Sertifikaadi, CRL-i ja OCSP profiil Eesti Vabariigi isikut tõendavatel dokumentidel

Versioon 8.2

1. November 2018

Version History		
Date	**Version**	**Changes**
01.11.2018	8.2	Peatükk 2.2.1 - parandatud sertifikaadi laienduste *AuthorityKeyIdentifier* ja *Subject KeyIdentifier* kirjeldust; Peatükk 4 - lisatud uued laiendused: *Archive Cutoff* ja *Extended Revoked Definition*; *CertStatus* kirjeldus uuendatud.
04.11.2017	8.1	Peatükk 1 - täpsustatud Mobiil-ID autentimissertifikaadi kasutusvaldkond Peatükk 3.1 - eemaldatud CRL'ist laiendus "Invalidity Date" Peatükk 2.2.2 - täpsustatud RSA ja ECC võtmete *Key Usage* väärtused
24.10.2017	8.0	Eemaldatud Mobiil-ID e-residentidele kogu profiili ulatuses. Peatükk 2.2.2 - lisatud KeyAgreement *Key Usage* väärtus ja eemaldatud ebavajalikud *KeyUsage* väärtused Peatükk 2.2.2 - eemaldatud *Extended Key Usage* väärtused Mobiil-ID sertifikaadiprofiilist Peatükk 2.1 - lisatud uus toetatud algoritm NIST P-384. Peatükk 5 - muudetud viide RFC5639 õigeks RFC5480 (*NIST Elliptic Curve Cryptography*). Muudetud ettevõtte nimi AS Sertifitseerimiskeskus uueks SK ID Solutions AS. Peatükk 2.2.1 - kasutusele võetud lühiaadressid (c.sk.ee) viidates kesktaseme CA'le. Peatükk 2.2.3 - lisatud puuduolev viide lepingule (Mobiil-ID). Peatükk 3.2 - kasutusele võetud CRL'i asukoha lühiaadressid (c.sk.ee). Peatükk 4 - muudetud *Responder ID* väärtused õigeks; lisatud märge OCSP *nonss* kasutuse kohta.

01.11.2016	7.0	Muudetud dokumendi nimi. Dokumendi struktuur muudetud. Punktis 2 - täiendatud peatükki “Sertifikaadi tehniline profiil”. Punktis 2.2 - täiustatud sertifikaadi laienduste tabelit. Punktis 2.2.3 - lisatud uued sertifikaadi poliitikate OID-id. Punktis 4 - Lisatud OCSP profiili kirjeldus; muudetud CN nimi. Eemaldatud sertifikaadi näited.
01.01.2016	6.0	Punktis 3.2 muudetud sertifikaadiomaniku andmete ASN.1 tüüpe. Punktis 4 uuendatud viidatud ja seonduvate dokumentide viiteid. Lisas A punktis 2.3 täiendatud kasutatavate sertifikaadi signeerimisalgoritmide nimekirja. Lisas A punktis A.2.5 täiendatud sertifikaadis sisalduva avaliku võtme pikkusi. Lisas A punktis A.3 uuendatud sertifikaadi laiendused. Lisas A punktis A.3.4 täiendatud sertifitseerimispõhimõtted. Lisas A punktis A.3.7 täiendatud STO lisanime kirjeldust. Lisas A punktis A.3.10 muudetud kvalifitseeritud sertifikaadi tunnuse kasutust. Lisas A punktides A.5.1 ja A.5.2 parandatud näitesertifikaatide kirjeldusi.
01.01.2015	5.0	Punktis 4.1 uuendatud viited Eesti Vabariigi seadustele. Lisas A punktis A.2.3 eemaldatud SHA-1 kasutatavate sertifikaatide signeerimisalgoritmide nimekirjast.

