<u>პროექტი</u>

„სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების გაწევის 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 გაწევის წესის 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:

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

1. შინაგანაწესის პირველი მუხლის:

ა) პირველი პუნქტის „ი“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რეჰდაქციით:

„ი) სერტიფიკატის გამცემი ძირითადი ორგანოების (GEO Root CA; GEO (*) Root CA G (n)) მიერ სერტიფიკატების გაცემა, მართვა და გამოყენება.“;

ბ) მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. დოკუმენტის დამოუკიდებელი იდენტიფიკატორია 1.3.6.1.4.1.37733.10.1.2.4.4.“;

2. მე-2 მუხლს დაემატოს შემდეგი შინაარსის „ძ“ და „წ“ ქვეპუნქტები:

„ძ) (*) - სერტიფიკატის გამცემი ძირითადი ორგანოს დასახელებაში ცვალებადი ნაწილი, რომელიც განსაზღვრავს მის ტიპს (Generic – (ზოგადი) გამოიყენება ყველა სერტიფიკატების

გასაცემად, Trust – (სანდო) გამოიყენება სანდო მომსახურების სერტიფიკატების გასაცემად და სხვა.);

წ) G(n) - სერტიფიკატის გამცემი ორგანოს რიგითი ნომერი.“.

3. მე-8 მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. შინაგანაწესის ამ მუხლის პირველი პუნქტის შესაბამისად განსაზღვრული ფუნქციის ფარგლებში, სერტიფიცირების ცენტრი მართავს:

ა) სერტიფიკატის გამცემ ძირითად ორგანოებს - „GEO Root CA; GEO (*) Root CA G(N)“, რომელიც მოქმედებს თვითხელმოწერილი სერტიფიკატებით და გამოიყენება საწყის ნდობის წერტილად ზოგადი გამოყენების სანდო მომსახურებებისთვის. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის X თავით დადგენილი წესის შესაბამისად;

ბ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO Signing 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 III თავით დადგენილი წესის შესაბამისად;

გ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO Authentication 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 III თავით დადგენილი წესის შესაბამისად;

დ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „Biometric Encryption CA“ , 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;

ე) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „SDA Time Stamping CA“ , რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის VIII თავით დადგენილი წესის შესაბამისად;

ვ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO ESeal 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 IV თავით დადგენილი წესის შესაბამისად;

ზ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO Organizational Authentication 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 V თავით დადგენილი წესის შესაბამისად;

თ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „SDA Time Stamping CA G(n)“, რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „ GEO (*) Root CA G(N) “ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის VIII თავით დადგენილი წესის შესაბამისად.“.

4. მე-11 მუხლის მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სუბიექტებს წარმოადგენენ ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ბ“-„თ“ ქვეპუნქტებით განსაზღვრული ორგანოები, რომლებიც ექვემდებარებიან სერტიფიკატების გამცემ ორგანოებს („GEO Root CA ან GEO (*) Root CA G(n)“) და მოქმედებენ ამავე ორგანოს მიერ გაცემული სერტიფიკატების საფუძველზე.“.

5. 29-ე მუხლის მე-3 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„3. სუბიექტს შეუძლია სააგენტოს დისტანციური მომსახურების სამსახურში ელექტრონული ფორმით წარადგინოს კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაუქმების შესახებ ზეპირი განცხადება, თუ ელექტრონული კომუნიკაცია იძლევა განმცხადებლისა და განცხადების მიღებაზე უფლებამოსილი პირის პირდაპირი ვიზუალური კონტაქტის საშუალებას. აღნიშნული მიმართვისას სუბიექტმა უნდა გაიაროს იდენტიფიკაცია და ავთენტიფიკაცია (სააგენტოს მონაცემთა ელექტრონულ ბაზაში პიროვნების პერსონალური მონაცემების შემოწმების გზით) ამასთან მან უნდა მიუთითოს სერტიფიკატის გაუქმების საფუძველი. ამ პუნქტით გათვალისწინებული განცხადების წარდგენა შესაძლებელია sda.gov.ge – მეშვეობით.“.

6. 74-ე მუხლის მე-7 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„7. 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.“.

7. 88-ე მუხლის მე-3 პუნქტის:

ა) „ა“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ა) სერტიფიკატის გამცემი ძირითადი ორგანო „GEO Root CA“ - http://crl.cra.ge/georootca.crl; ან GEO (*) Root CA G(n) თავისი მისამართით http://crl.cra.ge/geo(*)rootcag(n).crl;“;;

ბ) „ე“-„ვ“ ქვეპუნქტები ჩამოყალიბდეს შემდეგი რედაქციით:

ე) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „SDA Time Stamping CA“ – http://crl.cra.ge/sdatimestampingca.crl; ან SDA Time Stamping CA G(n) –

http://crl.cra.ge/sdatimestampingcag(n).crl;

ვ) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „GEO ESeal CA G(n)“ - http://crl.cra.ge/geoesealcag(n).crl;“.

