**VENDIM**
**Nr. 253, datë 27.4.2007**

# PËR CAKTIMIN E ELEMENTEVE TË SIGURISË DHE PËR MIRATIMIN E FORMËS DHE TË MODELIT TË DOKUMENTIT TË IDENTITETIT TË SHTETASVE SHQIPTARË

*(Ndryshuar me VKM nr. 715, datë 6.11.2007)*

*(i përditësuar)*

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 6 e 8 të ligjit nr. 8952, datë 10.10.2002 "Për dokumentin e identitetit të shtetasve shqiptarë", me propozimin e Ministrit të Brendshëm, Këshilli i Ministrave

VENDOSI:

1. Caktimin e elementeve të sigurisë së dokumentit të identitetit, sipas aneksit 1, që i bashkëlidhet këtij vendimi.

2. Miratimin e formës dhe të modelit të dokumentit të identitetit, sipas aneksit 2, që i bashkëlidhet këtij vendimi.

3. Vendimet e Këshillit të Ministrave nr. 320, datë 21.5.2004 "Për caktimin e elementeve të sigurisë dhe miratimin e formës së dokumentit të identitetit të shtetasve shqiptarë" dhe nr.579, datë 27.8.2004 "Për miratimin e modelit të dokumentit të identitetit të shtetasve shqiptarë", shfuqizohen.

4. Ngarkohet Ministria e Brendshme për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
**Sali Berisha**

ANEKSI 1

*(Ndryshuar paragrafi i gjashtë i pikës 1 me VKM nr. 715, datë 6.11.2007)*

1. Lloji i kartës

Karta e identitetit do të jetë një kartë me një chip elektronik.

2. Elementet e sigurisë të vendosura në trupin e kartës

- GUILLOCHE[1]. Në të dy anët e kartës 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 kartës në përmasa sa 1/3 e përmasave të fotografisë kryesore.

- Shtresë mbrojtëse transparente me shenja optikisht të variueshme[5], e aplikuar në të dy anët e kartës përgjatë gjithë sipërfaqes[6].

---

[1] Vizatimi i dizanjit me vija-vija të holla të vazhduara.

[2] Printimi i dizanjit 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 kartës.

[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.

- *Bojë UV. Një simbol i printuar me bojë të dukshme, me sipërfaqe 100 mm$^2$, 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 kartë, do të realizohet edhe gjatë procesit të personalizimit.

3. Chipi i kartës

Karta e identitetit do të pajiset me një chip të vendosur në brendësi të trupit të kartës dhe do të jenë në përputhje me standardet:

- ISO/ICE 7810 (Karta e identifikimit-karakteristikat fizike);
- ISO 10373 (Karta e identifikimit-metodat e testimit të chip-it me/pa kontakt);
- ISO 7501-3 (Karta e identifikimit-dokumentet e udhëtimit të lexueshme nga makina).
- 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 (Karta 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);
- Chip-i 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 v2.1.1;
- specifikimet e kartës Java minimalisht versionin 2.2.1;

Ruajtja e të dhënave në chip

- Kapaciteti i chip-it do të jetë minimumi 72KB.
- Ruajtja në chip dhe leximi nga chip-i i të dhënave do të realizohen në mënyrë të sigurt 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 kartë do të ruhen në një strukturë hierarkike të bazuar në *file* (skedarë) duke suportuar karakteristikat e mëposhtme:

- sistem skedarësh hierarkikë me shumë nivele sipas standardit ISO 7816-4 me një skedar kryesor (*Master File*-MF) si rrënjë;
- mundësinë për të krijuar skedarë të dedikuar (*Dedicated Files*-DF) dhe skedarë elementarë (*Elementary Files*-EF) aq sa nevojitetn dhe memorja 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), bazur 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 kartë do të ruhet edhe në chip.

- Jetëgjatësia e kartës me chip do të jetë 10 vjet. Chip-i i kartës 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 shfrytëzojë kriptografinë simetrike dhe asimetrike (PKI).

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

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

- Menaxhimii aplikacioneve të kartës-ngarkimi/fshirja e aplikacioneve të kartës;
- Menaxhimi i ciklit të kartës-aktivizimi/kyçja e kartës dhe e aplikimeve të saj;
- Përditësimi i të dhënave të kartës.

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 çelësa 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).v1.1".

Chip-i duhet të suportojë gjenerimin e çelësave RSA.

