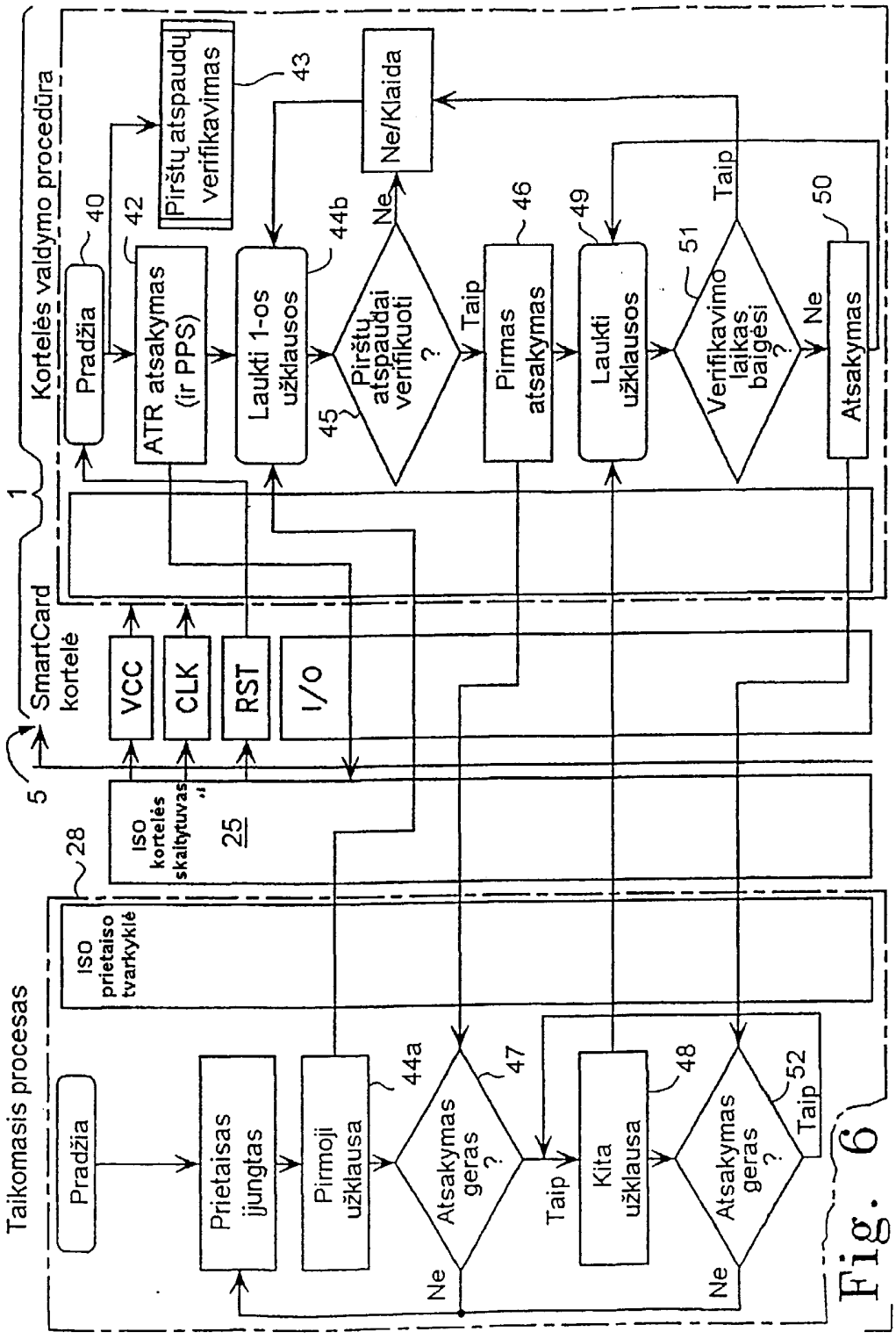

Taikomasis procesas
Pradžia
Prietaisas įjungtas
Pirmoji užklausa
44a
Atsakymas geras ?
Ne
47
Taip
Kita užklausa
48
Atsakymas geras ?
Ne
52
Taip
ISO prietaiso tvarkyklė
28
ISO kortelės skaitytuvas
25
5
SmartCard kortelė
VCC
CLK
RST
I/O
1
Kortelės valdymo procedūra
Pradžia
40
ATR atsakymas (ir PPS)
42
Pirštų atspaudų verifikavimas
43
Laukti 1-os užklausos
44b
Pirštų atspaudai verifikuoti ?
45
Ne
Ne/Klaida
Taip
Pirmas atsakymas
46
Laukti užklausos
49
Verifikavimo laikas baigėsi ?
51
Taip
Ne
Atsakymas
50

