



საქართველოს იუსტიციის სამინისტრო სახელმწიფო სერვისების განვითარების სააგენტო



KA011823328215425

ბ რ ძ ა ნ ე ბ ა

27 / აგვისტო / 2025 წ.

№ 541/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, „სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს მიერ სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების განვითარების შინაგანაწესის დამტკიცების შესახებ“ საქართველოს იუსტიციის მინისტრის 2018 წლის 29 ივნისის N315 ბრძანებით დამტკიცებული წესის მე-6 მუხლის მე-5 პუნქტის 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 დამტკიცებული **შინაგანაწესის:**

ა) პირველი მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. დოკუმენტის დამოუკიდებელი იდენტიფიკატორია 1.3.6.1.4.1.37733.10.1.2.4.6.“;

ბ) 33-ე მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. გასაღების პარამეტრებია:

ა) კრიპტოგრაფიული ალგორითმი - RSA;

ბ) გასაღების სიგრძე - მინიმუმ 2048 ბიტი.“;

გ) 49-ე მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. გასაღების პარამეტრებია;

ა) კრიპტოგრაფიული ალგორითმი - RSA;

ბ) გასაღების სიგრძე - მინიმუმ 2048 ბიტი.“;

დ) 58-ე მუხლის მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. გასაღების პარამეტრებია:

ა) კრიპტოგრაფიული ალგორითმი - RSA;

ბ) გასაღების სიგრძე - მინიმუმ 2048 ბიტი.“;

ე) 74-ე მუხლის:

ე.ა) მე-2 პუნქტის „ბ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ბ) დროის კვალიფიციური აღნიშვნის მომსახურება ხელმისაწვდომია მინიმუმ RSA-2048 ტიპის გასაღებით“;

ე.ბ) მე-7 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„7. მინიმუმ 2048-ბიტიანი დროის კვალიფიციური აღმნიშვნელი ერთეულის სერტიფიკატში სუბიექტის იდენტიფიკატორია C = GE, O = Ministry of Justice of Georgia, OU = Public Service Development Agency, CN = SDA Qualified TSU <ნომერი>, სადაც <ნომერი> არის 01, 02 ... NN და წარმოადგენს დროის აღმნიშვნელი ერთეულის ნომერს.“.

ვ) 76-ე მუხლის მე-2 პუნქტი „ბ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ბ) დროის კვალიფიციური აღნიშვნის მომსახურება ხელმისაწვდომია მინიმუმ RSA-2048 ტიპის გასაღებით“;

ზ) N2 დანართი ჩამოყალიბდეს თანდართული რედაქციით.

მუხლი 2. სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს საქმისწარმოების სამსახურმა უზრუნველყოს ამ ბრძანების გაცნობა სააგენტოსა და ტერიტორიული სამსახურებისათვის.

მუხლი 3. ეს ბრძანება ძალაშია ხელმოწერისთანავე.

სახელმწიფო სერვისების განვითარების
სააგენტოს თავმჯდომარე

ხელმოწერილია/
შტამპდასმულია
ელექტრონულად



რუსუდან კობოძე

„1. GEO Signing CA G(n)

დანართი N2

სერტიფიკატის ტექნიკური პროფილები

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკა ტორი (OID)	სავალდებუ ლო (Mandatory)	მნიშვნელო ბა (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 შესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ძირითადი 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)		+		-	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)		+	GEO Signing CA G(n)	-	შუალედური CA-ის დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Developmen t 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 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 იდენტიფი კატორი (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=1.3.6.1.4.1.37733.10.3.1.2.0 [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)				-	+
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		