Chip-i duhet të jetë i aftë të ruajë në të ardhmen dy certifikata X.509, një për firmën dixhitale dhe tjetrin për inkriptimin e të dhënave. Për të dy 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 kartën:

- PIN-i i mbajtësit të kartës; 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;
- do të mbrojë aksesin në operacionet PKI, që konfirmojnë identitetin e mbajtësit të kartës (firmosja dixhitale dhe operacionet e inkriptimit).
- PIN-i administrativ, që do të përdoret për të zhbllokuar kartën, kur kjo e fundit është bllokuar.

4. Të dhënat biometrike

- Fotografia e mbajtësit:
- printohet me ngjyra në anën e përparme të kartës;
- ruhet në chip në përputhje me standardin ISO/IEC 19794-5:2005 (Teknologjia e informcionit-formatet e shkëmbimit të të dhënave biometrike-të dhënat e imazhit të fytyrës), e kompresuar në formatin JPEG.
- Shenjat e dy gishtave ruhen si imazhe dixhitale 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-së për pasaportën elektronike.

ANEKSI 2

*(Ndryshuar paragrafi i dytë i pikës 2, fjalia e parë e pikës 1 dhe pika 2 me VKM nr. 715, datë 6.11.2007)*

1. Forma dhe përmasa

Karta e identitetit do të jetë e formatit ID-1 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 kartës së identitetit do të jetë në përputhje me standardin ICAO 9303 dhe ISO 7810.

*Karta e identitetit do të jetë vetëm polikarbonat, e ndërtuar nga disa shtresa. Teknologjia e bashkimit të shtresave të kartës të sigurojë formimin e një trupi të vetëm dhe të pandashën.*

Karta e kompozuar në këtë mënyrë, me disa shtresa, me antenën RF në brendësi dhe chip-in 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 kartës të jetë "UV Dull[7]".

Dokumenti i identitetit ka dy faqe:

1. Faqja kryesore do të jetë ajo në të cilën do të vendosen:

- *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 dykrenare, e paraprintuar;
- do të jetë e vendosur e paraprintuar shenja e globit në formë rrethore ku do të ketë pjesë të hartës së kontinenteve dhe mbi të do të jetë e vendosur harta e Shqipërisë e paraprintuar me teknikën OVI, me përmasa 19,5mm x 9mm;
- do të jenë emërtimet e përbërësve të gjendjes civile me shkronja të vogla të shtypit.

Në gjuhën shqipe:

emri, mbiemri, atësia, amësia, datëlindja, vendlindja, numri i identitetit, data e mbarimit të afatit.

Në gjuhën angleze:

*given name, family name, father's name, mother's name, gender, date of birth, place of birth, signature, ID number, expiru date.*

- Përbërësit e gjendjes civile do të printohen në fazën e personalizimit me shkronja të mëdha të shtypit.
- Shkrime të tjera të paraprintuara

REPUBLIKA E SHQIPËRISË, KARTË IDENTITETI, IDENTITY CARD, REPUBLIC OF ALBANIA.

- Mikrotext i paraprintuar do të jetë tekst me sipërfaqe totale shkrimi 100 $mm^2$.
- E printuar gjatë fazës së personalizimit me mikrotekst do të jetë mbiemri i mbjatësit të kartës dhe numri i identitetit.

---

[7] UV DULL përshkruan karakteristikën e trupit të kartës për të mospasur tipare floreshente, për të siguruar në këtë mënyrë printimin e padukshëm UV.

2. Në faqen e pasme të kartës:

*Chip-i me kontakt dhe pa kontakt. Përmasat e Chip-it dhe vendosja e tij në kartë do të jenë në përputhje me standardin ISO 7816.*

*- Do të jenë emërtimet e të dhënave të tjera të mbajtësit të dokumentit, me shkronja të vogla të shtypit.*

*Në gjuhën shqipe:*

*Ngjyra e syve, gjatësia, numri serial i dokumentit.*

*Në gjuhën angleze:*

*Eye colour, height, serial number.*

*- Do të jenë të dhënat e tjera (ngjyra e syve, gjatësia dhe numri serial i kartës), me shkronja të mëdha të shtypit.*

*- Në pjesën e pasme të kartës do të jetë një zonë e bardhë e painfluencuar 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.*