Fig. 6

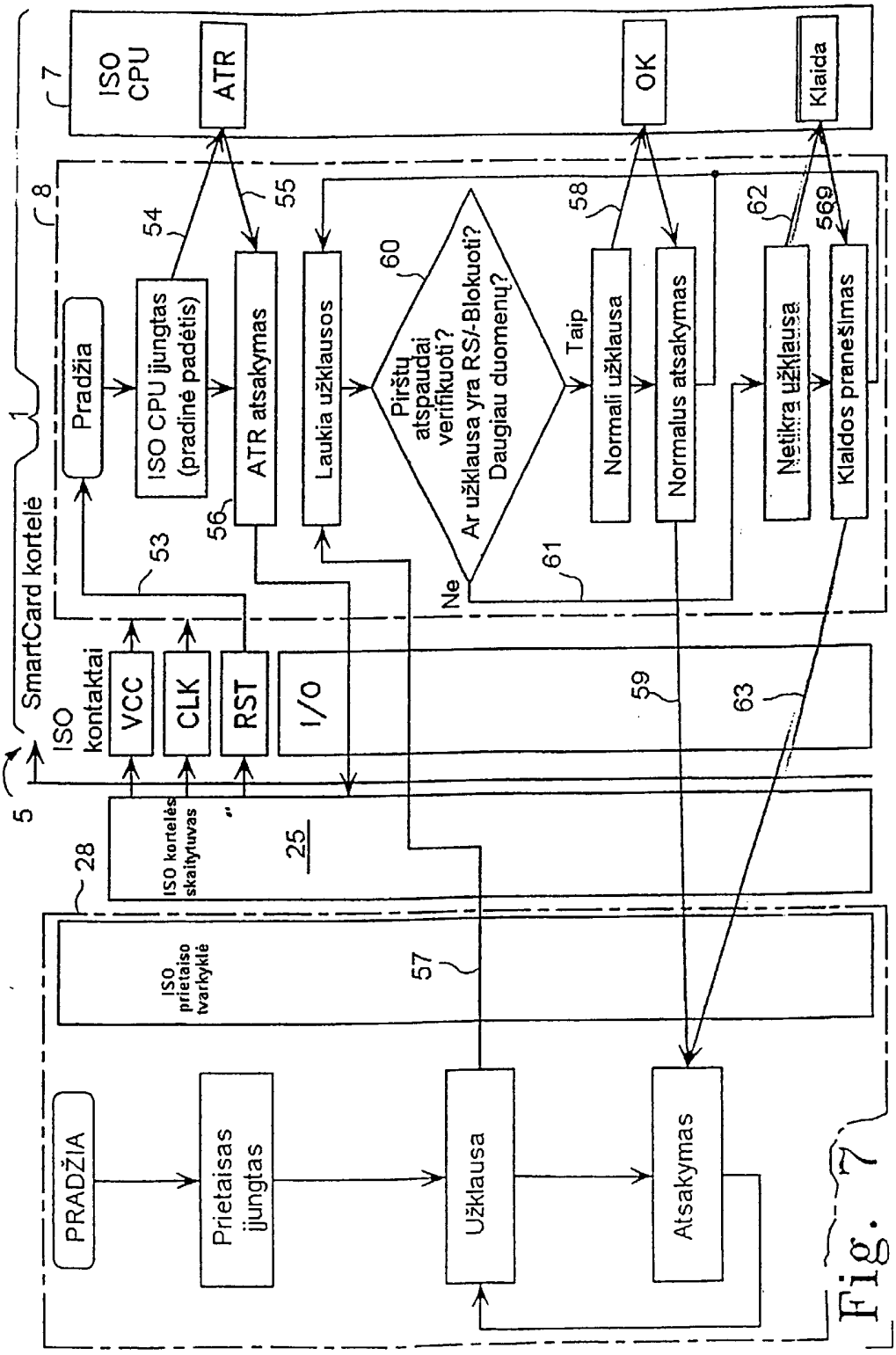

ISO CPU
7
ATR
OK
Klaida
8
1
SmartCard kortelė
Pradžia
ISO CPU įjungtas (pradinė padėtis)
ATR atsakymas
Laukia užklausos
Pirštų atspaudai verifikuoti? Ar užklausa yra RS/-Blokuoti? Daugiau duomenų?
Taip
Ne
Normali užklausa
Normalus atsakymas
