სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების გაწევის შინაგანაწესი

თავი I

ზოგადი დებულებები

მუხლი 1. შინაგანაწესის არსი

1. სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების გაწევის შინაგანაწესი (შემდგომში - შინაგანაწესი) წარმოადგენს საჯარო სამართლის იურიდიულ პირ - სახელმწიფო სერვისების განვითარების სააგენტოში (შემდგომში - სააგენტო) მოქმედი სანდო მომსახურების მიმწოდებლის შინაგანაწესს, რომელიც განსაზღვრავს ქვემოთ ჩამოთვლილი სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების მიდგომებსა და პროცედურებს:

   ა) სანდო მომსახურების მიმწოდებლის მომსახურების ზოგადი მიდგომები და პროცედურები;
   ბ) პირადობის (ბინადრობის) ელექტრონულ მოწმობებზე კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაცემა და მომსახურება;
   გ) პირადობის (ბინადრობის) ელექტრონულ მოწმობებზე ავთენტიფიკაციის სერტიფიკატების გაცემა და მომსახურება;
   დ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატების გაცემა და მომსახურება;
   ე) ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემა და მომსახურება;
   ვ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის, შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება;
   ზ) დროის კვალიფიციური აღნიშვნის მომსახურება;
   თ) გაუქმებული სერტიფიკატების სიის ხელმისაწვდომობა და სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურება;
   ი) სერტიფიკატის გამცემი ძირითადი ორგანოს (GEO Root CA) მიერ სერტიფიკატების გაცემა, მართვა და გამოყენება.

2. დოკუმენტის დამოუკიდებელი იდენტიფიკატორია 1.3.6.1.4.1.37733.10.1.2.4.3; **(ცვლილება 2021.06.07.N245/ს)**

3. ამ შინაგანაწესით განსაზღვრული საკითხები ემსახურება შემდეგი პოლიტიკებით დასახული მიზნების შესრულებას:

   ა) კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკა;
   ბ) პირადობის (ბინადრობის) ელექრონულ მოწმობაზე კვალიფიციური ელექტრონული ხელმოწერისა და ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკა;
   გ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკა;
   დ) დროის კვალიფიციური აღნიშვნის მოომსახურების მიწოდების პოლიტიკა.

მუხლი 2. ტერმინთა განმარტება

ამ შინაგანაწესის მიზნებისათვის მასში გამოყენებულ ტერმინებს აქვს შემდეგი მნიშვნელობა:

ა) დროის აღმნიშვნელი ორგანო - სანდო მომსახურების მიმწოდებლის დაქვემდებარებაში მყოფი კომპიუტერული სისტემის (პროგრამული და აპარატურული უზრუნველყოფა), როლებისა და პროცედურების კომპლექსი, რომელიც გამიზნულია დროის აღნიშვნის მომსახურების გასაწევად;

ბ) დროის აღმნიშვნელი ერთეული - კომპიუტერული სისტემა (პროგრამული და აპარატურული უზრუნველყოფა), რომელიც განკუთვნილია დროის აღნიშვნის მომსახურების გასაწევად, შესაძლებელია განცალკევდეს სხვა ერთეულებისგან და გააჩნია მხოლოდ ერთი აქტიური დახურული გასაღები კვალიფიციური ელექტრონული ხელმოწერის შესაქმნელად;

გ) დროის აღნიშვნის ტოკენი - სპეციალური წესით სტრუქტურირებული, კვალიფიციური ელექტრონული ხელმოწერით შესრულებული მონაცემების ერთობლიობა, რომელსაც შეუძლია დაადასტუროს გარკვეული ინფორმაციის არსებობა დროის კონკრეტულ მომენტში;

დ) UTC - კოორდინირებული უნივერსალური დრო, დროის აღრიცხვის საერთაშორისო სტანდარტი, რომელიც დადგენილია და იმართება ზომისა და წონის საერთაშორისო ბიუროს მიერ;

ე) HTTP - ჰიპერტექსტების გადაცემის პროტოკოლი;

ვ) GPS - გლობალური პოზიციონირების სისტემა (Global Positioning System) რადიოსიგნალებზე დაფუძნებული თანამგზავრული ნავიგაციის სისტემა, რომელიც შექმნილია და იმართება ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტის მიერ;

ზ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემა - კომპიუტერული სისტემა (პროგრამული და აპარატურული უზრუნველყოფა), რომელიც გამოიყენება სანდო მომსახურების მიწოდების მიზნით, მათ შორის, სერტიფიკატის შექმნაზე მოთხოვნის მიღების, დამუშავების, ასევე, სერტიფიკატების კვალიფიციური ელექტრონული ხელმოწერის შექმნის მოწყობილობებისა და სერტიფიკატის გაუქმების მართვისთვის;

