VALSTYBINĖ
DUOMENŲ APSAUGOS
INSPEKCIJA

BIOMETRINIŲ DUOMENŲ TVARKYMAS ELEKTRONINĖJE ERDVĖJE

Rekomendacija

Parengė
Modestas Zulonas
Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų skyriaus vyriausiasis specialistas

2017 m.

TURINYS

SĄVOKOS

Autorizavimas – tai procesas, kuris naudojamas patikrinti vartotojo privilegijas atlikti tam tikrus veiksmus sistemoje.

Autentifikavimas tikrina tai, kas yra susieta ir valdoma paties subjekto (pavyzdžiui, slaptažodžiai, skaičių žetonai), ir užtikrina, kad subjektas tai gali įrodyti.

Identifikavimas parodo tik specifinį subjektą tarp kitų subjektų.

Elektroninė erdvė – terpė, kurioje elektroniniu būdu gaunami, perduodami, kaupiami ir saugomi duomenys bei informacija.

Biometriniai duomenys – konkretūs požymiai, pagal kuriuos galima nustatyti unikalias žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė, balsas, kuriais remiantis galime patvirtinti žmogaus tapatybę.

Kitos rekomendacijoje vartojamos sąvokos ir terminai suprantami taip, kaip jie apibrėžti Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir Europos Sąjungos Bendrajame duomenų apsaugos reglamente.

ĮVADAS

Biometrinių duomenų analizė (biometrika) – technologijų sritis, kurioje, taikant automatinius atpažinimo metodus, asmuo, kaip duomenų subjektas, yra identifikuojamas, autentifikuojamas ar analizuojamas pagal subjekto fiziologines ar elgsenos charakteristikos savybes. Duomenų subjektą galima identifikuoti tiek pagal fiziologines savybes, tokias kaip pirštų atspaudai, plaštakos geometrija, akies rainelė, akies tinklainė, veidas, kvapas, DNR, tiek ir pagal elgesio charakteristikos savybes, t. y. klavišų paspaudimus, rašyseną, balsą.

Kritiškai svarbus yra vartotojų tapatybės ir prieigos prie kompiuterinių sistemų valdymas, užtikrinant sistemų saugumą ir funkcionalumą. Siekiant apsaugoti duomenų subjekto privatumą ir asmens duomenų saugumą, reikalinga prieigos kontrolė, kuri užtikrintų, kad atitinkamas vartotojas gauna atitinkamą prieigą prie informacinės sistemos ir ten saugomų asmens duomenų, tam reikalingas vartotojų identifikavimas, autentifikavimas ir autorizavimas. **Autorizavimas** – tai procesas, kuris naudojamas patikrinti vartotojo privilegijas atlikti tam tikrus veiksmus sistemoje. **Autentifikavimas** tikrina tai, kas yra susieta ir valdoma paties subjekto (pavyzdžiui, slaptažodžiai, skaičių žetonai), ir užtikrina, kad subjektas tai gali įrodyti. **Identifikavimas** parodo tik specifinį subjektą tarp kitų subjektų. Vienas iš autentifikavimo faktorių yra biometriniai duomenys, t. y. asmens fizinių savybių ar elgesio charakteristikos savybių patikrinimas.

Kompiuterinių sistemų pažeidžiamumui mažinti ar didesniam abipusiam pasitikėjimui užtikrinti gali būti įgyvendintas keleto autentifikavimo faktorių kompleksas. Kaip pavyzdys yra *PIN* kodas (tai, ką duomenų subjektas žino) ir kreditinė ar debetinė kortelė (tai, ką duomenų subjektas fiziškai turi). Jų pakanka, kad duomenų subjektas būtų autentifikuojamas kaip jam priklausančios banko paskyros valdytojas. Autentifikavimo faktorių parinkimas (jei reikia) tam tikrai užduočiai turi tiesioginę įtaką sistemos saugumui ir privatumui.