*- Do të vendoset simboli sipas sipërfaqes së përcaktuar në aneksin 1.*

*- I paprintuar me mikrotekst do të jetë një tekst, me sipërfaqe totale shkrimi 100 $mm^2$.*

*- Dokumenti i identitetit do të ketë në të dyja faqet edhe një shtresë mbrojtëse, me shenja optikisht të variueshme të tipit OVD (optically variable devices), e cila do të ketë simbole e citime shqiptare.*

*Vendosja e të gjitha elementeve të disajnit, që përfshijnë:*

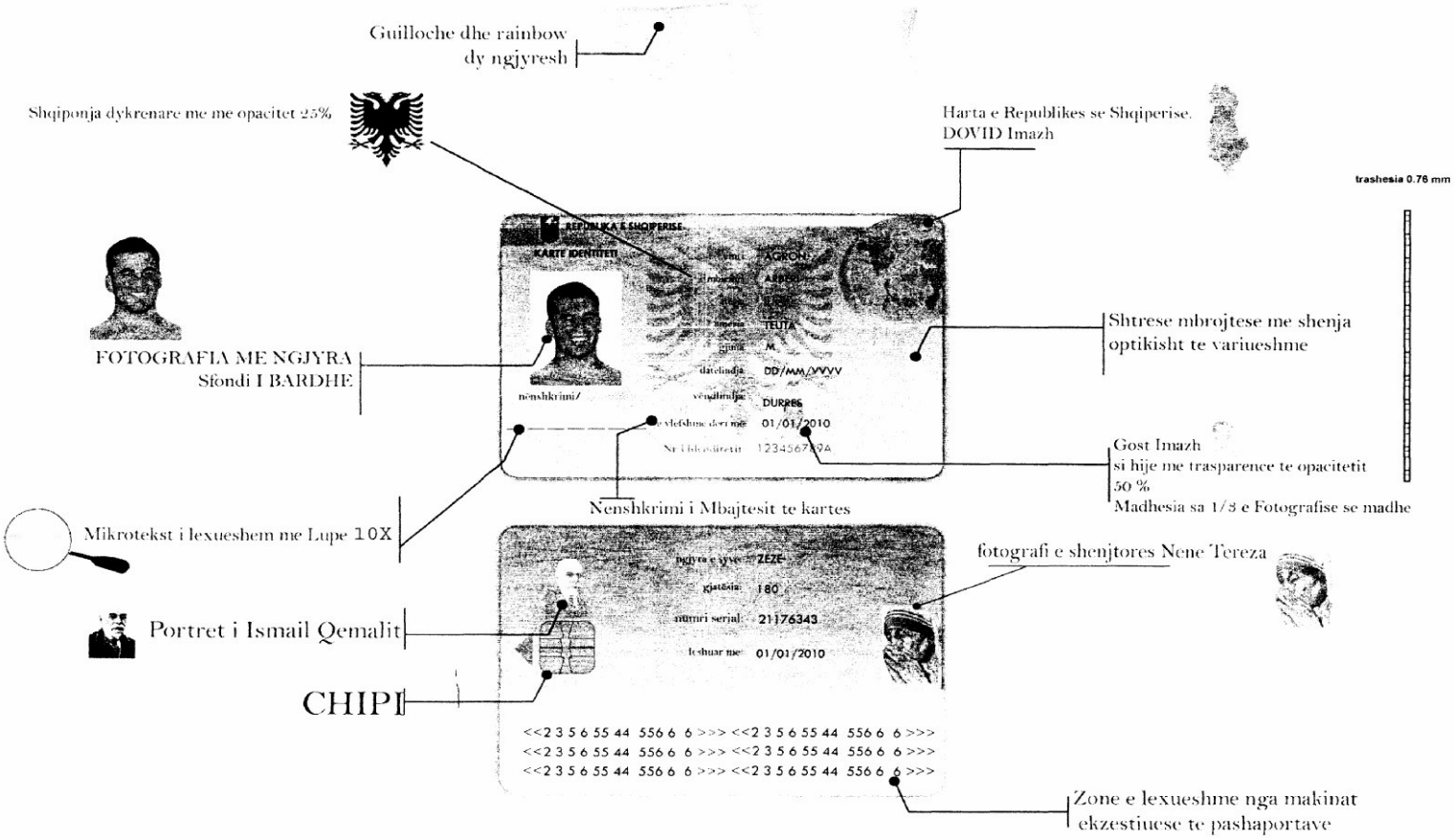
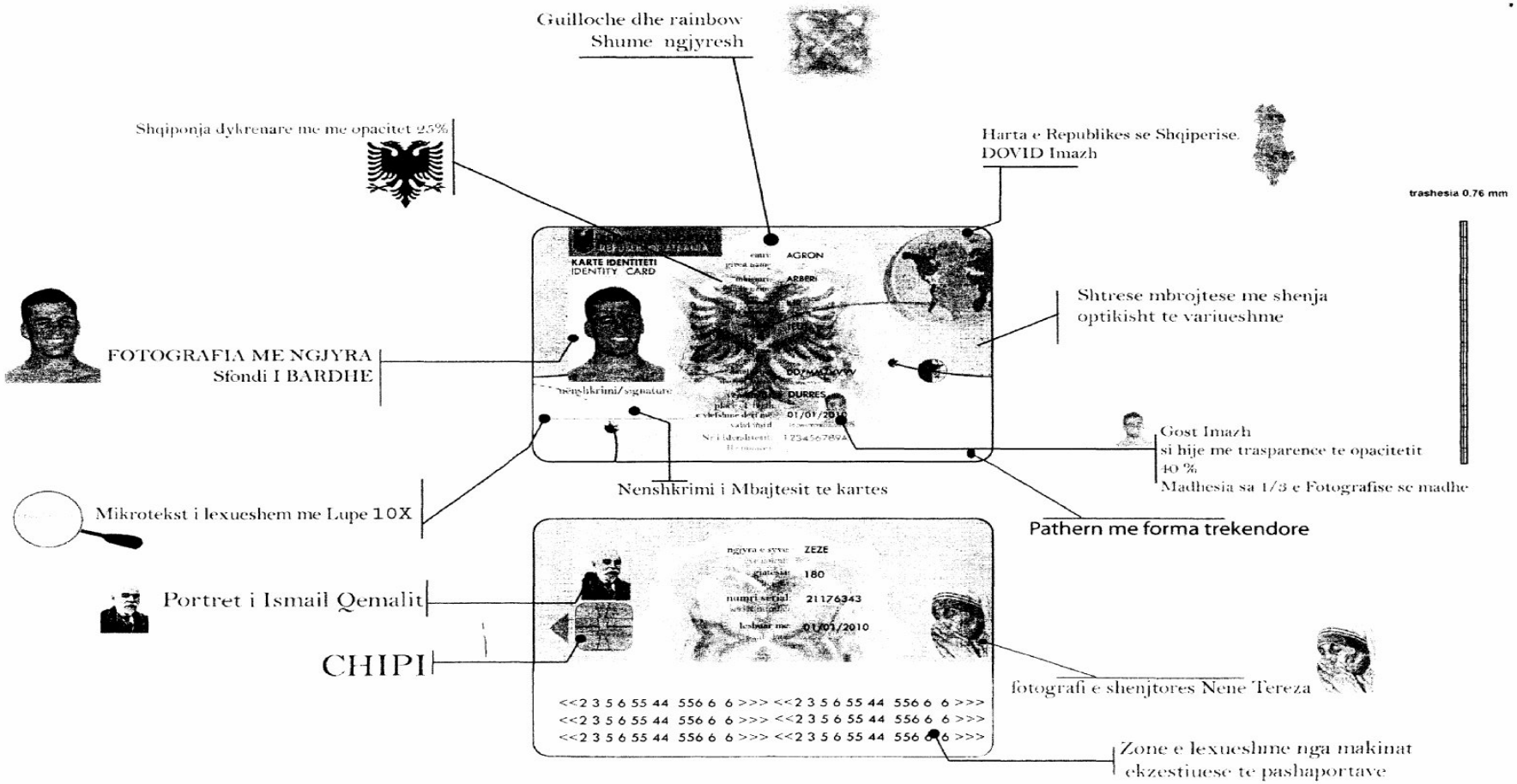
*- elementet grafike;*

*- elementet e sigurisë;*

*- elementet e rubrikave, përbërësit e gjendjes civile të mbajtësit, të dhënat shtesë të mbajtësit;*

*- kompozimi i shtresës mbrojtëse, si dhe pamja përfundimtare do të realizohen pas lidhjes së kontratës me kompaninë fituese.*

# Versioni i I-re Ilustrativ



# Versioni i II-te Ilustrativ