თ) უსაფრთხოების აპარატურული მოდული - სტაციონარული მოწყობილობა, რომელიც უზრუნველყოფს უსაფრთხოებას კრიპტოგრაფიული გასაღების შექმნის, შენახვისა და გარდაქმნისას;

ი) დროის აღნიშვნის მომსახურება - მომსახურება, რომელიც გულისხმობს მომხმარებლებისთვის დროის აღნიშვნის ტოკენების მიწოდებას მათ მიერ წარმოდგენილი ინფორმაციის არსებობის დროის დასადასტურებლად;

კ) ღია გასაღები - კრიპტოგრაფიული გასაღების წყვილის მდგენელი, რომლის გამოყენება შეზღუდული არ არის და, საჭიროების შემთხვევაში, გადაეცემა ნებისმიერ დაინტერესებულ პირს და მისგან გონივრულ ფარგლებში შეუძლებელია დახურული გასაღების გამოყვანა (აღდგენა), გარდა დახურული გასაღების ყველა შესაძლო ვარიანტის გადარჩევისა;

ლ) სუბიექტის მოწყობილობა - კვალიფიციური ელექტრონული შტამპის შექმნისა და ავთენტიფიკაციის სერტიფიკატის გამოყენების საშუალება, რომელიც აკმაყოფილებს "ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ" საქართველოს კანონით დადგენილ მოთხოვნებს და რომელზეც, ამ შინაგანაწესის შესაბამისად, იქმნება და ინახება სუბიექტის დახურული გასაღები კვალიფიციური ელექტრონული შტამპისა და ავთენტიფიკაციის სერტიფიკატისთვის;

მ) კრიპტოგრაფიული გასაღების სერტიფიკატი - ელექტრონული დოკუმენტი, გაცემული და განვითარებული ელექტრონული ხელმოწერით ან განვითარებული ელექტრონული შტამპით დამოწმებული სერტიფიკატის გამცემი ორგანოს მიერ, რომელიც ადასტურებს ღია გასაღების კუთვნილებას კონკრეტული სუბიექტისადმი;

ნ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატი - "ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ" საქართველოს კანონის მოთხოვნების დაცვით გაცემული ელექტრონული დოკუმენტი;

ო) კვალიფიციური ელექტრონული შტამპი - "ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ" საქართველოს კანონის მოთხოვნების დაცვით შექმნილი ელექტრონულ მონაცემთა ერთობლიობა;

პ) სერტიფიკატის გამცემი ორგანო - სანდო მომსახურების მიმწოდებლის მიერ მართული კომპიუტერული სისტემის (პროგრამული და აპარატურული უზრუნველყოფა), როლებისა და პროცედურების კომპლექსი, რომელიც გამიზნულია სერტიფიკატების შესაქმნელად, გასაცემად და მასთან დაკავშირებული მომსახურების გასაწევად;

ჟ) სანდო მომსახურების მიმწოდებელი - სააგენტოს სხვადასხვა სტრუქტურული ერთეულის თანამშრომლებისგან დაკომპლექტებული ჯგუფი, რომელიც ასრულებს კვალიფიციური სანდო მომსახურების მიწოდებისთვის „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ" საქართველოს კანონით განსაზღვრულ ფუნქციებს;

რ) კრიპტოგრაფიული გასაღების წყვილი - იმგვარად დაკავშირებული ორი ურთიერთგანსხვავებული მონაცემი (მდგენელი), რომელთაგან ერთ-ერთი მონაცემის თანამონაწილეობით საწყის ინფორმაციაზე მათემატიკური ან/და ლოგიკური გარდაქმნებით მიღებული ინფორმაციიდან საწყისი ინფორმაციის გამოყვანა (აღდგენა) გონივრულ ფარგლებში შესაძლებელია მხოლოდ მეორე მონაცემის თანამონაწილეობით, მათემატიკური ან/და ლოგიკური გარდაქმნებით, და დაცულია გონივრულ ფარგლებში, სულ მცირე, ერთ-ერთი მდგენელიდან (ღია გასაღები) მეორე მდგენელის (დახურული გასაღები) გამოყვანის (აღდგენის) შეუძლებლობის პირობა, გარდა მეორე მდგენელის ყველა შესაძლო ვარიანტის გადარჩევისა;

ს) სერტიფიკატის გაცემა - სერტიფიკატის გამცემი ორგანოს გამოყენებით ახალი სერტიფიკატის შექმნა სუბიექტისთვის;