Netikra užklausa
Klaidos pranešimas
54
55
56
53
60
61
58
62
569
ISO kontaktai
VCC
CLK
RST
I/O
5
59
63
ISO kortelės skaitytuvas
25
28
ISO prietaiso tvarkyklė
57
PRADŽIA
Prietaisas įjungtas
Užklausa
Atsakymas

Fig. 7

Fig. 8

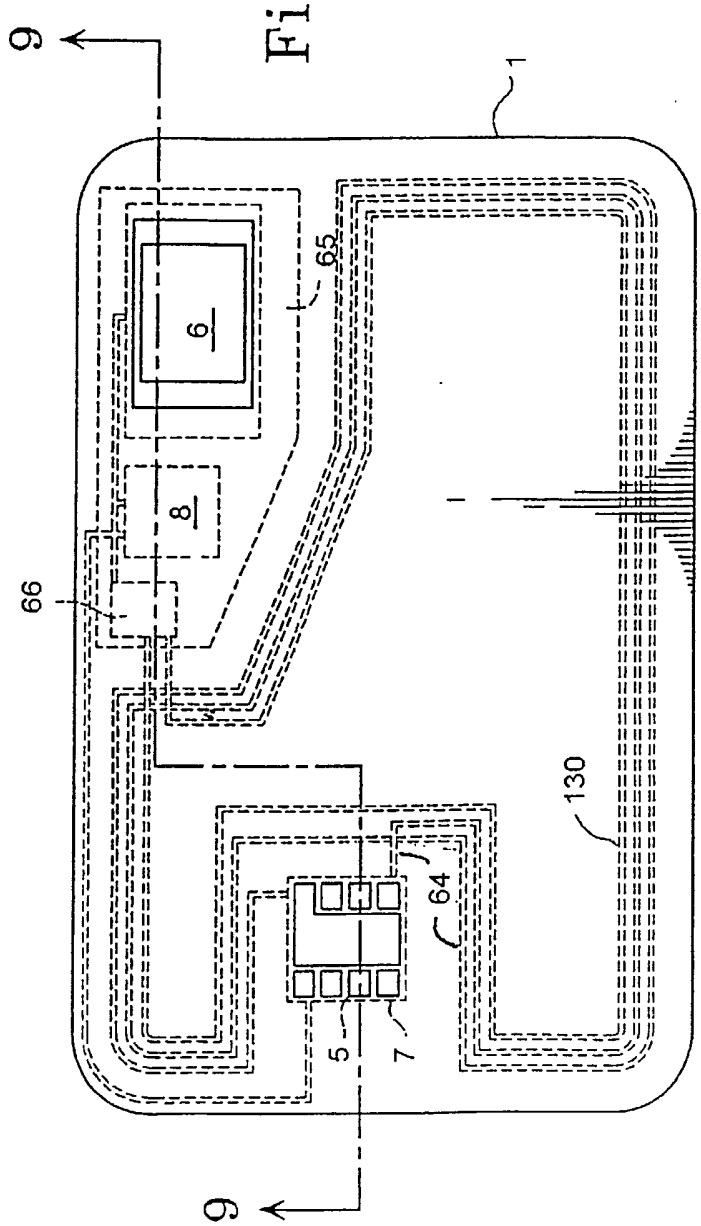
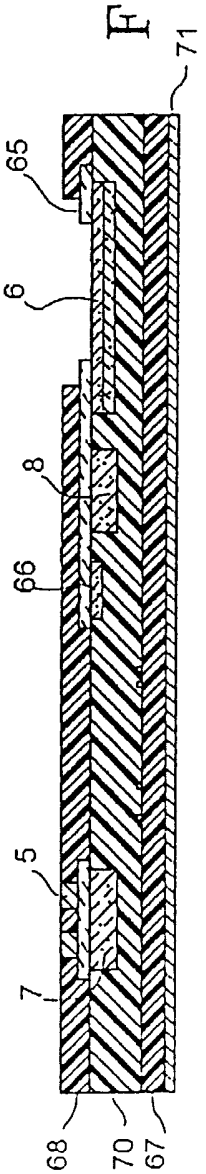


