ASMENS TAPATYBĖS KORTELĖ IR ELEKTRONINIS PARAŠAS

Parengta pagal Lietuvos Respublikos vidaus reikalų ministerijos, Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos, Asmens dokumentų išrašymo centro prie Lietuvos Respublikos vidaus reikalų ministerijos ir projekto „Bibliotekos pažangai“ pateiktą medžiagą.

Kaip pasirašyti dokumentą elektroniniu parašu?

Elektroninis parašas

Elektroninio parašo kūrimą, tikrinimą, galiojimą, parašo naudotojų teises ir atsakomybę reglamentuoja Lietuvos Respublikos elektroninio parašo įstatymas.

Elektroninio parašo galia

Saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme.

Elektroninis dokumentas

Elektroninio dokumento, pasirašyto elektroniniu parašu, specifikacija yra patvirtinta Lietuvos archyvų departamento direktoriaus įsakymu.

Elektroninis dokumentas sukuriamas naudojant asmens tapatybės kortelės (ATK) kvalifikuotą e. parašo sertifikatą ir specialią programinę įrangą SIGNA, kuri laisvai platinama ir ją galima atsisiųsti iš sertifikavimo centro, kurio funkcijas vykdo Gyventojų registro tarnyba, prie Vidaus reikalų ministerijos puslapio www.nsc.vrm.lt. Skiltyje „Elektroninio parašo formavimo ir tikrinimo programinė įranga“ pateikiama SIGNA programinis paketas ir jo naudojimo instrukcija. Programinę įrangą SIGNA reikia įdiegti kompiuteryje.

Elektroninio dokumento pasirašymas

Programinė įranga SIGNA atitinka Lietuvos archyvų departamento patvirtintus reikalavimus elektroniniam dokumentui ir ją galima pasirašyti elektroninius dokumentus, kurių formato plėtiniai yra – .docx. xlsx, pptx (*Microsoft Open Office XML*), .odt, .ods, .odp (Open Office); .pdf; .tif; .jpg.

Naudojant SIGNA, elektroninių dokumentų pasirašymo įranga sukuriamas ADOC formato elektroninis dokumentas. Norint perskaityti šio formato dokumentus, kompiuteryje turėtų būti įdiegta SIGNA programinė įranga.

Kiekvienoje naujo pavyzdžio (įsigytos 2009 m. ir vėliau) asmens tapatybės kortelėje (ATK) yra du sertifikatai – asmeniui identifikuoti elektroninėje erdvėje ir kvalifikuotas sertifikatas elektroniniams dokumentams pasirašyti. ATK pasinaudoti galima dviem būdais:

- asmeniniame kompiuteryje;
- nemokamai visuose viešosiose interneto prieigos taškuose (VIPT).

Trumpa informacija apie asmens tapatybės kortelę pateikiama ATK lankstinuke (1 paveikslas).

Lankstinukas .pdf formatu skelbiamas Ugdymo plėtotės centro interneto svetainėje prie šios metodinės medžiagos – failas *ATK 2009 LT.pdf*.

Norint pasinaudoti ATK asmeniniame kompiuteryje, reikia

- kompiuterio,
- ATK skaitytuvo,
- aktyvaus ATK sertifikato (voko su pin kodu).

Kompiuteris turi būti prijungtas prie interneto. Naudotojui turi būti suteiktos administratoriaus teisės.

Kortelės skaitytuvas gali būti įmontuotas kompiuteryje, klaviatūroje ar jungiamas atskira jungtimi kaip išorinis įrenginys (2 paveikslas).

Kortelių skaitytuvo programinė įranga turi atitikti kompiuterio programinę įrangą.

Antros pusės aprašymas

12. Optiškai kintantys dažai
Dizaino elementas atspausdintas dažais, kurie keičia spalvą žiūrint skirtingu kampu.

13. Vaivorykštinė spauda
Kortelės abi pusės yra padengtos apsauginiais tinkleliais, atspausdintais vaivorykštine spauda.

14. Brūkšninis kodas
Kortelėje yra įrašomas brūkšninis kodas.

15. Kortelės numeris
Kortelės numeris iš aštuonių skaitmenų.

16. Ultravioletiniai dažai
Dizaino elementas ir tekstas „LIETUVOS RESPUBLIKA“, atspausdinti nematomais dažais, švyti UV šviesoje.