ტ) სამეწარმეო რეესტრი - სსიპ საჯარო რეესტრის ეროვნული სააგენტოს მიერ წარმოებული მეწარმეთა და არასამეწარმეო (არაკომერციულ) იურიდიულ პირთა რეესტრი;

უ) ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობა - პორტატული მოწყობილობა, რომელსაც შეუძლია ბიომეტრიული მონაცემების დეშიფრაციის დახურული გასაღებისა და შიფრაციის სერტიფიკატის უსაფრთხოდ შენახვა, ასევე, დაშიფრული ბიომეტრიული მონაცემების დეშიფრაცია;

ფ) ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახი - უსაფრთხოების აპარატურული მოდული, რომელიც განკუთვნილია ბიომეტრიული მონაცემების დეშიფრაციის გასაღებებისა და შიფრაციის სერტიფიკატების უსაფრთხოდ შესანახად;

ქ) ბიომეტრიული მონაცემები - ნებისმიერი ფიზიკური, ფსიქიკური ან ქცევითი მახასიათებელი, რომელიც უნიკალური და მუდმივია თითოეული ფიზიკური პირისათვის და რომლითაც შესაძლებელია ამ პირის იდენტიფიცირება (თითის ანაბეჭდები, პირადი ხელმოწერის ინდივიდუალური მახასიათებლები, თვალის ფერადი გარსი, თვალის ბადურის გარსი (თვალის ბადურის გამოსახულება), სახის მახასიათებლები და დნმ-ის კოდი);

ღ) სანდო მომსახურების მიმწოდებლის ხელმძღვანელი - სააგენტოს სტრუქტურული ქვედანაყოფის ინფორმაციული ტექნოლოგიებისა და სისტემების დეპარტამენტის დირექტორი;

ყ) X.509 - ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ სერტიფიკატებისათვის დადგენილი RFC (Request for Comments) 5280 სტანდარტის მიხედვით დადგენილი ფორმატი;

შ) კომპრომეტირება - შემთხვევა როდესაც არსებობს დასაბუთებული ვარაუდი დახურული გასაღების ან/და აქტივაციის მონაცემების არაუფლებამოსილი პირის მიერ გამოყენების ან/და გამოყენების საფრთხის შესახებ;

ჩ) მომხმარებლის მოწყობილობა - აპარატურული ან/და პროგრამული საშუალება, რომლის გამოყენებაც შესაძლებელია მონაცემების შიფრაციისთვის. მომხმარებლის მოწყობილობას შეიძლება გააჩნდეს გასაღების წყვილის ამავე მოწყობილობაში გენერაციის შესაძლებლობა;

ც) დახურული გასაღები - კრიპტოგრაფიული გასაღების წყვილის მდგენელი, რომელიც, როგორც წესი, იმყოფება შეზღუდული რაოდენობის პირების (უმეტეს შემთხვევაში, ერთი პირის) კონტროლქვეშ და გამოიყენება ისეთი ოპერაციების ჩასატარებლად, რომლებზეც მხოლოდ ეს პირები არიან უფლებამოსილი.

მუხლი 3. მომსახურების მიწოდების სტანდარტები

1. კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან მიმართებით დოკუმენტი ეფუძნება QCP-l-qscd პროფილის მოთხოვნებს (იდენტიფიკატორი 0.4.0.194112.1.3).
2. ავთენტიფიკაციის სერტიფიკატთან მიმართებით დოკუმენტი ეფუძნება NCP+ პროფილის მოთხოვნებს (იდენტიფიკატორი 0.4.0.2042.1.2).
3. დროის კვალიფიციური აღნიშვნის მომსახურება სრულად შეესაბამება ევროპული სატელეკომუნიკაციო სტანდარტების ინსტიტუტის (European Telecommunications Standards Institute, ETSI) მიერ EN 319 421 სტანდარტით განსაზღვრულ საბაზისო შინაგანაწესს (BTSP; ობიექტის იდენტიფიკატორი 0.4.0.02023.1.1), ხოლო დროის აღმნიშვნელი ერთეულის სერტიფიკატები გაიცემა შესაბამისი სტანდარტით განსაზღვრული QCP-l (იდენტიფიკატორი 0.4.0.194112.1.1) პროფილის მიხედვით.
4. ბიომეტრიული მონაცემების შიფრაცია/დეშიფრაციისთვის საჭირო გასაღებთა წყვილების, სერტიფიკატების გაცემის წესი ეფუძნება NCP პროფილის მოთხოვნებს (იდენტიფიკატორი 0.4.0.2042.1.1).
5. ფიზიკური პირის სახელზე კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატთან მიმართებით წინამდებარე დოკუმენტი ეფუძნება QCP-n-qscd პროფილის მოთხოვნებს (იდენტიფიკატორი 0.4.0.194112.1.2).

