

VENDIM
Nr.469, datë 6.5.2009

**PËR PËRCAKTIMIN E ELEMENTEVE TË SIGURISË DHE PËR MIRATIMIN E
FORMËS E TË MODELIT TË LEJES SË QËNDRIMIT PËR SHTETASIT E HUAJ**

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 4 të nenit 22 të ligjit nr.9959, datë 17.7.2008 “Për të huajt”, me propozimin e Ministrit të Brendshëm, Këshilli i Ministrave

VENDOSI:

1. Përcaktimin e elementeve të sigurisë së lejes së qëndrimit, sipas aneksit 1, që i bashkëlidhet këtij vendimi.
2. Miratimin e formës e të modelit të lejes së qëndrimit, sipas aneksit 2, që i bashkëlidhet këtij vendimi.
3. Ngarkohet Ministria e Brendshme për zbatimin e këtij vendimi.
Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
Sali Berisha
Aneksi 1

1. Lloji i lejes së qëndrimit
Leja e qëndrimit do të jetë në formën e kartës, me një chip elektronik.
2. Elementet e sigurisë të vendosura në lejen e qëndrimit
 - GUILLOCHE (1). Në të dyja anët e lejes së qëndrimit do të jetë një kompozicion kompleks vijash GUILLOCHE.
 - RAINBOW (2). Kompozicioni Guilloche do të realizohet me teknikën e transformimit gradual të ngjyrave me teknikën RAINBOW.
 - Bojë OVI (3) (Bojërat e ndryshueshme optike). Harta e Republikës së Shqipërisë e printuar me bojë speciale OVI.
 - Fotografi Ghost (4) (hije). Fotografi e mbajtësit të lejes së qëndrimit në përmasa sa 1/3 e përmasave të fotografisë kryesore.
 - Shtresë mbrojtëse transparente me shenja optikisht të variueshme (5) e aplikuar në të dyja anët e kartës përgjatë gjithë sipërfaqes (6).
 - Bojë UV. Një simbol i printuar me bojë të dukshme, me sipërfaqe 100 mm², vetëm nën dritën ultravjollcë.
 - Mikrotekst i padukshëm me sy të lirë, por i lexueshëm me lupë me zmadhim 10 herë. Ky element sigurie, përveçse i paraprintuar në lejen e qëndrimit, do të realizohet edhe gjatë procesit të personalizimit.
3. Chipi i lejes së qëndrimit
Leja e qëndrimit do të pajiset me një chip të vendosur në brendësi të trupit të lejes së qëndrimit dhe do të jenë në përputhje me standardet:
 - ISO/ICE 7810 (Kartat e identifikimit – Karakteristikat fizike);
 - ISO 10373 (Kartat e identifikimit – Metodat e testimit të chip-it me/pa kontakt);
 - ISO 7501-3 (Kartat e identifikimit – Dokumentet e udhëtimit të lexueshme nga makina).
1. Vizatimi i dizajnit me vija të holla të vazhduara.
2. Printimi i dizajnit duke siguruar variacion progresiv të ngjyrave. Kjo teknikë realizon kalimin gradual të ngjyrave nëpërmjet shkrirjes së tyre.
3. Bojërat e ndryshueshme optike përmbajnë shtresa shumë të vogla të një filmi special, i cili ndryshon ngjyrë nëse shihet në kënde të ndryshme.
4. Një riprodhim me gjysmë toni i imazhit origjinal, që printohet në të njëjtin vend ku janë të vendosura të dhënat personale të mbajtësit të Lejes së Qëndrimit.
5. Imazhe dhe shkrime në volum të krijuara nga fenomeni i përthyerjes së dritës. Imazhet shfaqen dhe/ose ndryshojnë ngjyrë në varësi të këndit të shikimit (të përthyerjes së dritës) dhe të

krijojnë idenë e lëvizjes së tyre.

6. Tolerancat e nevojshme të aplikimit të kësaj shtrese do të përcaktohen me saktësi në momentin e lidhjes së kontratës.

Chipi do të ketë dy ndërfaqe komunikimi:

- Me kontakt – në përputhje me standardin:

- ISO 7816 pjesa 1 (Kartat e identifikimit – qarku i integruar – Karakteristikat fizike).