2. GEO Signing CA G(n)-ის მიერ გაცემული სერტიფიკატები

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკ ატორი (OID)	სავალდებუ ლო (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 შესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO Signing CA G(n)	-	სერტიფიკატის გამცემი ორგანოს 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 ინფრასტრუქტურაში სუბიექტის უნიკალური სახელი
სახელი (Common Name) (CN)		+		+	ფიზიკური პირის სახელი და გვარი
სერიული ნომერი (Serial Number)		+	PNOGE- ??????????	+	11-ნიშნა პირადი ნომერი, პრეფიქსით "PNOGE-"
სუბიექტის მოქალაქეობა (Organisation Name) (O)		+		+	ფიზიკური პირის საქართველოს მოქალაქეობა (Citizen/Resident)
სუბიექტის ბინადრობა (Organisational Unit) (OU)		+		+	სავალდებულოა ბინადრობის მოწმობის შემთხვევაში. ფიზიკური პირის ბინადრობის ნებართვა (მუდმივი/დროებითი)
ქვეყანა (Country) (C)		+	GE	-	საქართველოს კოდი ISO 3166-ის შესაბამისად
სახელი (Givenname) (G)		+		+	ფიზიკური პირის სახელი
გვარი (Surname) (SN)		+		+	ფიზიკური პირის გვარი

სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥ 2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 2048 ბიტი
ხელმოწერა (Signature)		+	ბინარული მოწმებები	-	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)		Non-Repudiation	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier=1.3.6.1.4.1.37733.10.3.1.2.0 [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/geosigningcag(n).crl	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)			-	+
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/GEOSigningCAG(n).crt		
სუბიექტის ალტერნატიული სახელი (Subject Alternative Name)				

Directory Address	CN	ფიზიკური პირის სახელი, გვარი ქართულად და პირადი ნომერი	-	-
კვალიფიციური სერტიფიკატის განცხადება (Qualified Certificate Statement)		- id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) - id-etsi-qcs-semanticId-Natural (0.4.0.194121.1.1) - etsiQcsCompliance (0.4.0.1862.1.1) - etsiQcsQcSSCD (0.4.0.1862.1.4) - QcType (0.4.0.1862.1.6)=QcType-esign(0.4.0.1862.1.6.1) - QcPDS (0.4.0.1862.1.5)= https://id.ge/pki, ka - QcCClegislation(0.4.0.1862.1.7)=GE		

4. Biometric Data Encryption

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფი კატორი (OID)	სავალდებუ ლო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)		+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)		+	7c 61 9d 4d cc 39 ae d8	-	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)		+	Biometric Encryption CA	-	სერტიფიკატის გამცემი ორგანოს 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)		+	2016 წლის 01 12, 15:49:26	-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)		+	2018 წლის 01 12, 15:49:26	-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)		+		+	სერტიფიკატების ინფრასტრუქტურაში სუბიექტის უნიკალური სახელი
დასახელება (Common Name) (CN)		+	Biometric Data Encryption	+	შუალედური CA-ის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+		+	ორგანიზაციის ის სახელი, რომელიც მითითებულია სერტიფიკატის განცხადებაში
სუბიექტის უნიკალური იდენტიფიკატორი (UID)		+		+	
ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
სერიული ნომერი (Serial Number)				-	ორგანიზაციისათვის გაცემული სერტიფიკატის რიგითი ნომერი
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥ 2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 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)		Key Encipherment, Data Encipherment	+	+

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/geobioencca.crl	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)		KeyID=e9 81 48 b7 32 6c 66 3b bc fc 0b 09 90 92 0c ad 81 30 9e 64	-	+
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/BiometricEncryptionCA.crt		
სუბიექტის ალტერნატიული სახელი (Subject Alternative Name)				

5. GEO Authentication CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფი კატორი (OID)	სავალდებუ ლო (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	-	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)			+		-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)			+		-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)			+		-	სერტიფიკატების ინფრასტრუქტურაში სუბიექტის უნიკალური სახელი
	დასახელება (Common Name) (CN)		+	GEO Authentication CA G(n)	-	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	-	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი ISO 3166-ის შესაბამისად
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 იდენტიფიკ ატორი (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=1.3.6.1.4.1.37733.10.4.1.2.0 [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)			-	+
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		