მუხლი 4. სანდო მომსახურების მიმწოდებლის ზოგადი ვალდებულებები

1. სანდო მომსახურების მიმწოდებელი პასუხისმგებელია სანდო მომსახურების მიწოდებასთან დაკავშირებული ვალდებულებების ჯეროვან შესრულებაზე იმ შემთხვევაშიც კი, როდესაც ცალკეული პროცედურები ან მომსახურებები მისი თანხმობით ხორციელდება მესამე პირის მიერ.

2. სანდო მომსახურების მიმწოდებლის ფუნქციებია:

   ა) ამ დოკუმენტით განსაზღვრული მომსახურების მიწოდება;

   ბ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების მართვა;

   გ) სანდო მომსახურების მიწოდებასთან დაკავშირებული პროცესების საერთაშორისო სტანდარტებთან და საუკეთესო პრაქტიკასთან შესაბამისობის უზრუნველყოფა;

დ) სანდო მომსახურების მიწოდებასთან დაკავშირებული პროცესების ზოგადი ზედამხედველობა/აუდიტი.

მუხლი 5. დოკუმენტის მართვა

1. წინამდებარე დოკუმენტის მიზნებისთვის, დოკუმენტის მართვა გულისხმობს მის პერიოდულ (სულ მცირე, წელიწადში ერთხელ) განხილვას და, საჭიროების შემთხვევაში, მასში ცვლილების/ცვლილებების შეტანას.

2. შინაგანაწესის მართვაზე პასუხისმგებელია სანდო მომსახურების მიმწოდებლის ხელმძღვანელი.

2[1].სანდო მომსახურების მიმწოდებელი სააგენტოს ოფიციალურ ვებგვერდზე - https://id.ge/pki შინაგანაწესის ცვლილების პროექტის გამოქვეყნების მეშვეობით, აცნობებს მისი მომსახურების მომხმარებელს შინაგანაწესში შეტანილი ნებისმიერი ცვლილების თაობაზე.

3. შინაგანაწესს სააგენტოს ოფიციალურ ვებგვერდზე - https://id.ge/pki აქვეყნებს სააგენტოს სტრუქტურული ერთეული, გარე მომხმარებლებთან ურთიერთობის სამსახური. აღნიშნულ ვებგვერდზე, ასევე, ქვეყნდება შინაგანაწესის ყველა ცვლილების პროექტი, შინაგანაწესში შესული ყველა ცვლილება და მათი შესაბამისი შინაგანაწესის კოდიფიცირებული ვერსია.

3[1]. სანდო მომსახურების მიმწოდებელი ცვლილების შეტანამდე სულ მცირე 14 კალენდარული დღით ადრე, წერილობით აცნობებს საზედამხედველო ორგანოს შინაგანაწესში შეტანილი ნებისმიერი ცვლილების თაობაზე.

4. სანდო მომსახურების მიმწოდებელი შინაგანაწესში ცვლილებების შეტანამდე აქვეყნებს ცვლილებების პროექტს. შინაგანაწესი მტკიცდება სააგენტოში დადგენილი წესით პროექტის გამოქვეყნებიდან არაუადრეს 30-ე კალენდარულ დღეს. აღნიშნულ პერიოდში დაინტერესებულ მხარეებს საშუალება აქვთ, ცვლილებების პროექტთან დაკავშირებული შენიშვნები წერილობით მიაწოდონ სააგენტოს.

5. დამტკიცებული შინაგანაწესის პირველი ვერსია და შინაგანაწესში შეტანილი ცვლილება ქვეყნდება სააგენტოში დადგენილი წესის შესაბამისად, ხელმოწერილი ფორმით.

6. წინამდებარე დოკუმენტი, კოდიფიცირებული ფორმით (ყველა ცვლილების ასახვით) ქვეყნდება ელექტრონული ფაილის სახით, PDF ფორმატში, რომელიც მოწმდება შესაბამისი უფლებამოსილი პირის კვალიფიციური ელექტრონული ხელმოწერით ან/და სააგენტოს კვალიფიციური ელექტრონული შტამპით. ფაილის სახელი შეიცავს დოკუმენტის ვერსიის ნომერს, მინიჭებულს წინამდებარე დოკუმენტის დანაწესის შესაბამისად.