Daugėjant internetu teikiamų paslaugų, duomenų subjektas gali turėti daug vartotojo paskyrų ir slaptažodžio, kaip autentifikavimo priemonės, naudojimas gali lemti tam tikrų saugumo užtikrinimą mažinančių problemų atsiradimą:

- To paties slaptažodžio naudojimas keliose paskyrose;
- Vartotojai savo noru dalijasi slaptažodžiais su trečiosiomis šalimis (programinę įrangą), siekiant užtikrinti paslaugų kokybę;
- Slaptažodis pamirštamas, todėl reikia laiko ir pakeitimo mechanizmų, kurie ne visada yra saugūs;
- Slaptažodžiai kaupiami nesaugiais metodais;
- Slaptažodžiai gali būti atskleisti „tikslingai išgaunant“ juos iš vartotojų.

Siekiant užtikrinti duomenų subjekto apsaugą elektroninėje erdvėje ir naudojantis elektroninės erdvės paslaugomis, yra pereinama nuo vieno faktoriaus (slaptažodžio, *PIN* kodo) autentifikavimo metodo prie kelių faktorių autentifikavimo, dažniausiai tai – vienkartinis slaptažodžio išdavimo *žetonas* (angl. *token*), išmaniosios programėlės (angl. *apps*), tokie patikimi įrenginiai, kaip išmaniosios kortelės (angl. *smartcards*), ir biometriniai duomenys.

BIOMETRINIAI DUOMENYS

Biometriniai duomenys *ISO/IEC 2382:2015* standarte apibūdinami kaip:

„*Konkretūs požymiai, pagal kuriuos galima nustatyti unikalias žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė, balsas, kuriais remiantis galime patvirtinti žmogaus tapatybę.*“

Biometrinių duomenų analizė yra patraukli todėl, kad kiekvienas duomenų subjektas turi savo unikalius identifikavimo požymius ir pati technologija yra lengvai pritaikoma praktikoje. Biometrinių duomenų naudojimas autentifikavimui nėra naujas dalykas, tai yra tęstinė pirštų atspaudų analizės technologija, kuri buvo naudojama gana ilgai. Daugelis šiuolaikinių išmaniųjų įrenginių, tokių kaip išmanieji telefonai, planšetiniai kompiuteriai, nešiojamieji kompiuteriai, turi biometrinius jutiklius, kurie gali būti panaudoti vartotojo autentifikacijai (pirštų atspaudų jutikliai, vaizdo kamera, garso mikrofonas).

Kai vartotojo autentifikacijai yra naudojamas tik vieno faktoriaus (slaptažodžio) apsaugos mechanizmas, tada tai yra tik kompiuterio skaičiuojamoji užduotis patvirtinti, ar vartotojas įvedė teisingą slaptažodį, ar ne, o autentifikuojant biometriniu būdu yra naudojama tikimybinė metodika, t. y. lyginamas skenuotas pavyzdys su išsaugotu šablonu ir sugeneruojamas procentinis sutapimas, tikrumo rezultatas. Jei tikrumo rezultatas yra didesnis už slenkstinę vertę, yra laikoma, kad įvyko sutapimas ir autentifikavimo procesas teigiamas. Duomenų subjekto autentifikavimo tikslumui pagerinti ir klastojimo galimybėms sumažinti autentifikavimo sistema gali naudoti daugiau kaip vieną subjekto biometrinį požymį arba kompleksinę biometrinių ir ne biometrinių subjekto duomenų sistemą. Atsižvelgiant į aplinkybes, norint autentifikuotis, gali būti privaloma teigiamai patvirtinti visus subjekto požymius (biometrinius ir ne biometrinius) arba tik jų dalį.

Subjekto biometriniams duomenims užfiksuoti reikia specialaus įrenginio, kuris turėtų būti integruotas į kompiuterinę sistemą ar išmanųjį įrenginį, pavyzdžiui, išmaniojo telefono piršto atspaudų skaitytuvas ar bankomatuose integruotas plaštakos linijų išsidėstymo rašto skaitytuvas. Tokie biometriniai duomenys, kaip subjekto veidas ar balsas, gali būti užfiksuojami naudojant bendresnius įrenginius, kaip antai, vaizdo kamera ar mikrofonas, ir gali būti apdorojami vietoje arba persiunčiami tretiesiems asmenims.