6. GEO Authentication CA G(n)-ის გაცემული სერტიფიკატი

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკა ტორი (OID)	სავალდებუ ლო (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 შესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO Authentication CA G(n)	-	სერტიფიკატის გამცემი ორგანოს 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 ინფრასტრუქტურაში სუბიექტის უნიკალური სახელი
სახელი (Common Name) (CN)		+		+	ფიზიკური პირის სახელი და გვარი
სერიული ნომერი (Serial Number)		+	PNOGE-?????????	+	11-ნიშნა პირადი ნომერი, პრეფიქსით "PNOGE-"
სუბიექტის მოქალაქეობა (Organisation Name) (O)		+		-	ფიზიკური პირის საქართველოს მოქალაქეობა (Citizen/Resident)
სუბიექტის ბინადრობა (Organisational Unit) (OU)		+		-	სავალდებულოა ბინადრობის მოწმობის შემთხვევაში. ფიზიკური პირის ბინადრობის ნებართვა (მუდმივი/დროებითი)
ქვეყანა (Country) (C)		+	GE	-	საქართველოს კოდი ISO 3166-ის შესაბამისად
სახელი (Givenname) (G)		+		+	ფიზიკური პირის სახელი
გვარი (Surname) (SN)		+		+	ფიზიკური პირის გვარი
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥ 2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 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, Key Encipherment	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier=1.3.6.1.4.1.37733.10.4.1.2.0 [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/geoauthenticationcag(n).crl	-	+
გასაღების გაფართოებული გამოყენება (Extended Key Usage)		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)			-	+
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/GEOAuthenticationG(n).crt		
სუბიექტის ალტერნატიული სახელი (Subject Alternative Name)				
Directory Address	CN	ფიზიკური პირის სახელი, გვარი ქართულად და პირადი ნომერი	-	-
სხვა სახელი (Other Name)	Principal Name	UPN_?????????@citizen.ge	-	-

8. GEO ESeal CA G(n)-ის გაცემული სერტიფიკატი

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკა ტორი (OID)	სავალდებუ ლო (Mandatory)	მნიშვნელობა (Value)	ცვალეადი (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 შესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	GEO eSeal CAG(n)	-	სერტიფიკატის გამცემი ორგანოს 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 ინფრასტრუქტურაში სუბიექტის უნიკალური დასახელება
დასახელება (Common Name) (CN)		+		+	სუბიექტის სერტიფიკატის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+		+	ორგანიზაციის ის დასახელება, რომელიც მითითებულია სერტიფიკატის განცხადებაში
ორგანიზაციის იდენტიფიკატორი		+	NTRGE???????	+	ორგანიზაციის საიდენტიფიკაციო კოდი, პრეფიქსით NTRGE
ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 2048 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)		ობიექტის იდენტიფი კატორი (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)			Non-Repudiation	+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)			Policy Identifier=1.3.6.1.4.1.37733.10.7.1.1.0 [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/geosealca g(n).crl	-	+
სუბიექტის ალტერნატიული სახელი (Subject Alternate Name)			O=ორგანიზაციის დასახელება ქართულ ენაზე		
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)				-	+
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)		URI: http://aia.id.ge/pki/GEOESealCAG (n).crt		
კვალიფიციური სერტიფიკატის განცხადება (Qualified Certificate Statement)			- id-qcs-pkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2) - id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) - etsiQcsCompliance (0.4.0.1862.1.1) - etsiQcsQcSSCD (0.4.0.1862.1.4) - QcType (0.4.0.1862.1.6)= QcType-eseal (0.4.0.1862.1.6.2) - QcPDS (0.4.0.1862.1.5)= https://id.ge/pki, ka		

- QcCClegislation (0.4.0.1862.1.7) =GE

9¹. GEO (*) Root CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკა ტორი (OID)	სავალდებუ ლო (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 ინფრასტრუქტურაში სუბიექტის 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
სუბიექტის დასახელება (Organisation Name) (O)		+	Ministry of Justice of Georgia	+	სტრუქტურის დასახელება

ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
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)			+	+
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier=1.3.6.1.4.1.37733.10.1.2.4.6 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://id.ge/pki	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)		KeyID=	-	+
სუბიექტის გასაღების იდენტიფიკატორი (Subject Key Identifier)			-	+

11. SDA TimeStamping CA

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	-	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)		+		-	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	+	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 შესაბამისად
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=1.3.6.1.4.1.37733.10.5.1.2.0 [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)				-	+
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		