7. წინამდებარე დოკუმენტის კოდიფიცირებულ ვერსიას ამზადებს სააგენტოს საქმისწარმოებისა და სამართლებრივი უზრუნველყოფის სამსახური.

8. წინამდებარე შინაგანაწესთან დაკავშირებით კითხვებისათვის საკონტაქტო ელექტრონული ფოსტის მისამართია - online@sda.gov.ge; ტელეფონი - (+995) 32 2401010.

მუხლი 6. სანდო მომსახურების მიმწოდებლის მიერ მომსახურების მიწოდების წესი

1. სანდო მომსახურების მიმწოდებლის საკადრო შემადგენლობა განისაზღვრება სააგენტოს თავმჯდომარის ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტით. სანდო მომსახურების მიმწოდებლის მიერ მომსახურების გაწევის წესები და პირობები განსაზღვრულია საქართველოს იუსტიციის მინისტრის ბრძანებით, შესაბამისი პოლიტიკითა და წინამდებარე შინაგანაწესით.

2. მომსახურების საფასურები განსაზღვრულია „საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – სახელმწიფო სერვისების განვითარების სააგენტოს და დელეგირებული უფლებამოსილების ფარგლებში საკონსულო თანამდებობის პირის მიერ გაწეული მომსახურების ვადების, ამ მომსახურებისათვის დაწესებული საფასურების ოდენობების და საფასურის გადახდის წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 2011 წლის 29 დეკემბრის №508 დადგენილებით.

3. კვალიფიციური სანდო მომსახურების მიმწოდებლის „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონით დადგენილ მოთხოვნებთან შესაბამისობასა და დამატებით პირობებს განსაზღვრავს „კვალიფიციური სანდო მომსახურების მიმწოდებლისთვის სავალდებულო ტექნიკური რეგლამენტის დამტკიცების შესახებ“ საქართველოს მთავრობის 2018 წლის 28 ივნისის N343 დადგენილება.

4. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტით განსაზღვრული სანდო მომსახურების მიწოდებისა და სანდო მომსახურების მიწოდების პროცესში შექმნილი დოკუმენტების შენახვის ვადა განისაზღვრება სააგენტოში დამტკიცებული ნომენკლატურის შესაბამისად.

თავი II

ღია გასაღების ინფრასტრუქტურა და მასში მონაწილე მხარეები

მუხლი 7. ღია გასაღების ინფრასტრუქტურა და მასში მონაწილე მხარეები

1. წინამდებარე დოკუმენტის მიზნებისათვის ღია გასაღების ინფრასტრუქტურაში შესაძლოა მონაწილეობდნენ შემდეგი მხარეები:

   ა) სერტიფიცირების ცენტრი;

   ბ) მარეგისტრირებელი ორგანო;

   გ) პერსონალიზაციის ორგანო;

   დ) სუბიექტი;

   ე) წარმომადგენელი;

   ვ) მომხმარებელი;

   ზ) კონტრაჰენტი.

2. წინამდებარე დოკუმენტის მიზნებისათვის, კვალიფიციური ელექტრონული შტამპის სერტიფიკატების გაცემა და მომსახურება სრულად ხორციელდება ღია გასაღების ინფრასტრუქტურის გამოყენებით, სადაც:

   ა) კვალიფიციური ელექტრონული შტამპის შექმნის მონაცემები ტექნიკურად წარმოდგენილია კრიპტოგრაფიული დახურული გასაღების, შემდგომში „კვალიფიციური ელექტრონული შტამპის დახურული გასაღების“ სახით;
   ბ) კვალიფიციური ელექტრონული შტამპის შემოწმების მონაცემები ტექნიკურად წარმოდგენილია კრიპტოგრაფიული ღია გასაღების, შემდგომში „კვალიფიციური ელექტრონული შტამპის ღია გასაღების“ სახით;
   გ) კვალიფიციური ელექტრონული შტამპის ღია და დახურული გასაღებები ქმნიან კრიპტოგრაფიული გასაღების წყვილს;
   დ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატი ტექნიკურად წარმოდგენილია კრიპტოგრაფიული გასაღების სერტიფიკატის სახით.

3. წინამდებარე დოკუმენტის მიზნებისათვის, ორგანიზაციის ავთენტიფიკაციის სერტიფიკატი წარმოადგენს კრიპტოგრაფიული გასაღების სერტიფიკატს, რომელიც გაიცემა და იმართება ღია გასაღების ინფრასტრუქტურის მეშვეობით.