01.12.2014	4.0	Muudetud dokumendi nimi. Parandatud dokumendi sõnastust ja vormindust. Dokument viidud vastavusse dokumendiga RFC5280. Punktis 1 täpsustatud käesoleva dokumendi sisu. Punktis 1.2.1 lisatud uued mõisted Residendi digi-ID, E-residendi digi-ID, E-residendi mobiil-ID, Dokument; ära kaotatud mõisted Isikutunnistus ja Isikutunnituse kehtivusperiood. Punktis 3.1 parandatud sertifikaadis sisalduvaid väljaandja andmeid. Punktis 3.2 parandatud sertifikaadis sisalduvaid sertifikaadiomaniku andmeid. Lisas A punktis A.2.3 täiendatud kasutatavate sertifikaadi signeerimisalgoritmide nimekirja. Lisas A punktis A.2.4 muudetud sertifikaatide kehtivusperioodi kirjeldust. Lisas A punktis A.2.5 täiendatud sertifikaadis sisalduvate avalike võtmete ja nende esitusalgoritmide nimekirja. Lisas A punktides A.5.1 ja A.5.2 parandatud näitesertifikaatide kirjeldusi.
01.06.2014	3.5	Kõik versiooni 3.4 planeeritud muudatused viiakse sisse versiooni 3.5, välja arvatud Mobiil-ID sertifikaatide kehtivusaja piiramine.

01.05.2014	3.4	Lisatud versiooni info tabel. Viidatud ja seonduvad dokumendid viidud eraldi punkti 4 alla. Parandatud dokumendi sõnastust ja vormindust. Punktis 1 täpsustatud käesoleva dokumendi sisu. Punktis 1.2.1 lisatud uued mõisted EL-kaart, Digi-ID, Mobiil-ID, parandatud mõisted ID-kaart ja Isikutunnistus. Lisas A punktis A.2.4 lahti kirjutatud erinevate dokumentide sertifikaatide kehtivusperioodid. Lisas A punktis A.3.6 täiendatud isiku e-posti aadressi loomise reegleid punkti kasutamise osas (muudatus kehtib alates 28.02.2013). Lisas A punktis A.3.10 täiendatud kvalifitseeritud sertifikaadi tunnuse laiendusi (muudatus kehtib alates 28.02.2013). Lisas A punktides A.5.1 ja A.5.2 täiendatud näitesertifikaatides kvalifitseeritud sertifikaadi tunnuseid (muudatus kehtib alates 28.02.2013). See versioon ei hakanud kunagi kehtima, kuna selle eelduseks olnud määrust mobiil-ID vormis digitaalse isikutunnistuse väljaandmise üksikasjade kohta, millega oli plaanis muuta perioodil 01.05.2014 kuni 31.12.2014 väljaantavate Mobiil-ID sertifikaatide kehtivusaega, Vabariigi Valitsus vastu ei võtnud.
01.01.2010	3.3	Versioon avalikustamiseks.

1. Sissejuhatus

Käesolev dokument kirjeldab Eesti Vabariigi isikut tõendavatele dokumentidele kantavate digitaalsete sertifikaatide profiile. Lisaks kirjeldab dokument ka CRL-i ja OCSP profiile.

Sertifikaadid on väljastatud kesktaseme sertifitseerija ESTEID [16] poolt. Käesolev dokument täiendab sertifitseerimispoliitikaid [2][3][4] ja sertifitseerimispõhimõtteid [1].

Punktis 2 kirjeldatakse sertifikaadi tehnilist profiili.

Antud dokument ei käsitle teisi isikut tõendavates dokumentides sisalduvaid andmekogumeid.

Dokumentidele kantavaid digitaalseid sertifikaate on kahte tüüpi:

1. Kvalifitseeritud elektroonilise allkirja sertifikaat, mida kasutatakse:
   - loomaks kvalifitseeritud digitaalset allkirja, mis on vastavuses eIDAS-ega [13].
2. Autentimissertifikaat, mida kasutatakse:
   - sertifikaat isiku digitaalseks tuvastamiseks,
   - krüpteerimiseks*,
   - e-posti signeerimiseks.

**Ei laiene Mobiil-ID sertifikaadile*

Sertifikaate väljastab sertifitseerimisteenuste osutaja SK ID Solutions AS.

[16] - Kesktaseme sertifitseerija võib olla ESTEID-SK 2011 ja ESTEID-SK 2015.

1.1. Definitsioonid ja lühendid

Juhindu peatükist 1.6 dokumentides Sertifitseerimispõhimõtted [1] ja Sertifitseerimispoliitika [2], [3], [4].

2. Sertifikaadi tehniline profiil

Füüsilise isiku sertifikaadid on vastavuses järgmiste standarditega: X.509 version 3, IETF RFC 5280 [6], ETSI EN 319 412-2 [8] ja ETSI EN 411-2 (peatükk 6.6) [15].