LIETUVOS RESPUBLIKA
ASMENS TAPATYBĖS KORTELĖ

Asmens tapatybės kortelė (toliau – ATK) pagaminta iš polikarbonato, į kurį įdiegtos kontaktinė ir nekontaktinė elektroninės laikmenos. Duomenys polikarbonate išgraviruojami lazeriniu įrenginiu.

ATK paskirtį, jos išdavimo, keitimo, naudojimo ir galiojimo sąlygas, joje įrašomus duomenis reglamentuoja Lietuvos Respublikos asmens tapatybės kortelės įstatymas (Žin., 2001, Nr. 97-3417; 2008, Nr. 76-3007).

ATK yra pagrindinis asmens tapatybę ir pilietybę patvirtinantis dokumentas, privalomas kiekvienam Lietuvos Respublikos piliečiui, kuriam sukako 16 metų, ir neturinčiam iki 2003 m. sausio 1 d. išduoto Lietuvos Respublikos piliečio paso. Prireikus, ATK gali būti išduodama ir piliečiui, nesulaukusiam 16 metų. ATK privaloma šalies viduje ir gali būti naudojama vykti į užsienio valstybes, su kuriomis yra sudarytos atitinkamos tarptautinės sutartys ar susitarimai.

Piliečiui nuo 16 metų išduota ATK galioja 10 metų. Piliečiui iki 16 metų išduota ATK galioja ne ilgiau kaip 5 metus.

ATK, išduodama nuo 2009 m. sausio 1 d., atitinka 2004 m. gruodžio 13 d. Europos

Tarybos (ET) reglamento Nr. 2252/2004, nustatančio valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartus, reikalavimus bei Tarptautinės civilinės aviacijos organizacijos (ICAO) rekomendacijas.

Asmens tapatybės kortelės patikra

Lietuvos Respublikos vardu prašome valstybes neturinčias galimybių nuskaityti

ATK įrašytą skaitmeninę informaciją ar asmens pirštų atspaudus, nesudaryti kliūčių Lietuvos Respublikos piliečiui keliauti ar teisėtai naudoti ATK, kai patikrinama ATK tradiciniais būdais nekyla abejonių dėl šio dokumento autentiškumo ir jį pateikusio asmens tapatybės.

Asmens dokumentų išrašymo centras
prie Vidaus reikalų ministerijos
Žirmūnų g. 1D, LT-09229 Vilnius
LIETUVA

LIETUVOS RESPUBLIKA
ASMENS TAPATYBĖS KORTELĖ

REPUBLIC OF LITHUANIA
PERSONAL IDENTITY CARD

2009

1 a pav. *Lankstinuko apie asmens tapatybės kortelę viena pusė*

Pirmos pusės aprašymas

1. Specialus linijų išdėstymas
Trijų spalvų apsauginiai tinkleliai.

2. Vaivorykštinė spauda
Kortelės abi pusės yra padengtos apsauginiais tinkleliais, atspausdintais vaivorykštine spauda.

3. Mikrotekstas
Pasikartojantis mikrotekstas „LIETUVOS RESPUBLIKA“ suformuoja savarankišką liniją kortelės viršuje.

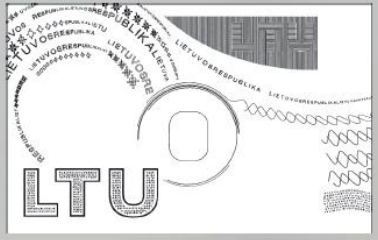
4. Kinegrama
Difrakcinis optinis elementas su kinematiniu efektu.

5. Ultravioletiniai dažai
Dizaino elementas ir tekstas „LIETUVOS RESPUBLIKA“, atspausdinti nematomais dažais, švyti UV šviesoje.