4. წინამდებარე დოკუმენტის მიზნებისათვის, დროის აღნიშვნასთან დაკავშირებული სერტიფიკატების გაცემა და მომსახურება სრულად ხორციელდება ღია გასაღების ინფრასტრუქტურის გამოყენებით. დროის აღმნიშვნელი ერთეულის სერტიფიკატი წარმოადგენს კრიპტოგრაფიული გასაღების სერტიფიკატს, რომელიც გაიცემა და იმართება ღია გასაღების ინფრასტრუქტურის მეშვეობით.

მუხლი 8. სერტიფიცირების ცენტრი

1. სერტიფიცირების ცენტრი წარმოადგენს სააგენტოს თავმჯდომარის ინდივიდუალური ადმინისტრაციულ-სამართლებრივი აქტით სანდო მომსახურების მიწოდების ფარგლებში შექმნილ, სააგენტოს თანამშრომელთა სპეციალურ ჯგუფს. წინამდებარე დოკუმენტის მიზნებისათვის სერტიფიცირების ცენტრი მართავს სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემებს და უზრუნველყოფს მათ გამართულ და უსაფრთხო მუშაობას.

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

   ა) **სერტიფიკატის გამცემ ძირითად ორგანოს - „GEO Root CA“**, 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“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის III თავით დადგენილი წესის შესაბამისად;**(ცვლილება 2021.06.07.N245/ს)**

გ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO Authentication CA G(n) “, რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის III თავით დადგენილი წესის შესაბამისად;“;**(ცვლილება 2021.06.07.N245/ს)**

დ) **სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „Biometric Encryption CA“** , რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA“ 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 - „SDA ESeal CA G(n)“, რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის IV თავით დადგენილი წესის შესაბამისად; **(ცვლილება 2021.06.07.N245/ს);**

ზ) სერტიფიკატის გამცემ დაქვემდებარებულ ორგანოს - „GEO Organizational Authentication CA G(n) “, რომელიც მოქმედებს სერტიფიკატის გამცემი ძირითადი „GEO Root CA“ ორგანოს მიერ გაცემული სერტიფიკატით. მისი მართვის წესები და გამოყენების სფერო განისაზღვრება ამ შინაგანაწესის V თავით დადგენილი წესის შესაბამისად. **(ცვლილება 2021.06.07.N245/ს)**

3. სერტიფიცირების ცენტრი უზრუნველყოფს ამავე მუხლის მე-2 პუნქტში მითითებული სერტიფიკატების გამცემი ძირითადი და დაქვემდებარებული ორგანოების სერტიფიკატების გამოქვეყნებას მისამართზე - https://id.ge/pki.

4. სერტიფიკატების გამცემი სატესტო ორგანოების სერტიფიკატები არ ქვეყნდება.

მუხლი 9. მარეგისტრირებელი ორგანო

1. წინამდებარე დოკუმენტის მიზნებისთვის, მარეგისტრირებელ ორგანოს შესაძლოა წარმოადგენდეს სააგენტოს სტრუქტურული ან/და ტერიტორიული ერთეული, ასევე, მოქმედი კანონმდებლობის შესაბამისად სააგენტოს მიერ დელეგირებული უფლებამოსილების ფარგლებში მოქმედი პირი.

2. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ბ“ და „გ“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში, მარეგისტრირებელ ორგანოებს წარმოადგენენ სააგენტოს ტერიტორიული სამსახურები, რომელთა ფუნქციები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის III თავის შესაბამისად.

3. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „დ“-„თ“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში, მარეგისტრირებელ ორგანოს წარმოადგენს სააგენტოს სტრუქტურული ერთეული, გარე მომხმარებლებთან ურთიერთობის სამსახური, რომლის ფუნქციები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის IV - IX თავების შესაბამისად.

4. მარეგისტრირებელი ორგანო უფლებამოსილია, ამავე მუხლის მე-2 და მე-3 პუნქტებით განსაზღვრული კომპეტენციის შესაბამისად, მიიღოს გადაწყვეტილება გადახდილი მომსაურების საფასურის უკან დაბრუნებასთან დაკავშირებით.

5. მარეგისტრირებელი ორგანო უფლებამოსილია, ამავე მუხლის მე-2 და მე-3 პუნქტებით განსაზღვრული კომპეტენციის შესაბამისად, მიიღოს გადაწყვეტილება სუბიექტის საფასურის გადახდისაგან გათავისუფლების შესახებ, თუ შეუძლებელია მასზე გაცემული სერტიფიკატის გამოყენება, რაც გამოწვეულია შესაბამისი მომსახურების გაწევისას სააგენტოს მიერ დაშვებული შეცდომით.