2.1. Sertifikaadi keha

Välja nimi	OID	Kohustuslikkus	Väärtus	Muudetav	Kirjeldus
Version		jah	V3	ei	Sertifikaadi formaadi versioon
Serial Number		jah		ei	Unikaalne sertifikaadi seerianumber
Signature Algorithm	1.2.840.113549.1.1.11	jah	sha256WithRSAEncryption	ei	Signatuuri algoritm vastavalt standardile RFC 5280 [6]
Issuer Distinguished name					Sertifikaadi väljaandja andmed
Common Name (CN)	2.5.4.3	jah	ESTEID-SK 2015		Sertifitseerimisteenuse sertifitseerija eraldusnimi
Organisation Identifier	2.5.4.97	jah	NTREE-10747013	ei	Sertifikaadi väljastaja identifitseerimistunnus, mis erineb organisatsiooni nimest. Vastavalt peatükile 5.1.4 standardist ETSI EN 319 412-1 [7].
Organisation (O)	2.5.4.10	jah	AS Sertifitseerimiskeskus		Sertifitseerimisteenuse osutaja nimi.
Country (C)	2.5.4.6	jah	EE		Maatähis: EE - Estonia (2 kohaline ISO 3166 riigi kood [5])
Valid from		jah			Sertifikaadi kehtivuse algusaeg
Valid to		jah			Sertifikaadi kehtivuse lõppaeg

Subject Distinguished Name		jah		jah	Sertifikaadi omaniku andmed
Serial Number (S)	2.5.4.5	jah		jah	Sertifikaadi omaniku isikukood
Given Name (G)	2.5.4.42	jah		jah	Eesnimed UTF8 formaadis vastavalt standardile RFC5280. Lisaks vastavuses ka isikut tõendavate dokumentide seadusele [12], rahvusvahelised tähed šifreeritakse vastavalt vajadusel IC AO reeglitele.
SurName (SN)	2.5.4.4	jah		jah	Perekonnanimed UTF8 formaadis vastavalt standardile RFC5280. Lisaks vastavuses ka isikut tõendavate dokumentide seadusele [12], rahvusvahelised tähed šifreeritakse vastavalt vajadusel ICAO reeglitele.
Common Name (CN)	2.5.4.3	jah		jah	Perekonna- ja eesnimed, isikukood (eraldatud komaga)
Organisational Unit (OU)	2.5.4.11	jah		jah	Sertifikaadi kasutusvaldkond. Kasutatakse väärtusi vastavalt sertifikaadi tüübile: "authentication" või "digital signature"
Organisation Name (O)	2.5.4.10	jah		jah	Sertifikaadi tüüp [17]
Country (C)	2.5.4.6	jah		jah	Päritoluriik, vastavalt standardile ISO 3166 [5].
Subject Public Key		jah	RSA 2048, NIST P-256, NIST P-384	jah	RSA algoritm vastavalt standardile RFC 4055 [10] ja ECC algoritm vastavalt standardile RFC 5480 [11].

[17]

ID-kaart ja EL-kaart O = ESTEID

Digi-ID: O = ESTEID (DIGI-ID)

Mobiil-ID: O = ESTEID (MOBIIL-ID)

E-residendi digi-ID: O = ESTEID (DIGI-ID E-RESIDENT)

2.2. Sertifikaadi laiendused

2.2.1. Laiendused

Allolev tabel kirjeldab sertifikaadi sees kasutatavaid laiendusi:

