



საქართველოს იუსტიციის სამინისტრო სახელმწიფო სერვისების განვითარების სააგენტო



KA011883710287024

ბ რ ძ ა ნ ე ბ ა

05 / სექტემბერი / 2024 წ.

№ 676/ს

„სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების განვითარების შინაგანაწესის დამტკიცების შესახებ“ საჯარო სამართლის იურიდიული პირის - სახელმწიფო სერვისების განვითარების სააგენტოს თავმჯდომარის 2021 წლის 24 მარტის N140/ს ბრძანებაში ცვლილების შეტანის თაობაზე

საქართველოს ზოგადი ადმინისტრაციული კოდექსის 63-ე მუხლის და „საჯარო სამართლის იურიდიული პირის – სახელმწიფო სერვისების განვითარების სააგენტოს დებულების დამტკიცების შესახებ“ საქართველოს იუსტიციის მინისტრის 2019 წლის 28 ნოემბრის N462 ბრძანებით დამტკიცებული დებულების მე-6 მუხლის მე-2 პუნქტის „დ“ და „ნ“ ქვეპუნქტების შესაბამისად,

ვ ბ რ ძ ა ნ ე ბ ა:

მუხლი 1. „სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების განვითარების შინაგანაწესის დამტკიცების შესახებ“ საჯარო სამართლის იურიდიული პირის - სახელმწიფო სერვისების განვითარების სააგენტოს თავმჯდომარის 2021 წლის 24 მარტის N140/ს ბრძანებით დამტკიცებულ შინაგანაწესში შეტანილ იქნეს შემდეგი ცვლილებები:

1. პირველი მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. დოკუმენტის დამოუკიდებელი იდენტიფიკატორია 1.3.6.1.4.1.37733.10.1.2.4.5.“.

2. მე-8 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„დ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „Biometric Encryption CA G(n)“, რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA ან GEO (*) Root CA G(n)“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის VI და VII თავებით დადგენილი წესის შესაბამისად;“.

3. 99-ე მუხლის პირველი პუნქტის „დ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„დ) „Biometric Encryption CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service Development Agency, CN=Biometric Encryption CA G(n);“.

4. შინაგანაწესის N2 დანართის (სერტიფიკატის ტექნიკური პროფილები):

ა) მე-3 პუნქტი (Biometric Encryption CA G(n)) ჩამოყალიბდეს შემდეგი რედაქციით:

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)		+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)		+	53E43DC35143 EE526A2FCE2B 6CDA0940D80F BFF5	-	გაცემული სერტიფიკატის სერიული ნომერი
ხელმოწერის ალგორითმი (Signature Algorithm)		+	sha256RSA	-	ხელმოწერის ალგორითმი, რომელიც შეესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO Root CA	-	სერტიფიკატის გამცემი ძირითადი ორგანოს (Root) დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Civil Registry Agency	-	სანდო მომსახურების მიმწოდებლის დასახელება
ორგანიზაცია (Organisation) (O)		+	Ministry of Justice of Georgia	-	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	-	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო ISO 3166-ის შესაბამისად)
ძალაშია (-დან) (Valid from)		+	2021 წლის 09 04, 17:36:30	-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)		+	2031 წლის 07 04, 17:36:30	-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)		+		+	სერტიფიკატების ინფრასტრუქტურაში სუბიექტის უნიკალური სახელი
დასახელება (Common Name) (CN)		+	Biometric Encryption CA	+	შუალედური CA-ის დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Development Agency	+	სანდო მომსახურების მიმწოდებლის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+	Ministry of Justice of Georgia	+	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA 4096	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, 4096 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფიკატორი (OID)	მნიშვნელობა და შეზღუდვები (Values and Limitations)	კრიტიკულობა (Criticality)	სავალდებულო (Mandatory)
ძირითადი შეზღუდვები (Basic Constraints)			+	+
სუბიექტის ტიპი (Subject Type)		CA		
გზის სიგრძის შეზღუდვა (Path Length Constraint)		None		
გასაღების გამოყენება (Key Usage)		Certificate Signing, CRL Signing	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier=1.3.6.1.4.1.37733.10.6.1.1.0 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://id.ge/pki	-	+
CRL-ის გავრცელების წერტილები (CRL Distribution Points)		Full Name: URL=http://crl.cra.ge/georootca.crl	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)		KeyID=93 00 66 db 95 51 d3 87 90 78 07 92 22 ed 30 6f 60 e5 88 bf	-	+
სუბიექტის გასაღების იდენტიფიკატორი (Subject Key Identifier)		e9 81 48 b7 32 6c 66 3b bc fc 0b 09 90 92 0c ad 81 30 9e 64	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს ინფორმაციის ხელმისაწვდომობა (Authority Information Access)			-	+
OCSP		URL= http://ocsp.cra.ge/ocsp	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს სერტიფიკატის URL (CA Issuer Certificate URL)		CA Issuers: URI: https://id.ge/pki/GEORootCA.crt		