6. Duomenys, veido atvaizdas ir parašas
Duomenys, veido atvaizdas ir parašas graviruojami lazeriu.

7. Daugialypis lazerinis vaizdas
Atkartotas veido atvaizdas pakreipus kortelę transformuojasi į triženklį valstybės kodą „LTU“.

8. Kortelės reljefas
Kortelės reljefas suformuotas pozityviniu (iškilusiu) ir negatyviniu (įdubusiu) įspaudimu.



9. Optiškai kintantys dažai
Dizaino elementai atspausdinti dažais, kurie keičia spalvą žiūrint skirtingu kampu.

10. Nekontaktinė elektroninė laikmena
Nekontaktinėje elektroninėje laikmenoje įrašyti biometriniai duomenys: veido atvaizdas ir pirštų atspaudai.

Veido atvaizdas įrašytas JPEG2000 formatu ir atitinka išgraviruotąjį veido atvaizdą.

Informacija apie šalies sertifikavimo įstaigos (CSCA) sertifikatą publikuojama interneto tinklalapyje adresu: www.csca.lt.

Sertifikatai, skirti sertifikuoti pirštų atspaudų nuskaitymo įrangą, išduodami dvišalių sutarčių pagrindu.

11. Kontaktinė elektroninė laikmena
Kontaktinėje, Europos piliečio kortelės specifikacijas atitinkančioje elektroninėje laikmenoje, įrašyti asmens atpažinimo elektroninėje erdvėje ir kvalifikuotas, elektroniniam parašui skirtas, sertifikatai.

1 b pav. *Lankstinuko apie asmens tapatybės kortelę kita pusė*

Asmens tapatybės kortelės skaitytuvai

2 a pav. *Asmens tapatybės kortelės skaitytuvai jungiami prie kompiuterio kaip atskiri įrenginiai USB jungtimi*

2 b pav. *Integruoti į klaviatūrą arba įmontuojami į kompiuterį asmens tapatybės kortelės skaitytuvai*

2 c pav. *PC card arba Express Card*

Populiariausi gamintojai

Advanced card System Ltd (http://www.acs.com.hk/)
Gemalto Ltd (http://www.gemalto.com/products/pc_link_readers/)
TX Systems Ltd (https://www.txsystems.com/)

Yra daugiau gamintojų, kuriuos galima rasti internete, paieškai pasirinkus *Smart Card Reader*.

Kortelių skaitytuvai turi atitikti tarptautinį standartą pripažintą Lietuvoje LST ISO/IEC 7816 „Atpažinimo kortelės. Lustinės kortelės su kontaktais“ (ISO 7816 *Smart Card Standart*).

Kortelių skaitytuvų programinė įranga

Kortelių skaitytuvų programinė įranga turi atitikti kompiuterio programinę įrangą ir yra gamintojo / pardavėjo pateikiama kartu su skaitytuvu (dažniausiai CD) arba ją galima atsisiųsti iš gamintojo internetinio svetainės.

Diegiant kortelių skaitytuvų programinę įrangą, turi būti suteikta administratoriaus teisė.

Kortelės sertifikatai aktyvuojami gaunant ATK kai pasirašote, jog sutinkate, kad sertifikatai būtų aktyvūs. Išduodamas vokas su 8 skaičių PIN kodu, kurį reikės surinkti kiekvieną kartą naudojantis ATK sertifikatais.

Daugiau informacijos rasite čia.

Lietuvos Respublikos piliečiai, kurie jau naudojasi arba ketina naudotis asmens tapatybės kortelėmis elektroniniam pasirašymui ar asmens identifikavimui elektroninėje erdvėje, turėtų nepamiršti, kad sertifikatas kortelėje galioja 3 metus (tokią galimybę gyventojams, kurie įsigijo korteles 2009 m. ir vėliau, suteikia naujo pavyzdžio kortelėse įdiegta sertifikavimo sistema (kontaktinis ir nekontaktinis lustai). Praėjus šiam laiku nuo kortelės išdavimo gyventojas turi kreiptis į apskričių centrus arba Gyventojų registro tarnybą prie LRVRM dėl kortelės sertifikato atnaujinimo. Atnaujinti sertifikatą nėra privaloma, tai aktualu tiems asmenims, kurie sertifikatu naudojasi. Kortelės sertifikato atnaujinimo paslauga yra nemokama.