Laiendus	OID	Väärtused ja kitsendused	Kriitilisus	Kohustuslik
Basic Constraints	2.5.29.19	Subject Type=End Entity Path Length Constraint=None	Mittekriitiline	jah
Certificate Policies	2.5.29.32	Vaata p 2.2.3 "Sertifitseerimis poliitikad"	Mittekriitiline	jah
Subject Alternative Name	2.5.29.17	Vaata p 2.2.2 "Laienduste erisused"	Mittekriitiline	jah
Key Usage	2.5.29.15	Vaata p 2.2.2 "Laienduste erisused"	Kriitiline	jah
Extended Key Usage	2.5.29.37	Vaata p 2.2.2 "Laienduste erisused"	Kriitiline	jah
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	Vaata p 2.2.2 "Laienduste erisused"	Mittekriitiline	jah
AuthorityKeyIdentifier	2.5.29.35	SHA-1 räsi avalikust võtmest	Mittekriitiline	jah
CRL distribution Points	2.5.29.31	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://c.sk.ee/esteid2015.crl	Mittekriitiline	jah
SubjectKeyIdentifier	2.5.29.14	SHA-1 räsi avalikust võtmest	Mittekriitiline	jah
Authority Information Access	1.3.6.1.5. 5.7.1.1		Mittekriitiline	jah
ocsp	1.3.6.1.5. 5.7.48.1	http://aia.sk.ee/esteid2015		jah
calssuers	1.3.6.1.5. 5.7.48.2	http://c.sk.ee/ESTEID-SK_2015.der.crt		jah

2.2.2. Laienduste erisused

Järgnevad erisused laiendites kehtivad dokumendi tüüpidele: ID-kaart, EL-kaart, Digi-ID (kaasa arvatud E-resident) ja Mobiil-ID.

Laiendus	AUTENTIMISSERTIFIKAAT	ALLKIRJASTAMISE SERTIFIKAAT
Subject Alternative Name	Vaata p. 6.1 "Lisa A"	
ECC võtmed: Key Usage	DigitalSignature, KeyAgreement	nonRepudiation
RSA võtmed: Key Usage	DigitalSignature, KeyEncipherment, dataEncipherment	nonRepudiation
Extended Key Usage (*Kehtib ainult: ID-kaart, EL-kaart, Digi-ID*)	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	-

Qualified Certificate Statement [18]		
id-etsi-qcs-QcCompliance		jah
id-etsi-qcs-QcSSCD		jah
id-etsi-qcs-QcType [19]		1
id-etsi-qcs-QcPDS	https://sk.ee/en/repository/conditions-for-use-of-certificates/	https://sk.ee/en/repository/conditions-for-use-of-certificates/

[18] - qcStatements vastavalt peatükile 6.6.1 standardis ETSI EN 319 411-2 [15]

[19] - Tüübid vastavalt peatükile 4.2.3 standardis ETSI EN 319 412-5 [14]

2.2.3. Sertifitseerimispoliitikad

Profiil	Identifikaator (autentimissertifikaat)	Identifikaator (allkirjastamise sertifikaat)	Identifikaator väärtus	*Identifikaatori märgend [20]*
ID-kaart; EL-kaart	1.3.6.1.4.1.10015.1.1 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.1 0.4.0.194112.1.2	https://www.sk.ee/repositorium/CPS	
Digi-ID ; E-residendi digi-ID	1.3.6.1.4.1.10015.1.2 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.2 0.4.0.194112.1.2	https://www.sk.ee/repositorium/CPS	
Mobiil-ID	1.3.6.1.4.1.10015.1.3 0.4.0.2042.1.2	1.3.6.1.4.1.10015.1.3 0.4.0.194112.1.2	https://www.sk.ee/repositorium/CPS	Contract 1.11-9

20 - *Väljal esitatakse viide lepingule, mille alusel sertifikaat on välja antud.*

3. Tühistusnimekirja profiil

SK väljastab sertifikaatide tühistusnimekirja (*CRL*) vastavalt standardile RFC 5280 [6].

3.1. Tühistusnimekirja põhiväljad

Välja nimi	OID	Kohustuslikkus	Väärtus	Kirjeldus
Version		jah	Version 2	Tühistusnimekirja formaadi versioon, vastavalt standardile X.509
Signature Algorithm		jah	sha256WithRSA Encryption	Tühistusnimekirja signeerimisalgoritm, vastavalt standardile X.509
Issuer Distinguished Name		jah		Tühistusnimekirja väljaandja andmed