- ISO 7816 pjesa 2 (Kartat e identifikimit – Qarku i integruar – Dimensionet dhe pozicionimi i kontaktit të chip-it).

- ISO 7816 pjesa 3 (Kartat e identifikimit – Qarku i integruar – Ndërfaqja elektrike dhe protokollet e transmetimit).

- ISO 7816 pjesa 4 (Kartat e identifikimit – Qarku i integruar, organizimi, siguria dhe komandat për ndërveprim).

- Pa kontakt - në përputhje me standardin:

- ISO 14443 pjesa 1 (Kartat e identifikimit – Qarku i integruar, pa kontakt – Karakteristikat fizike).

- ISO 14443 pjesa 2 (Kartat e identifikimit – Qarku i integruar pa kontakt – Fuqia e radio-frekuencës dhe ndërfaqja e sinjalit).

- ISO 14443 pjesa 3 (Kartat e identifikimit – Qarku i integruar pa kontakt – Inicializimi dhe antikolizioni).

- ISO 14443 pjesa 4 (Kartat e identifikimit – Qarku i integruar pa kontakt – Protokolli i transmetimit).

Chipi duhet të jetë i certifikuar minimalisht CC EAL4+

- JAVA do të jetë gjuha e programimit dhe e zhvillimit të aplikacioneve në chip, dhe do të suportojë:

- specifikimet e *GlobalPlatform* v 2.1.1;

- Specifikimet e Kartës Java minimalisht versionin 2.2.1

Ruajtja e të dhënave në chip

- Kapaciteti i chip-it do të jetë minimumi 72 KB.

- Ruajtja në chip dhe leximi nga chip-i i të dhënave do të realizohen në mënyrë të sigurtë në përputhje me standardin:

- ISO 7816 pjesa 4 (Kartat e identifikimit – Qarku i integruar organizimi, siguria dhe komandat për ndërveprim).

- ISO 7816 pjesa 8 (Kartat e identifikimit – Qarku i integruar - Komandat për veprimet e sigurisë).

Të dhënat në lejen e qëndrimit do të ruhen në një strukturë hierarkike të bazuar në file (skedarë) duke suportuar karakteristikat e mëposhtme:

- Sistem skedarësh hierarkik me shumë nivele sipas standardit ISO 7816-4 me një Skedar Kryesor (Master File-MF) si rrënjë.

- Mundësinë për të krijuar Skedarë të Dedicuar (Dedicated Files-DF) dhe Skedarë Elementare (Elementary Files-EF) aq sa nevojiten dhe memoria e chip-it mund të mbartë.

- Mundësinë e krijimit të EF nën MF dhe/ose DF të zgjedhur.

- Informacioni në chip ruhet në Strukturën Logjike të të Dhënave (SLD) bazuar në standardet e zhvilluara nga ICAO dhe të dokumentuara në “ICAO NTWG, zhvillimi i LDS për teknologjinë opsionale të shtimit të kapaciteteve, raporti teknik, përsëritje 1.7, 18 maj 2004”. I gjithë informacioni i printuar në lejen e qëndrimit do të ruhet edhe në chip.

- Jetëgjatësia e lejes së qëndrimit me chip do të jetë 10 vjet. Chip-i i lejes së qëndrimit duhet të sigurojë minimalisht:

- 100 000 cikle leximi të memories;

- 20 000 futje në lexuesin e chip-it me kontakt.

Siguria – Kriptografia (në chip)

Platforma e chip-it dhe aplikacionet e vendosura në të duhet të plotësojnë kërkesat e sigurisë për modulet kriptografike në përputhje me specifikimet e FIPS 140-2, minimalisht niveli i dytë.

Aplikimi i chip-it do të shfytëzojë kriptografinë simetrike dhe asimetrike (PKI).

Kriptografia simetrike do të realizohet nëpërmjet përdorimit të algoritmit 3 DES.