Kortelės ir sertifikatų programinė įranga

Kortelės programinė įranga

Asmens tapatybės kortelės kontaktiniame luste (mikroprocesoriuje) įdiegta *Gemalto MultiApp ID Core Technology* operacinė sistema (OS).

Įsidiekite savo kompiuteryje atitinkamą Jūsų kompiuterio operacinei sistemai ATK programinę įrangą „*Middleware for Gemalto Sealys Multi App ID Classic Client 5.2* (*Gem Safe 5.2*), kurią nemokamai galite atsisiųsti pagal atitinkamas nuorodas:

- Classic Client Toolbox 32 bitų versija (Windows 2000 Professional / XP Home / XP Professional / Vista / Server 2000 / Server 2003) (9 MB);
- Classic Client Toolbox 64 bitų versija (Windows XP Professional / Vista / Server 2003) (14 MB);
- Classic Client LINUX (6 MB).

Pagal pateiktas nuorodas, ATK programinė įranga yra imama iš Asmens dokumentų išrašymo centro (ADIC) prie VRM serverio. Ši programinė įranga taip pat pasiekiama www.dokumentai.lt.

Neturite kompiuterio arba dar nesate įsigiję kortelių skaitytuvo?

Jei neturite kompiuterio, interneto ryšio ar dar nesate įsigiję kortelių skaitytuvo, nemokamai elektroninėmis paslaugomis galite pasinaudoti Viešuose interneto prieigos taškuose (VIPT sąrašas http://www.nsc.vrm.lt/docs/Bibliotekos.pdf). Daugiau informacijos apie VIPT galima rasti adresu www.vipt.lt.

Naudokitės ATK teikiamomis galimybėmis!

Filmas „Asmens tapatybės kortelė. El. paslaugos ir el. parašas“. Filmą galite rasti adresu http://kursai.bibliotekospazangai.lt/content/asmens-tapatybes-kortele-el-paslaugos-ir-el-parasas arba Ugdymo plėtotės centro svetainėje prie šių metodinių rekomendacijų – failas *Asmens tapatybės kortelė. El. paslaugos ir el. parašas.mp4*.

Elektroninio dokumento, pasirašyto elektroniniu parašu, saugumas ir vientisumas

Elektroninio dokumento, pasirašyto elektroniniu parašu, saugumas ir vientisumas užtikrinamas specialiais kodavimo metodais, pasirašant elektroninį dokumentą. Koduojamas ne visas tekstas, o taip vadinama *HashValue („sumaišyta vertė“)*, kuri specialiu būdu paskaičiuojama iš viso teksto. Paprasčiausiai atliekamą procesą galima paaiškinti taip – raidės keičiamos skaičiais pagal jų vietą abėcėlėje ir paskaičiuojama tų skaičių suma. Pavyzdžiui:

Raidė	***S***	***E***	***R***	***T***	***I***	***F***	***I***	***K***	***A***	***T***	***A***	***S***	***Suma***
Raidės vieta abėcėlėje	19	5	18	20	9	6	9	11	1	20	1	19	**138**

Priklausomai nuo kodavimo metodo pasirenkami atitinkami algoritmai (pvz.: SHA, SHA-256 ar RIPEMD-160, *SHA – Secure Hash Algorithm*).

Teksto „SERTIFIKATAS“, pasirašyto elektroniniu parašu, naudojant SHA-256 kodavimo algoritmą, *HashValue* atrodytų taip:

2253cb58f95672905f8c4ac58373851d6df735b60f81c6297550f2091163a4c4 (*HashValue* išraiška įprastai pateikiama šešioliktainių skaičių sistemoje (*HashValue* paskaičiuotas pasinaudojant on-line *hashing* generatoriumi).