Common Name (CN)	2.5.4.3	jah	ESTEID-SK 2015 või ESTEID-SK 2011	Sertifitseerimisteenuse osutaja alam CA nimi
Organisation Identifier	2.5.4.97	jah	NTREE-10747013	Sertifikaadi väljastaja identifitseerimistunnus, mis erineb organisatsiooni nimest. (Ei laiene alam CA ESTEID-SK 2011 sertifikaatidele). Vastavalt peatükile 5.1.4 standardist ETSI EN 319 412-1 [7].
Organisation (O)	2.5.4.10	jah	SK ID Solutions AS	Organisatsiooni nimi
Country (C)	2.5.4.6	jah	EE	Maatähis: EE - Estonia (2 kohaline ISO 3166 riigi kood [5])
Last Update		jah		CRL-i genereerimise aeg (kuupäev ja kellaaeg)
Next Update		jah		Järgmise CRL-i väljastamise aeg (kuupäev ja kellaaeg). Tingimused on kirjeldatud ESTEID sertifitseerimispõhimõtete peatükis 4.9.7.
Revoked Certificates				Tühistatud sertifikaatide nimekiri
Serial Number		jah		Tühistatud sertifikaadi unikaalne seerianumber
CRL Reason Code	2.5.29.21	jah		Tühistatud sertifikaadi tühistamiskood (põhjus)
Revocation Date		jah		Kuupäev mil sertifikaat tühistati või tunnistati mõnel teisel põhjusel kehtetuks.

3.2. Tühistusnimekirja *(CRL)* laiendused

Välja nimi	OID	Väärtused ja kitsendused	Kriitilisus
CRL Number	2.5.29.20	Tühistusnimekirja järjekorra number	ei
Authority Key Identifier	2.5.29.35	SHA-1 räsi avalikust võtmest, mida kasutatakse sertifikaadi signeerimiseks	ei
Issuing Distribution Point	2.5.29.28	Tühistusnimekirja asukoht http://c.sk.ee/esteid2015.crl või http://c.sk.ee/esteid2011.crl	jah

4. Kehtivuskinnitusteenuse *(OCSP)* profiil

OCSP v1 vastavalt standardile [RFC 6960] [9]

Välja nimi	Kohustuslikkus	Väärtus	Kirjeldus
ResponseStatus	jah	0 for successful or error code	Päringu vastuse väärtus
ResponseBytes			
ResponseType	jah	id-pkix-ocsp-basic	Vastuse tüüp
Response Data	jah		
Version	jah	1	Vastuse versiooni formaat
Responder ID	jah	CN = ESTEID-SK 2015 AIA OCSP RESPONDER YYYYMM OU = OCSP 2.5.4.97 = NTREE-10747013 O = SK ID Solutions AS C = EE	OCSP teenuse väljaandja andmed. Märkus: eraldusnimi (CN) on muutuv kuude lõikes, kasutatakse ajaformaati YYYYMM (AAAAKK) vormingut.
Produced At	jah		OCSP vastuse signeerimisaeg
Responses	jah		
CertID	jah		Sertifikaadi seerianumber
Cert Status	jah		Sertifikaadi staatuse väärtused:
Revocation Time	ei		Sertifikaadi tühistamis- või aegumiskuupäev *good* - sertifikaat on väljastatud ja pole tühistatud ega peatatud *revoked* - sertifikaat on tühistatud, peatatud või ei ole väljastatud kõnealuse CA poolt *unknown* - sertifikaadi väljastaja on tundmatu OCSP teenusele
Revocation Reason	ei		Tühistamiskood vastavalt standardile RFC5280 [6].
This Update	jah		Staatuse küsimise aeg andmebaasist
Archive Cutoff	ei	CA sertifikaadi "valid from" kuupäev.	ArchiveCutOff date - CA sertifikaadi "valid from" kuupäev. Vastavalt standardi RFC 6960 [9] p unktile 4.4.4.
Extended Revoked Definition	ei	NULL	Identifitseerib, et semantika sertifikaadi staatuse kohta OCSP vastuses, vastab laiendatud määratlusele mis on kirjeldatud standardis RFC 6 960 punktis 2.2 [9]
Signature Algorithm	jah	sha256WithRSAEncryption	Signeerimisalgoritm vastavalt RFC 5280 [6] standardile
signature	jah		
Certificate	jah		Sertifikaat vastavalt selle privaatvõtmele, kasutamaks seda vastuse signeerimiseks

*OCSP ei toeta nonss (*nonce)* laiendust.