Keletas paplitusių biometrinių duomenų saugumo užtikrinimą stiprinančių technologijų – biometrinis šifravimas ir biometrinis „panaikinimas“ (angl. *cancellable*), kai biometriniai duomenys yra sistemiškai iškraipomi, siekiant apsaugoti jautrią subjekto informaciją. Šios technologijos yra pranašesnės, palyginti su tradicinėmis biometrinėmis sistemomis, ypač kalbant apie kaupiamų biometrinių duomenų „atšaukiamumą“ (angl. *revocability*). Taip pat yra kuriamas nuotolinis biometrinio autentifikavimo protokolas. Jis yra patikimesnis susidūrus su sudėtingesnėmis saugumo grėsmėmis. Šis protokolas išsaugo duomenis net tokiu atveju, jei vartotojo įrenginiui ar nuotoliniam serveriui kyla pavojus (bet ne abiem vienu metu).

GRĖSMĖS PRIVATUMUI IR DUOMENŲ APSAUGAI

Vystantis technologinėms naujovėms ir jas pritaikant vartotojų patogumui bei efektyvesniam naudojimui, biometrinių duomenų analizė tampa prieinama, efektyvi, pažangi, sąlyginai nebrangi autentifikavimosi sistema. Tai bene geriausias kaštų ir naudos santykis kokybiškai ir patogiai autentifikuoti duomenų subjektą, nereikalaujant iš jo nieko papildomo, kai reikia vienareikšmiškai nustatyti asmens tapatybę, tačiau tai siejasi ir su tam tikromis grėsmėmis.

Skirtingos biometrinės sistemos duomenų apsaugai ir privatumui turi skirtingą poveikį, todėl reikia detalios rizikų analizės. Pavyzdžiui, veido atpažinimo sistema gali rinkti informaciją apie duomenų subjektus jiems to nežinant, o piršto atspaudų sistemai reikia, kad subjektas aktyviai dalyvautų procese.

Tam tikri biometriniai duomenys gali būti laisvai prieinami trečiosioms šalims, duomenų subjektui to nežinant, pavyzdžiui, palikti pirštų atspaudai ant įvairių paviršių, veido atpažinimas, vaizdų kaupimas. Skirtingai negu slaptažodžiu apsaugotos sistemos, biometriniai duomenys nėra įslaptinti bei lengvai pakeičiami. Duomenų subjektai dažnai yra susipažinę su pavojais, kurie gali kilti paviešinus slaptažodį, bet, nutekėjus biometrinei informacijai, būdai ją sufalsifikuoti, pavyzdžiui, veidą ar balsą, gali būti tiesiog nepraktiški.

Faktas, kad biometrinis autentifikavimas remiasi matematine tikimybe (kaip tiksliai nuskaityti subjekto duomenys sutampa su įrašu), reiškia, kad yra paklaidos ribos. Kai subjekto duomenys nesutampa su įrašu, autentifikavimas yra nepatvirtinamas ir tolimesnis priėjimas prie sistemos yra uždraustas. Paklaidų ribos turi užtikrinti pusiausvyrą tarp sistemos našumo ir saugumo. Jei subjekto duomenų sutapimo slenkstinę vertę nustatysime per aukštą, sistema bus tikslesnė, bet teisėti sistemos vartotojai gali dažniau susidurti su autentifikavimo problemomis. Galima sumažinti sistemos slenkstinės vertės tikslumą, taip sistemą darant našesnę, tačiau sumažės ir sistemos saugumo užtikrinimas.

Specialūs biometriniai įrenginiai ar į asmeninius, nešiojamuosius kompiuterius, išmaniuosius telefonus integruoti komponentai dėl mažesnių gamybos kaštų gali prasčiau užtikrinti saugumą. Tokie žemos kokybės jutikliai turi didesnes paklaidos ribų vertes ir mažina sistemos vartotojų duomenų saugumą ir privatumą. Dauguma tokių jutiklinių sistemų gali būti „apeitos“ panaudojant svetimus ar suklastotus biometrinius duomenis.

Tokiu atveju, kai duomenų subjektas negali pateikti reikiamų biometrinių duomenų, pavyzdžiui, dėl pažeistų pirštų, ar nesutinka pateikti tokių duomenų, pavyzdžiui, dėl išvaizdos, fiksavimo įrenginiui, tolimesnis autentifikavimo procesas yra nutraukiamas.