ბ) 9¹ (GEO (*) Root CA G(n)) პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„9¹. GEO (*) Root CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)		+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)		+		-	გაცემული სერტიფიკატის სერიული ნომერი
ხელმოწერის ალგორითმი (Signature Algorithm)		+	sha256RSA	-	ხელმოწერის ალგორითმი, რომელიც შეესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ძირითადი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO (*) Root CA G(n)	-	სერტიფიკატის გამცემი ძირითადი ორგანოს (Root) დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Development Agency	-	სანდო მომსახურების მიმწოდებლის დასახელება
ორგანიზაცია (Organisation) (O)		+	Ministry of Justice of Georgia	-	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	-	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო ISO 3166-ის შესაბამისად)
ძალაშია (-დან) (Valid from)		+		-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)		+		-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)		+		+	სერტიფიკატების იხფრასტრუქტურაში უნიკალური დასახელება სუბიექტის
დასახელება (Common Name) (CN)		+	GEO (*) Root CA G(n)	+	სერტიფიკატის გამცემი ძირითადი ორგანოს (Root) დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		-	Public Service Development Agency	+	სანდო მომსახურების მიმწოდებლის დასახელება
სუბიექტის		+		+	სტრუქტურის დასახელება

დასახელება (Organisation Name) (O)			Ministry of Justice of Georgia		
ქვეყანა (Country) (C)		+	GE	+	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო ISO 3166-ის შესაბამისად)
სუბიექტის ლია გასალები (Subject Public Key)		+	RSA 4096	-	ლია გასალები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, 4096 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფიკატორი (OID)	მნიშვნელობა და შეზღუდვები (Values and Limitations)	კრიტიკულობა (Criticality)	სავალდებულო (Mandatory)
ძირითადი შეზღუდვები (Basic Constraints)			+	+
სუბიექტის ტიპი (Subject Type)		CA		
გზის სიგრძის შეზღუდვა (Path Length Constraint)		None		
გასალების გამოყენება (Key Usage)		Certificate Signing, CRL Signing	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier= 1.3.6.1.4.1.37733.10.1.2.4.5 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://id.ge/pki	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასალების იდენტიფიკატორი (Authority Key Identifier)		KeyID=	-	+
სუბიექტის გასალების იდენტიფიკატორი (Subject Key Identifier)			-	+

გ) N11¹ (SDA TimeStamping CA G(n)) და N12¹ პუნქტები (SDA Qualified TSU) ჩამოყალიბდეს შემდეგი რედაქციით:

„ 11¹. SDA TimeStamping CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)		+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)		+		-	გაცემული სერტიფიკატის სერიული ნომერი
ხელმოწერის ალგორითმი (Signature Algorithm)		+	sha256RSA	-	ხელმოწერის ალგორითმი, რომელიც შეესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ძირითადი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO (*) Root CA (n)	-	სერტიფიკატის გამცემი ძირითადი ორგანოს (Root) დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Development Agency	-	სანდო მომსახურების მიწოდებლის დასახელება
ორგანიზაცია (Organisation) (O)		+	Ministry of Justice of Georgia	-	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	-	სანდო მომსახურების მიწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო ISO 3166-ის შესაბამისად)
ძალაშია (-დან) (Valid from)		+		-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)		+		-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)		+		+	სერტიფიკატების ინფრასტრუქტურაში სუბიექტის უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	SDA TimeStamping CA G(n)	+	შუალედური CA-ის დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		-	Public Service Development Agency	+	სანდო მომსახურების მიწოდებლის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+	Ministry of Justice of Georgia	+	სტრუქტურის დასახელება

ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის
სუბიექტის ღია გასაღები (Subject Public Key ხელმოწერა)		+	RSA 4096	-	შესაბამისად ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, 4096 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფიკატორი (OID)	მნიშვნელობა და შეზღუდვები (Values and Limitations)	კრიტიკულობა (Criticality)	სავალდებულო (Mandatory)
ძირითადი შეზღუდვები (Basic Constraints)			+	+
სუბიექტის ტიპი (Subject Type)		CA		
გზის სიგრძის შეზღუდვა (Path Length Constraint)		None		
გასაღების გამოყენება (Key Usage)		Certificate Signing, CRL Signing	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier= 1.3.6.1.4.1.37733.10.5.1.1.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://id.ge/pki	-	+
CRL-ის გავრცელების ნერტილები (CRL Distribution Points)		Full Name: URL= http://crl.cra.ge/geo(*)rootcag(n).crl	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)		KeyID=	-	+
სუბიექტის გასაღების იდენტიფიკატორი (Subject Key Identifier)			-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს ინფორმაციის ხელმისაწვდომობა			-	+

(Authority Information Access)				
OCSP		URL=http://ocsp.cra.ge/ocsp	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს სერტიფიკატის URL (CA Issuer Certificate URL)		URL: http://aia.id.ge/pki/GEORootCA.crt		

12¹. SDA Qualified TSU

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)		+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)		+		-	გაცემული სერტიფიკატის სერიული ნომერი
ხელმოწერის ალგორითმი (Signature Algorithm)		+	sha256RSA	-	ხელმოწერის ალგორითმი, რომელიც შეესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	SDA TimeStamping CA G(n)	-	სერტიფიკატის გამცემი ორგანოს დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Development Agency	-	სანდო მომსახურების მიწოდებლის დასახელება
ორგანიზაცია (Organisation) (O)		+	Ministry of Justice of Georgia	-	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	-	სანდო მომსახურების მიწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო ISO 3166-ის შესაბამისად)
ძალაშია (-დან) (Valid from)		+		-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)		+		-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება		+		+	სერტიფიკატების ინფრასტრუქტურაში

(Subject Distinguished Name)					სუბიექტის უნიკალური დასახელება
დასახელება (Common Name) (CN)		+		+	დროის კვალიფიციური აღნიშვნის დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		-	Public Service Development Agency	+	სანდო მომსახურების მიმწოდებლის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+	Ministry of Justice of Georgia	+	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	+	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი ISO 3166-ის შესაბამისად
სუბიექტის ლია გასაღები (Subject Public Key) ხელმოწერა		+	RSA 2048	-	ლია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, 2048 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფიკატორი (OID)	მნიშვნელობა და შეზღუდვები (Values and Limitations)	კრიტიკულობა (Criticality)	სავალდებულო (Mandatory)
ძირითადი შეზღუდვები (Basic Constraints)			+	+
სუბიექტის ტიპი (Subject Type)		End Entity		
გზის სიგრძის შეზღუდვა (Path Length Constraint)		None		
გასაღების გამოყენება (Key Usage)		Digital Signature, Non-Repudiation	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier= 1.3.6.1.4.1.37733.10.5.1.1.0 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://id.ge/pki	-	+
CRL-ის გავრცელების წერტილები (CRL Distribution Points)		Full Name: URL= http://crl.cra.ge/sdatimestampingcag(n).crl	-	+
გასაღების გაფართოებული გამოყენება		Time Stamping	-	+


(Extended Key Usage) სერტიფიკატის გამცემი ორგანოს გასაღების იდენტიფიკატორი			-	+
(Authority Key Identifier) სუბიექტის გასაღების იდენტიფიკატორი			-	+
(Subject Key Identifier) სერტიფიკატის გამცემი ორგანოს ინფორმაციის ხელმისაწვდომობა			-	+
(Authority Information Access) OCSP		URL=http://ocsp.cra.ge/ocsp	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს სერტიფიკატის URL (CA Issuer Certificate URL)		URL=http://aia.id.ge/pki/TimeStampingCAG(n).crt		

“

მუხლი 2. სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს ადმინისტრაციის (დეპარტამენტი) საქმისწარმოების სამსახურმა უზრუნველყოს ამ ბრძანების გაცნობა სააგენტოს სტრუქტურული ერთეულების/ქვედანაყოფებისა და ტერიტორიული სამსახურებისათვის, ასევე პერსონალურ მონაცემთა დაცვის ოფიცრისა და ინფორმაციული უსაფრთხოების მენეჯერისთვის.

მუხლი 3 . ეს ბრძანება ამოქმედდეს ხელმოწერისთანავე.

სახელმწიფო სერვისების განვითარების სააგენტოს თავმჯდომარე

ხელმოწერილია/
შტამგდასმულია
ელექტრონულად 

ქეთევან ბეთლემიძე