Kriptografia simetrike do të përdoret nëpërmjet ndërfaqes *GlobalPlatform* për të dhënë autorizimin e nevojshëm sistemeve administrative të lejes së qëndrimit. Nëpërmjet kësaj kriptografie do të mbrohen dhe sigurohen funksionet e mëposhtme:

- Menaxhimi i aplikacioneve të lejes së qëndrimit – ngarkimi/fshirja e aplikacioneve të lejes së qëndrimit.

- Menaxhimi i ciklit të lejes së qëndrimit – aktivizimi/kyçja e lejes së qëndrimit dhe e aplikimeve të saj.

- Përditësimi i të dhënave të lejes së qëndrimit.

Kriptografia simetrike do të përdoret edhe për të ruajtur konfidencialitetin dhe integritetin e komunikimit midis ndërfaqes pa kontakt të kartës dhe lexuesit, duke evituar në këtë mënyrë përgjimin dhe marrjen e të dhënave në mënyrë të paautorizuar (data skimming/eavesdropping).

Kriptografia asimetrike (PKI) do të realizohet nëpërmjet algoritmit RSA duke përdorur çelsa me gjatësi 2048 bit. Kriptografia asimetrike do të përdoret për të mbrojtur chip-in dhe të dhënat e tij duke përdorur metodat e përshkruara në raportin teknik të ICAO.

“PKI për dokumentet e udhëtimit të lexueshme nga makina duke ofruar akses vetëm për lexim të chip-it (ICC). vl.1”.

Chip-i duhet të suportoje gjenerimin e çelësve RSA.

Chip-i duhet të jetë i aftë të ruajë në të ardhmen dy certifikata X.509, një për firmën digjitale dhe tjetrin për inkriptimin e të dhënave. Për të dyja certifikatat, në chip do të ruhen edhe dy çelësat korrespondues privatë RSA.

PIN-i (Numri personal i identifikimit)

Do të jenë dy PIN-e të vlefshme për lejen e qëndrimit:

- PIN-i mbajtësit të lejes së qëndrimit; përdorimi i këtij PIN-i do të:

- japë autorizimin e mbajtësit për të aksesuar informacione të caktuara (si p.sh. të dhënat biometrike) nëpërmjet ndërfaqes me kontakt;

- mbrojë aksesin në operacionet PKI që konfirmojnë identitetin e mbajtësit të kartës (firmosja digjitale dhe operacionet e inkriptimit).

- PIN-i administrativ, që do të përdoret për të zhbllokuar lejen e qëndrimit kur kjo e fundit është bllokuar.

4. Të dhënat biometrike

- Fotografia e mbajtësit:

- printohet me ngjyra në anën e përparme të lejes së qëndrimit;

- ruhet në chip në përputhje me standardin ISO/IEC 19794-5: 2005 (Teknologjia e informacionit – Formatet e shkëmbimit të të dhënave biometrike – Të dhënat e imazhit të fytyrës) e kompresuar në formatin JPEG.

- Shenjat e dy gishtave (nga 0-14 vjeç) ruhen si imazhe digjitale në chip, sipas standardit ISO/IEC 19794-4: 2005 (Teknologjia e informacionit – Formatet e shkëmbimit të të dhënave biometrike – Të dhënat e imazhit të shenjave të gishtit), e kompresuar në formatin WSQ.

- Të dhënat biometrike duhet të jenë në përputhje me ICAO 9303, Iso 7501-3 dhe specifikimet e BE për pasaportën elektronike.

Aneksi 2

1. Forma dhe përmasa

Karta e identitetit do të jetë e formatit ID-i e përcaktuar në standardin ISO 7810 me këto përmasa:

Gjerësia 85.60 mm,

Lartësia 53.98 mm,

Trashësia 0.76 mm (ISO 7813)

Qoshe të harkuara me rreze 3.18 mm (ISO 7813).

2. Përbërja e kartës

Kompozimi i materialit të lejes së qëndrimit do të jetë në përputhje me standardin ICAO 9303

dhe ISO 7810.

Leja e qëndrimit do të jetë vetëm e ndërtuar nga disa shtresa.