Fig. 9



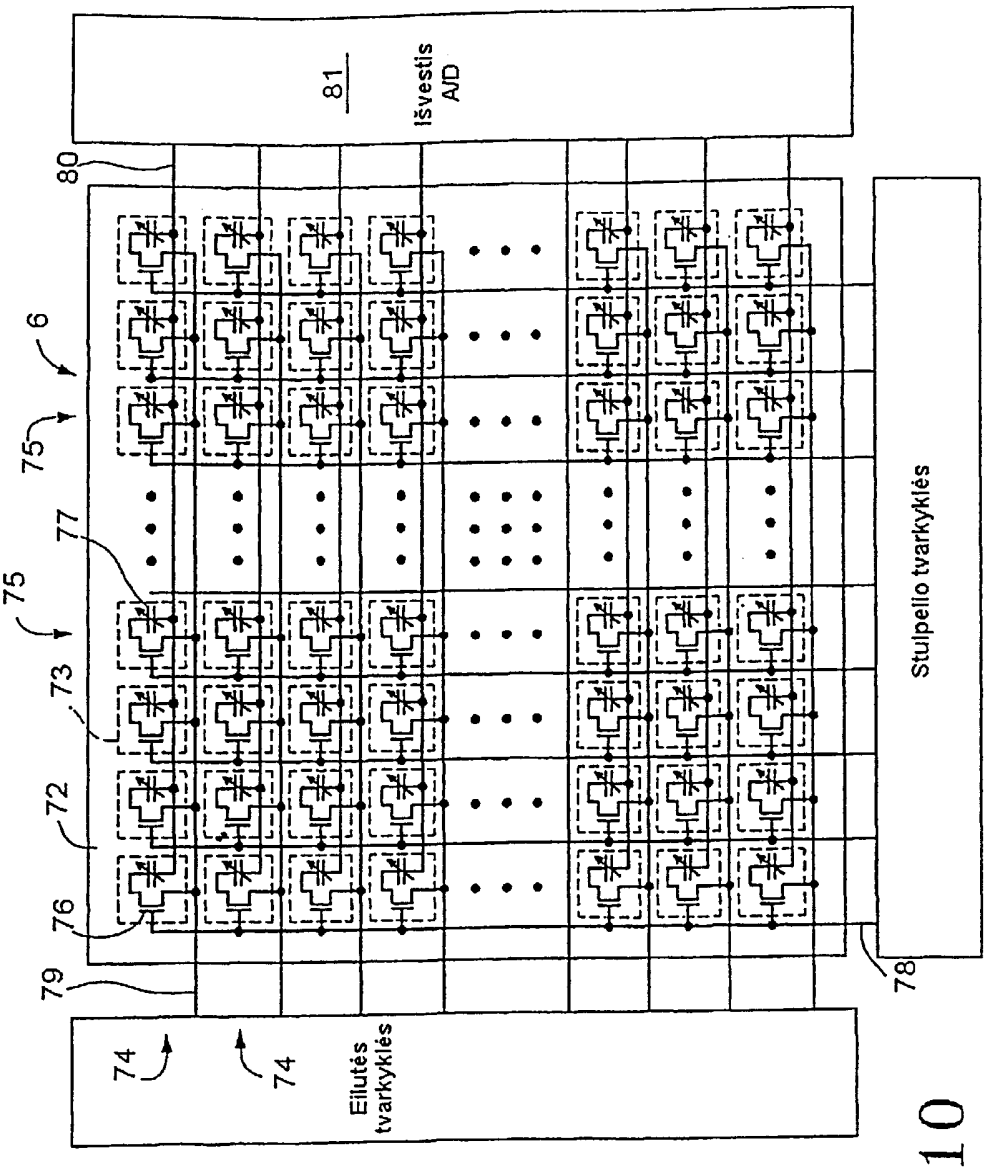

81
Išvestis A/D
80
6
75
77
75
73
72
76
79
74
74