მუხლი 10. პერსონალიზაციის ორგანო

1. წინამდებარე დოკუმენტის მიზნებისთვის, პერსონალიზაციის ორგანოს წარმოადგენს სააგენტოს სტრუქტურული ერთეული, ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრი (სამსახური).

2. წინამდებარე დოკუმენტის მიზნებისათვის, პერსონალიზაციის ორგანო პასუხისმგებელია სუბიექტის იმ მოწყობილობების პერსონალიზაციაზე (სუბიექტზე გაპიროვნებაზე), რომელიც სუბიექტზე გაიცემა უშუალოდ სააგენტოს მიერ.

3. პერსონალიზაციის ორგანოს ფუნქციები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის III - V თავების შესაბამისად.

მუხლი 11. სუბიექტი

1. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ბ“ და „გ“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში სუბიექტს წარმოადგენს ნებისმიერი ფიზიკური პირი, რომელზეც წინამდებარე შინაგანაწესის საფუძველზე გაიცემა კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატი.
2. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „დ“ და „ე“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში სუბიექტს წარმოადგენს ნებისმიერი იურიდიული პირი, რომელიც უფლებამოსილია, გამოიყენოს კვალიფიციური ელექტრონული შტამპი ან/და ავთენტიფიკაციის სერტიფიკატი.
3. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში სუბიექტს შეიძლება წარმოადგენდეს ორი სხვადასხვა კატეგორიის ფიზიკური ან იურიდიული პირი:
    ა) ბიომეტრიული მონაცემების შემგროვებელი - იურიდიული პირი, რომელიც თავისი ფუნქციების შესრულებისას აგროვებს და დაშიფრული სახით ინახავს ბიომეტრიულ მონაცემებს, ამ დოკუმენტის საფუძველზე გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გამოყენებით;
    ბ) ბიომეტრიული მონაცემების მიმღები - საექსპერტო საქმიანობის განმახორციელებელი ფიზიკური ან იურდიული პირი, რომელსაც თავისი ფუნქციების შესრულებისას (ბიომეტრიული მონაცემების ექსპერტიზის, პირის იდენტიფიკაციის და სხვა) მიზნით ესაჭიროება გაშიფრული ბიომეტრიული მონაცემების მიღება უსაფრთხო გზით.
4. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სუბიექტებს წარმოადგენენ ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ბ“-„ზ“ ქვეპუნქტებით განსაზღვრული ორგანოები, რომლებიც ექვემდებარებიან სერტიფიკატების გამცემ ორგანოს („GEO Root CA“) და მოქმედებენ ამავე ორგანოს მიერ გაცემული სერტიფიკატების საფუძველზე.
5. სუბიექტის უფლებამოსილებები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის III - VII თავების შესაბამისად.

მუხლი 12. წარმომადგენელი

1. წინამდებარე დოკუმენტის მიზნებისათვის, წარმომადგენელი შეიძლება იყოს ნებისმიერი პირი, რომელიც, საქართველოში მოქმედი კანონმდებლობის შესაბამისად, მოქმედებს სუბიექტის ან მომხმარებლის სახელით.

2 წარმომადგენელს ეკისრება იგივე ვალდებულებები, რომლებსაც წინამდებარე დოკუმენტი უწესებს სუბიექტს ან მომხმარებელს.

მუხლი 13. მომხმარებელი

1. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „ზ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, მომხმარებელს შეიძლება წარმოადგენდეს ნებისმიერი პირი, რომელიც იყენებს დროის აღნიშვნის მომსახურებას გარკვეულ ინფორმაციაზე დროის აღნიშვნის ტოკენის მისაღებად.
2. ამ შინაგანაწესის პირველი მუხლის პირველი პუნქტის „თ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, მომხმარებელს შეიძლება წარმოადგენდეს ნებისმიერი პირი, რომელიც იყენებს აღნიშნულ მომსახურებას სერტიფიკატის ავტომატური შემოწმებისათვის.
3. მომხმარებლის უფლებამოსილებები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის VIII და IX თავების შესაბამისად.

მუხლი 14. კონტრაჰენტი

1. წინამდებარე დოკუმენტის მიზნებისთვის, კონტრაჰენტი შეიძლება იყოს პირი, რომელიც ნებისმიერი ფორმით მიიღებს წინამდებარე დოკუმენტის შესაბამისად გაცემულ სერტიფიკატებს, რომელიმე მათგანის საშუალებით ჩატარებული ოპერაციის შედეგს, ან კონკრეტული ინფორმაციის დროის კონკრეტულ მომენტში არსებობის დადასტურების ან სხვა მიზნით - დროის აღნიშვნის ტოკენს.
2. კონტრაჰენტის უფლებამოსილებები და ვალდებულებები განისაზღვრება ამ შინაგანაწესის III - X თავების შესაბამისად.