8. 98-ე მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

„მუხლი 98. სერტიფიკატის გამცემი ძირითადი ორგანოს სერტიფიკატი, ძირითადი ორგანოს მიერ გაცემული სერტიფიკატები, სერტიფიკატების გამოყენების წესი

1. სერტიფიკატის გამცემი ძირითადი ორგანოები - GEO Root CA; GEO (*) Root CA G(n) - გამოიყენება საწყის ნდობის წერტილად ზოგადი გამოყენების სანდო მომსახურებებისთვის. ისინი მოქმედებენ თვითხელმოწერილი სერტიფიკატებით.

2. GEO Root CA-სა და GEO (*) Root CA G(n) - ს მიერ გაცემული სერტიფიკატების გამოყენება დასაშვებია მხოლოდ სერტიფიკატების გასაცემად და გაუქმებული სერტიფიკატების სიაზე ხელმოსაწერად, წინამდებარე შინაგანაწესით დადგენილი წესის შესაბამისად.

3. სერტიფიკატის გამცემი ძირითადი ორგანოები - GEO Root CA და GEO (*) Root CA G(n) - სერტიფიკატებს გასცემს მხოლოდ სააგენტოს ფარგლებში მოქმედ და წინამდებარე შინაგანაწესში განსაზღვრულ სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოებზე და სერტიფიკატის სტატუსის ონლაინ დადასტურების მომსახურებაზე. სხვა ფიზიკურ ან იურიდიულ პირებზე სერტიფიკატი არ გაიცემა. ახალი სერტიფიკატის ასაღებად საჭიროა დასაბუთებული მიმართვის წარდგენა, წინამდებარე შინაგანაწესით დადგენილი წესის შესაბამისად.

4. სერტიფიკატის გამცემი ძირითადი ორგანოების მიერ გაცემული სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. ეს მომსახურებები და მათი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.“.

9. 99-ე მუხლის პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. სერტიფიკატის გამცემ ორგანოებს მინიჭებული აქვთ შემდეგი განმასხვავებელი სახელები:

ა) „GEO Root CA“: C=GE, O=Ministry of Justice of Georgia, OU=Civil Registry Agency, CN=GEO Root CA; GEO (*) Root CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service Development Agency, CN=GEO (*) Root CA G(n);

ბ) „GEO Signing CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU= Public Service Development Agency, CN=GEO Signing CA G(n);

გ) „GEO Authentication CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU= Public Service Development Agency, CN=GEO Authentication CA G(n);

დ) „Biometric Encryption CA“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service

Development Agency, CN=Biometric Encryption CA;

ე) „GEO ESeal CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service

Development Agency, CN= GEO ESeal CA G(n);

ვ) „SDA TimeStamping CA“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service Development Agency, CN= SDA TimeStamping CA ; და „SDA TimeStamping CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service Development Agency, CN= SDA TimeStamping CA G(n);

ზ) „GEO Organizational Authentication CA G(n)“: C=GE, O=Ministry of Justice of Georgia, OU=Public Service Development Agency, CN= GEO Organizational Authentication CA G(n).”.

10. 130-ე მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. სერტიფიკატის გამცემი ძირითადი ორგანოების (GEO Root CA; GEO (*) Root CA G(n)) გასაღების წყვილი იქმნება და ინახება უსაფრთხოების აპარატურული მოდულის მოსახსნელ სეგმენტში, რომელიც მუდმივად განცალკევებულია უსაფრთხოების აპარატურული მოდულისგან, მოთავსებულია იმავე მონაცემთა დამუშავების ცენტრში არსებულ სეიფში და მისი მიერთება უსაფრთხოების აპარატურულ მოდულთან და გააქტიურება ხდება მხოლოდ აუცილებლობის შემთხვევაში (გაუქმებული სერტიფიკატების სიის შესაქმნელად, სერტიფიკატის სტატუსის ონლაინ დადასტურების მომსახურების, სერტიფიკატის გამცემი დაქვემდებარებული ორგანოს და სხვა სერტიფიკატების გაცემისას და სხვა). მოსახსნელი სეგმენტის გააქტიურებისათვის აუცილებელია მინიმუმ ორი უფლებამოსილი პირის მონაწილეობა.“.

11. შინაგანაწესს დაემატოს :

ა) N9[1] დანართი თანდართული რედაქციით;

ბ) N11[1] და N12 [1] დანართები თანდართული რედაქციით.

მუხლი 2 სსიპ - სახელმწიფო სერვისების განვითარების სააგენტოს 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.

9[1]. 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 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	+	სანდო მომსახურების მიმწოდებლის ქვეყნის კოდი: GE – Georgia (2 სიმბოლო 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= 1.3.6.1.4.1.37733.10.1.2.4.4 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[1]. 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 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

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 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)				-	+

12[1]. 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 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

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/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 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		