11¹. SDA TimeStamping CA

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 შესაბამება 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)		+	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)		+		-	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 მიმწოდებლის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+	Ministry of Justice of Georgia	+	სტრუქტურის დასახელება
ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
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=1.3.6.1.4.1.37733.10.5.1.2.0 [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/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		

12. SDA Qualified TSA

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		+			გაცემული სერტიფიკატის სერიული

(Serial Number)				-	ნომერი
ხელმოწერის ალგორითმი (Signature Algorithm)		+	sha256RSA	-	ხელმოწერის ალგორითმი, რომელიც შესაბამება RFC 5280 სტანდარტს
სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება (Issuer Distinguished Name)		+		-	სერტიფიკატის გამცემი ორგანოს უნიკალური დასახელება
დასახელება (Common Name) (CN)		+	SDA TimeStamping CA	-	სერტიფიკატის გამცემი ორგანოს 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 ინფრასტრუქტურაში 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	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 2048 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფი კატორი (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=1.3.6.1.4.1.37733.10.5.1.2.0 [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/sdtimestamping.ca.crl	-	+
გასაღების გაფართოებული გამოყენება (Extended Key Usage)			Time Stamping	-	+
სერტიფიკატის გამცემი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)				-	+
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/TimeStampingCA.crt		

12¹. SDA Qualified TSU

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფი კატორი (OID)	სავალდებუ ლო (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 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 ინფრასტრუქტურაში 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	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 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= 1.3.6.1.4.1.37733.10.5.1.2.0 [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/sdatimestamping cag(n).crl	-	+
გასაღების გაფართოებული გამოყენება (Extended Key Usage)		Time Stamping	-	+
სერტიფიკატის გამცემი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)			-	+
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/TimeStampin gCAG(n).crt		

14. GEO Organizational Authentication CA G(n)-ის გაცემული სერტიფიკატი

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკა ტორი (OID)	სავალდებუ ლო (Mandatory)	მნიშვნელო ბა (Value)	ცვალბადი (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)		+	GEO Organizatio nal Authenticati on CA G(n)	-	სერტიფიკატის გამცემი ორგანოს დასახელება
ორგანიზაციული ერთეული (Organisational Unit) (OU)		+	Public Service Developmen t 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 ინფრასტრუქტურაში სუბიექტის უნიკალური დასახელება
დასახელება (Common Name) (CN)		+		+	სუბიექტის სერტიფიკატის დასახელება
სუბიექტის დასახელება (Organisation Name) (O)		+		+	ორგანიზაციის ის დასახელება, რომელიც მითითებულია სერტიფიკატის განცხადებაში
ორგანიზაციის იდენტიფიკატორი		+	NTRGE- ??????????	+	ორგანიზაციის საიდენტიფიკაციო კოდი, პრეფიქსით NTRGE

ქვეყანა (Country) (C)		+	GE	+	საქართველოს კოდი ISO 3166-ის შესაბამისად
სუბიექტის ღია გასაღები (Subject Public Key)		+	RSA ≥ 2048	-	ღია გასაღები, რომელიც შექმნილია RSA ალგორითმით RFC 4055-ის შესაბამისად, მინიმუმ 2048 ბიტი
ხელმოწერა (Signature)		+	ბინარული მონაცემები	-	სერტიფიკატის გამცემი ორგანოს დადასტურების ხელმოწერა

სერტიფიკატის გაფართოებები

გაფართოება (Extension)	ობიექტის იდენტიფი კატორი (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, Key Encipherment	+	+
გასაღების გაფართოებული გამოყენება (Extended Key Usage)		Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)		
სერტიფიკატის პოლიტიკები (Certificate Policies)		Policy Identifier=1.3.6.1.4.1.37733.10.8.1.1.0 [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/geoorganizationalauthenticationcag(n).crl	-	+
სუბიექტის ალტერნატიული სახელი (Subject Alternate Name)		O=ორგანიზაციის დასახელება ქართულ ენაზე	-	+
სერტიფიკატის გამცემი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)			-	+
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)		URI:http://aia.id.ge/pki/GEOOrganizationalAuthenticationCAG(n).crt		