5. Viidatud ja seonduvad dokumendid

1 SK ID Solutions AS - ESTEID-SK Sertifitseerimispõhimõtted: https://sk.ee/en/repository/CPS/;
2 ID-kaardi sertifitseerimispoliitika: https://sk.ee/en/repository/CP/;

3. Digi-ID sertifitseerimispoliitika: https://sk.ee/en/repository/CP/;
4. Mobiil-ID sertifitseerimispoliitika: https://sk.ee/en/repository/CP/;
5. ISO 3166 Codes: http://www.iso.org/iso/country_codes;
6. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
7. ETSI EN 319 412-1 v1.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1: Overview and common data structures;
8. ETSI EN 319 412-2 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
9. RFC 6960 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
10. RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
11. RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information;
12. Isikut tõendavate dokumentide seadus, RT I 1999, 25, 365, https://www.riigiteataja.ee/akt/123032015016?leiaKehtiv;
13. eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
14. ETSI EN 319 412-5 v2.1.1 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 5: QCStatements;
15. ETSI EN 319 411-2 v2.6.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

6. Lisa A - Sertifikaadikohane tehniline lisainformatsioon

6.1. Isiku e-posti aadress (Subject Alternative Name)

Väljal esitatakse sertifikaadi omaniku e-posti aadress. E-posti aadress sisaldub vaid isiku digitaalseks tuvastamiseks kasutatavas sertifikaadis.

E-posti aadress luuakse isiku ees- ja perekonnanime(de)st (eesnimed.perekonnanimed@eesti.ee) vastavalt sertifikaadis G ja SN väljadel olevatele väärtustele, teostades eelnevalt vajalikud teisendused vastavalt käesolevale punktile. Korduvate nimede puhul, kui samade nimedega e-posti aadress on juba väljastatud, lisatakse nimedele järjestikuline kümnendarv järgmises vormis:

eesnimed.perekonnanimed.N@eesti.ee.

Alamdomeeniks on eesti.ee.

Aadressis on iga nime eraldavaks ühikuks punkt. Juhul, kui nimes on sidekriips, kasutatakse sidekriipsu. Muud märgid peale sidekriipsu asendatakse punktiga.

Kui märkide asendamisel punktidega tekib e-posti aadress kujul, kus on järjest mitu punkti, siis asendatakse korduvad punktid ühekordse punktiga (nt. isik nimega ANTS E. PALUSAAR saab enda e-posti aadressiks ants.e.palusaar@eesti.ee). Juhul kui teisenduse tulemusena tekib e-posti aadressi algusesse või vahetult enne @ märki punkt, siis need punktid kaotatakse (nt. kui isiku nimi on MARK GIREE' siis tema e-posti aadressiks saab mark.giree@eesti.ee).

Tähe koodid on esitatud kuueteistkümnendsüsteemis allolevas tabelis UTF-32 kodeeringus, mis on kirjeldatud rahvusvahelises standardis ISO/IEC 10646 (Unicode).

Nimedes tehakse järgmiste tähemärkide puhul asendused:

Jrk	Täht	Tähe kood	Asendustäht	Asenduskood
1	A	0041		
2	a	0061		
3	B	0042		
4	b	0062		
5	C	0043		
6	c	0063		
7	D	0044		
8	d	0064		
9	E	0045		
10	e	0065		
11	F	0046		
12	f	0066		
13	G	0047		

14	g	0067		
15	H	0048		
16	h	0068		
17	I	0049		
18	i	0069		
19	J	004A		
20	j	006A		
21	K	004B		
22	k	006B		
23	L	004C		
24	l	006C		
25	M	004D		
26	m	006D		
27	N	004E		
28	n	006E		
29	O	004F		
30	o	006F		
31	P	0050		
32	p	0070		
33	Q	0051		
34	q	0071		
35	R	0052		
36	r	0072		
37	S	0053		
38	s	0073		
39	Š	0160	S	0053
40	š	0161	s	0073
41	Z	005A		
42	z	007A		
43	Ž	017D	Z	005A
44	ž	017E	z	007A
45	T	0054		
46	t	0074		
47	U	0055		
48	u	0075		
49	V	0056		
50	v	0076		
51	W	0057		
52	w	0077		
53	Õ	00D5	O	004F
54	õ	00F5	o	006F
55	Ä	00C4	A	0041
56	ä	00E4	a	0061
57	Ö	00D6	O	004F
58	ö	00F6	o	006F
59	Ü	00DC	U	0055