Dažnai biometriniai duomenys, kaip ir slaptažodžiai, yra saugomi skaitmeniniu formatu centralizuotose sistemose, tačiau tikimybė, kad kaupiami duomenys gali būti nutekinti ar įvyktų vagystė, išlieka. Paviešinti gali būti tiek nuskaityti pirštų atspaudų įrašai, tiek veido atvaizdai ar balso įrašai.

Biometriniai duomenys yra ilgalaikiai ir nėra lengvai pakeičiami ar išduodami naujai, ką nesunkiai galima atlikti su slaptažodžiais, raktinėmis kortelėmis ar žetonais. Kurdamas slaptažodį, duomenų subjektas gali rinktis iš daugybės simbolių, tačiau biometrinių duomenų analizei gali būti panaudota tik keletas žmogaus atributų, pavyzdžiui, dvi akies rainelės, dvi tinklainės, 10 pirštų atspaudų, veidas. Svarbu atkreipti dėmesį, kad, net ir naudojant biometrinius duomenis, išlieka rizika, jog vartotojo paskyros gali persidengti, pavyzdžiui, kai vienąkart nuskaitytas piršto atspaudas yra panaudojamas keliose paslaugų sistemose, ir tai yra analogiška problema slaptažodžius naudojančiose sistemose.

Biometrinių duomenų analizė gali sumažinti galimybę vartotojams naudoti anonimines paskyras. Tai mažina paslaugų pasirinkimą vartotojams, kurie nenori atskleisti savo tikrosios tapatybės, ar vartotojams, kurie nori išlaikyti keletą atskirų paskyrų skirtingiems tikslams, pavyzdžiui, po atskirą paskyrą profesionaliam ar asmeniniam naudojimui.

Apsauga nuo masinių išpuolių, neautorizuoto priėjimo prie duomenų bazių, kaupiančių biometrinius įrašus, taip pat sprendžiant, kaip biometrines sistemas pritaikyti lengvesniam naudojimui, yra vienas iš pagrindinių standartizavimo tikslų. Dauguma privatumą užtikrinančių biometrinių sistemų kaupia biometrinius įrašus lokaliai, galutinių vartotojų įrenginiuose (išmaniuosiuose telefonuose, planšetiniuose kompiuteriuose), todėl turi būti užtikrinta, kad lokaliai kaupiami biometriniai duomenys būtų apsaugoti, užtikrintas duomenų saugumas.

Biometrinių sistemų gamintojai vis dar pasitiki algoritmų slaptumu, skirtu duomenų apsaugai. Privatūs gamintojų algoritmai ir technologijos, kurių stiprumas paremtas algoritmų įslaptinimu, bendrai paėmus, yra mažiau verti pasitikėjimo, negu tie, kuriuos nepriklausomai prižiūri trečioji šalis ar yra visuotinai pripažinti standartai.

REKOMENDACIJOS

1. Valstybinės, verslo ir kitos organizacijos, siekiančios naudoti biometrinius duomenis duomenų subjektų autentifikavimui, turi padrąsinti kurti tokias biometrines asmenų privatumą ir duomenų saugumą užtikrinančias autentifikavimo technologijas, kurios pakeistų mažiau saugias, slaptažodžiais paremtas autentifikavimo technologijas.

2. Iniciatyvūs privatumo įrankiai, tokie kaip privatumo poveikio vertinimas (angl. *privacy impact assessments*), pritaikytoji duomenų apsauga (angl. *privacy by design*) bei standartizuotoji duomenų apsauga (angl. *privacy by default*), turi būti skatinami, palaikomi rengiant gaires ir reikalaujami teisiškai.

3. Paslaugų teikėjai, programinės įrangos kūrėjai ir techninės įrangos gamintojai skatinami domėtis ir produktuose naudoti modernias duomenų privatumą stiprinančias technologijas, o ypač – naudojant biometrinius duomenis. Turi būti konsultuojamasi su duomenų apsaugos pareigūnais ir privatumo specialistais, jie turi būti įtraukiami į ankstyvas biometrinių sistemų kūrimo pakopas ir nuolat atliekami poveikio privatumui vertinimai.

4. Organizacijos, kuriančios biometrines autentikavimo sistemas, turėtų atsisakyti biometrinių šablonų kaupimo centrinėse duomenų bazėse ar panašiose saugyklose. Idealiausias sprendimas būtų kaupti lokalius biometrinius šablonus saugiu metodu (pavyzdžiui, kaip pagalbinius duomenis arba kaip pakeistus duomenis panaikinamojoje biometrijoje). Labai svarbu, kad autentikavimas vyktų lokaliai ir kad biometriniai duomenys (jutiklių duomenys ar šablonai) būtų tik biometriniame įrenginyje.