Eilutės tvarkyklės
78
Stulpelio tvarkyklės

Fig. 10

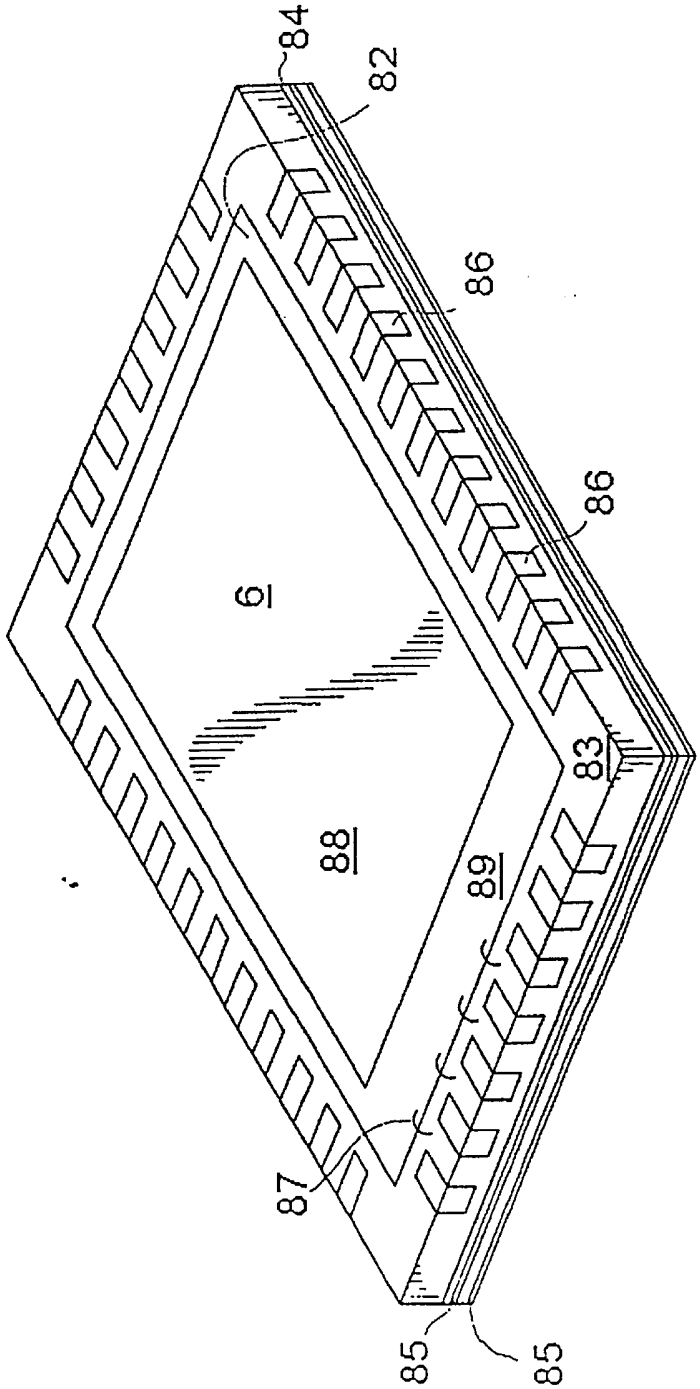


Fig. 11