60	ü	00FC	u	0075
61	X	0058		
62	x	0078		
63	Y	0059		
64	y	0079		
65	À	00C0	A	0041
66	à	00E0	a	0061
67	Á	00C1	A	0041
68	á	00E1	a	0061
69	Â	00C2	A	0041
70	â	00E2	a	0061
71	Ã	00C3	A	0041
72	ã	00E3	a	0061
73		0100	A	0041
74		0101	a	0061
75		0102	A	0041
76		0103	a	0061
77	Å	00C5	A	0041
78	å	00E5	a	0061
79		0104	A	0041
80		0105	a	0061
81	Æ	00C6	A	0041
82	æ	00E6	a	0061
83		0106	C	0043
84		0107	c	0063
85		010C	C	0043
86		010D	c	0063
87	Ç	00C7	C	0043
88	ç	00E7	c	0063
89		010E	D	0044
90		010F	d	0064
91		0110	DJ	0044; 004A
92		0111	dj	0064; 006A
93	Ð	00D0	DH	0044; 0048
94	ð	00F0	dh	0064; 0068
95	È	00C8	E	0045
96	è	00E8	e	0065
97	É	00C9	E	0045
98	é	00E9	e	0065
99	Ê	00CA	E	0045
100	ê	00EA	e	0065
101		0112	E	0045
102		0113	e	0065
103		0116	E	0045
104		0117	e	0065
105	Ë	00CB	E	0045

106	ë	00EB	e	0065
107		011A	E	0045
108		011B	e	0065
109		0118	E	0045
110		0119	e	0065
111		011E	G	0047
112		011F	g	0067
113		0122	G	0047
114		0123	g	0067
115	Ì	00CC	I	0049
116	ì	00EC	i	0069
117	Í	00CD	I	0049
118	í	00ED	i	0069
119	Î	00CE	I	0049
120	î	00EE	i	0069
121		012A	I	0049
122		012B	I	0069
123		0130	I	0049
124		0131	i	0069
125	Ï	00CF	I	0049
126	ï	00EF	i	0069
127		012E	I	0049
128		012F	i	0069
129		0136	K	004B
130		0137	k	006B
131		0139	L	004C
132		013A	l	006C
133		013D	L	004C
134		013E	l	006C
135		013B	L	004C
136		013C	l	006C
137		0141	L	004C
138		0142	l	006C
139		0143	N	004E
140		0144	n	006E
141	Ñ	00D1	N	004E
142	ñ	00F1	n	006E
143		0147	N	004E
144		0148	n	006E
145		0145	N	004E
146		0146	n	006E
147	Ò	00D2	O	004F
148	ò	00F2	o	006F
149	Ó	00D3	O	004F
150	ó	00F3	o	006F
151	Ô	00D4	O	004F

152	ô	00F4	O	006F
153		014C	O	004F
154		014D	o	006F
155		0150	O	004F
156		0151	o	006F
157	Ø	00D8	O	004F
158	ø	00F8	o	006F
159	OE	0152	OE	004F; 0045
160	oe	0153	oe	006F; 0065
161		0154	R	0052
162		0155	r	0072
163		0158	R	0052
164		0159	r	0072
165		0156	R	0052
166		0157	r	0072
167		015A	S	0053
168		015B	s	0073
169		015E	S	0053
170		015F	s	0073
171	ß	00DF	ss	0073; 0073
172		0164	T	0054
173		0165	t	0074
174		0162	T	0054
175		0163	t	0074
176	Þ	00DE	TH	0054; 0048
177	þ	00FE	Th	0074; 0068
178	Ù	00D9	U	0055
179	ù	00F9	u	0075
180	Ú	00DA	U	0055
181	ú	00FA	u	0075
182	Û	00DB	U	0055
183	û	00FB	u	0075
184		016A	U	0055
185		016B	u	0075
186		016E	U	0055
187		016F	u	0075
188		0170	U	0055
189		0171	u	0075
190		0172	U	0055
191		0173	u	0075
192	Ý	00DD	Y	0059
193	ý	00FD	y	0079
194	Ÿ	0178	Y	0059
195	ÿ	00FF	y	0079
196		0179	Z	005A
197		017A	z	007A

198		017B	Z	005A
199		017C	z	007A