5. Biometrinės sistemos turi būti sukurtos taip, kad nuskaityti neapdoroti (angl. *raw data*) biometriniai duomenys būtų saugiai ištrinami, kai tik sugeneruojamas biometrinis šablonas, nebent atsirastų specifinių duomenų išsaugojimo reikalavimų. Kai vartotojo paskyra išjungiama ar panaikinama, biometriniai šablonai (biometriniai duomenys) turi būti saugiai ištrinami. Techninės įrangos gamintojai turi pasiūlyti saugius būdus biometriniams šablonams naikinti galutinių vartotojų įrenginiuose.

6. Biometrinės sistemos, kai tik įmanoma, turi būti standartizuotos. Standartai yra keletą kartų peržiūrimi, patikrinami ir įvertinami, taip užtikrinant aukštesnę kokybę ir sąveiką.

7. Jei tik įmanoma, biometrinių sistemų techninė ir programinė įranga turi būti išsamiai dokumentuota ir, prireikus, lengvai prieinama.

8. Siekiant apsisaugoti nuo vidinių ir išorinių sistemos atakų, biometrinėse sistemos turi būti įgyvendintos atitinkamos moderniausios fizinės, techninės ir organizacinės apsaugos priemonės. Biometriniams šablonams kaupti organizacijose turi būti naudojami specializuoti apsaugos moduliai.

9. Biometrinių paslaugų tiekėjai registracijos ir autentifikavimo metu privalo apriboti kaupiamų ir apdorojamų asmens biometrinių duomenų kiekį.

10. Paslaugos tiekėjai, kurie naudoja biometrinius duomenis autentifikavimui, turi informuoti savo klientus apie naudojamus privatumo ir apsaugos mechanizmus, t. y. turi būti pateikta informacija, kas yra programinės ir techninės įrangos gamintojai, kokie apsaugos metodai ir biometrinių duomenų kaupimo moduliai yra naudojami, kokios paklaidų ribos ir koks biometrinių duomenų saugojimo laikotarpis.

11. Tarp kaupiamų duomenų keliose biometrinėse sistemose neturi būti jokio ryšio, kuriuo remiantis būtų galima atsekti, identifikuoti sistemos vartotojus. Tai svarbu, kai biometrinių sistemų paslaugos tiekėjas diegia identiškas sistemas skirtingiems klientams.

12. Atsižvelgiant į situaciją, biometrinės sistemos turi būti testuojamos su realiais biometriniais duomenimis tik diegimo vietoje. Organizacijos privalo užtikrinti, kad eksploatacinės savybės ir tikslumo lygiai yra tinkami.

13. Biometrinės sistemos turi būti parengtos taip, kad vartotojų autentikavimas būtų praktiškas ir paprastas naudoti. Svarbu atkreipti dėmesį, kad paslaugų tiekėjai privalo užtikrinti alternatyvią (ne biometrinę) autentikavimo galimybę, atsižvelgiant į saugumo lygį.