Teknologjia e bashkimit të shtresave të lejes së qëndrimit të sigurojë formimin e një trupi të vetëm dhe të pandashëm.

Leja e qëndrimit e kompozuar në këtë mënyrë, me disa shtresa, me chip duhet të ketë karakteristikat e mëposhtme:

- Jetëgjatësi minimale 10 vjet;
- Rezistencë në temperaturë nga - 25°C në +85°C;
- Rezistencë mekanike në përkulje >50 000 përkulje e përcaktuar në standardin ISO 10373;
- Trupi i lejes së qëndrimit të jetë “UV Dull”¹.

Leja e qëndrimit ka dy faqe.

Në faqen e përparme:

- fotografia e mbajtësit,
- fotografia hije e mbajtësit në përmasa sa një e treta e përmasave të fotos kryesore (në sipërfaqe sa një e nënta e sipërfaqes së fotos kryesore) e realizuar me teknikën GHOST,
- poshtë fotografisë së mbajtësit do të jetë vendi ku do të vendoset nënshkrimi i mbajtësit,
- në qendër të dokumentit si sfond do të jetë shqiponja dykrenore, e paraprintuar,
- do të jetë e vendosur e paraprintuar me teknikën OVL një rresht me bedena.
- do të jenë emërtimet e përbërësve të gjendjes civile me shkronja të vogla të shtypit.

Në gjuhën shqipe:

- emri, mbiemri, datëlindja, vendlindja, gjinia, numri i identitetit, numri i lejes së qëndrimit, motivi, data e lëshimit, data e skadimit, autoriteti.

Në gjuhën angleze:

- given name, family name, date of birth, place of birth, gender, personal number, RP number, purpose, date of issue, date of expiry, authority.

- Shkrime të tjera të paraprintuara REPUBLIKA E SHQIPËRISË, LEJE QËNDRIMI, REPUBLIC OF ALBANIA, RESIDENT PERMIT

- Mikrotex i paraprintuar do të jetë tekst me sipërfaqe totale shkrimi 100 mm².

2.- Në faqen e pasme të lejes së qëndrimit do të jenë:

- Chip-i me kontakt. Përmasat e chip-it dhe vendosja e tij në leje qëndrimi do të jenë në përputhje me standardin ISO 7816.

- Do të jenë emërtimet e përbërësve të gjendjes civile të prindërve/kujdestarit të minorenëve të moshës 0-14 vjeç, me shkronja të vogla të shtypit:

Në gjuhën shqipe:

- emri, mbiemri, numri i identitetit, lidhja me minorenin (atësia, amësia ose kujdestaria).

Në gjuhën angleze:

- given name, family name, personal number, relationship to the minor (father, mother or guardian).

- Në pjesën e pasme të lejes së qëndrimit do të jetë një zonë e bardhë e pa influencuar nga sfondi, guilloshi, rainbow e të tjera teknika të përdorura më sipër, kjo për të mundësuar leximin e qartë të kodit alfanumerik që do të printohet në fazën e personalizimit. Printimi do të kryhet me OCR-B zonë e lexueshme nga makinat, në përputhje me standardin ICAO 9303. Ky kod do të lexohet nga makinat ekzistuese të pasaportave.

- I paraprintuar me Mikrotex do të jetë një tekst me sipërfaqe totale shkrimi 100 mm².

- Leja e qëndrimit do të ketë në faqen e përparme një shtresë mbrojtëse me shenja optikisht të variueshme të tipit OVD (optically variable devices).

Vendosja e të gjitha elementeve të disajnit që përfshijnë:

- elementet grafike,
- elementet e sigurisë,
- emërtimet e rubrikave, përbërësit e gjendjes civile të mbajtësit, të dhënat shpesh të mbajtësit,

¹ UV DULL përshkruan karakteristikën e trupit të lejes së qëndrimit për të mos pasur tipare fluoreshence, për të siguruar në këtë mënyrë printimin e padukshëm UV.

- kompozimi i shtresës mbrojtëse, si dhe pamja përfundimtare.
E gjitha kjo do të realizohet pas lidhjes së kontratës me kompaninë fituese.