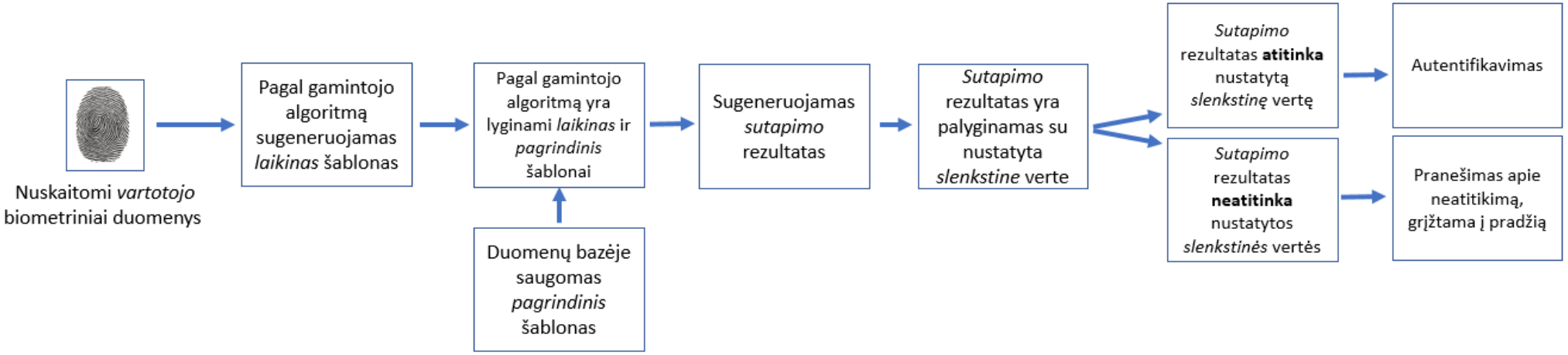
14. Biometrinių paslaugų tiekėjai privalo operatyviai reaguoti į saugumo ir privatumo spragas biometrinėse sistemose. Saugumas ir privatumas biometrinėse sistemose turi būti aktyvuojamas pagal nutylėjimą.

15. Biometrinių sistemų vartotojai privalo susipažinti su pasirinkto biometrinių sistemų paslaugos tiekėjo reikalavimais, autentifikavimo būdais, biometrinių duomenų naudojimo taisyklėmis, saugumo ir privatumo savybėmis prieš pradėdami naudoti biometrinių sistemų paslaugas.

Toliau paveiksle yra pateikta tipinio biometrinio patikrinimo procedūra. Iš pradžių vartotojas pateikia savo biometrinius duomenis skaitytuvui, kuris duomenis nuskaito, ir, panaudodamas gamintojo algoritmus, sugeneruoja *laikinąjį* duomenų šabloną. *Laikinasis* duomenų šablonas yra lyginamas su *pagrindiniu* duomenų šablonu, kuris buvo sukurtas vartotojui registruojantis sistemoje. Pagal gamintojo algoritmus yra sugeneruojamas *laikinojo* ir *pagrindinio* duomenų šablonų sutapimo rezultatas. Sugeneruotas sutapimo rezultatas yra palyginimas su biometrinėje sistemoje nustatyta *slenkstine* verte. Atsižvelgiant į tai, kokia nustatyta *slenkstinė* vertė ir koks sutapimo rezultatas, vartotojas gali būti autentifikuotas arba pranešama apie autentifikacijos klaidą, vartotojo biometrinių duomenų neatitikimą ir grįžtama į biometrinio proceso patikrinimo pradžią.

TIPINIO BIOMETRINIO PROCESO PATIKRINIMO EIGA

Paveikslas. Tipinio biometrinio patikrinimo procedūra



LITERATŪRA

- Biometrics in Online Authentication, International Working Group on Data Protection in Telecommunications. Berlin (Germany), 60th meeting, 22–23 November 2016.
- Cancellable biometrics add a repeatable distortion to the stored template, e. g. see Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. Biometric perils and patches. Elsevier, 2002, Vol. 35, p. 2727–2738.
- SOUTAR, Colin; ROBERGE, Danny; STOIANOV, Alex; GILROY, Rene; KUMAR, B.V.K. Vijaya. Biometric Encryption. McGraw-Hill, 1999.
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf
- http://www.lstp.lt/sites/www.lstp.vgtu.lt/files/Biometrines%20technologijos%20-%2013_03_16%20(Kaklauskas)%20%5BCompatibility%20Mode%5D_0.pdf
- www.maf.vu.lt/~bastys/academic/ATE/biometrika/
- http://www.mita.lt/uploads/documents/eureka/biomet_security_ataskaita.pdf
- NANAVATI, Samir; THIEME, Michael; NANAVATI, Raj. Biometrics: Identity Verification in a Networked World. Wiley, 2002, 1 edition (April 4, 2002), ISBN: 978-0-471-09945-1, 320 p.
- SYTA et al. Private Eyes: Secure Remote Biometric Authentication. 2015, http://dedis.cs.yale.edu/dissent/papers/secrypt15-biometric.pdf.
- http://www.upc.smm.lt/naujienos/ikt/konferencija/Intelektini%C5%B3_ir_biometrini%C5%B3_technologij%C5%B3_taikymas_mokymo_procese.pdf