თავი III

პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე კვალიფიციური ელექტრონული ხელმოწერისა და ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატის გაცემა და მომსახურება

მუხლი 15. პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე გაცემული კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატი და სერტიფიკატის გამოყენების წესი

1. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის დანიშნულებაა ელექტრონულ დოკუმენტებზე კვალიფიციური ელექტრონული ხელმოწერის შექმნა.

2. დაუშვებელია სუბიექტზე გაცემული კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა.

3. დაუშვებელია სუბიექტზე გაცემული კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა. ასევე დაუშვებელია მისი გამოყენება სხვა სერტიფიკატების გასაცემად, მათი გაუქმების შესახებ ინფორმაციაზე ან დროის აღნიშვნის ტოკენზე ხელმოსაწერად.

4. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატი გაიცემა 2 წლისა და 6 თვის მოქმედების ვადით. არასრულწლოვანზე სერტიფიკატი გაიცემა პირის სრულწლოვანებამდე დარჩენილი, მაგრამ არაუმეტეს 2 წლისა და 6 თვის ვადით.

5. პირადობის (ბინადრობის) ელექტრონული მოწმობის გაცემასთან ერთად კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაცემის შემთხვევაში, სერტიფიკატი უნდა გაიცეს პირადობის (ბინადრობის) ელექტრონული მოწმობის გაცემისათვის გათვალისწინებულ ვადაში. განმეორებით გაცემის შემთხვევაში, სერტიფიკატი გაიცემა 2 სამუშაო დღის ვადაში.

6. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. სერტიფიკატის ავტომატური შემოწმების მომსახურებები და მათი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.

მუხლი 16. პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე გაცემული ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატი და სერტიფიკატის გამოყენების წესი

1. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატი წარმოადგენს კრიპტოგრაფიული გასაღებების სერტიფიკატს.
2. ფიზიკური პირის ავთენტიფიკაცის სერტიფიკატის დანიშნულებაა ელექტრონულ სისტემებში სუბიექტის რწმუნების მაღალი ხარისხით იდენტიფიკაცია და ავთენტიფიკაცია, მასთან უსაფრთხო კავშირის დამყარების და ინფორმაციის უსაფრთხოდ გაცვლის უზრუნველყოფის მიზნით.
3. დაუშვებელია სუბიექტზე გაცემული პესრონალური ავთენტიფიკაციის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა.

4. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატი გაიცემა 2 წლის და 6 თვის მოქმედების ვადით. არასრულწლოვანზე სერტიფიკატი გაიცემა პირის სრულწლოვანებამდე დარჩენილი, მაგრამ არაუმეტეს 2 წლისა და 6 თვის ვადით.

5. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. სერტიფიკატის ავტომატური შემოწმების მომსახურებები და მათი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.

6. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატი გაიცემა კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატთან ერთად. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატის მოთხოვნა კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატისაგან დამოუკიდებლად დაუშვებელია.

7. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატი უქმდება კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატთან ერთად. ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატის გაუქმების მოთხოვნა კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატისაგან დამოუკიდებლად დაუშვებელია.

მუხლი 17. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატში და ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატში სუბიექტის განმასხვავებელი სახელის სახელდებისა და ინტერპრეტირების წესი

1. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაცემის მიზნებისათვის სუბიექტებს განმასხვავებელი სახელი ენიჭებათ X.509v3 ფორმატით, შემდეგი წესით:

ა) C=GE;

ბ) O=Citizen (პირადობის მოწმობისათვის) ან O=Resident (ბინადრობის მოწმობისათვის);

გ) OU ველი ცარიელია პირადობის მოწმობისათვის, OU=Permanent მუდმივი ბინადრობის მოწმობისათვის, OU=Temporary დროებითი ბინადრობის მოწმობისათვის;

დ) SERIALNUMBER=პირადი ნომერი რომელიც ჩაიწერება ETSI EN 319 412 სტანდარტით განსაზღვრული წესით, შემდეგი ფორმატით: PNOGE-XXXXXXXXXXX, სადაც XXXXXXXXXXX არის 11-ციფრა პირადი ნომერი;

ე) CN=სახელი და გვარი ლათინური ასოებით.

ვ) Givenname= სახელი ლათინური ასოებით; (**ცვლილება 2021.06.07.N245/ს)**

ზ) Surname=გვარი ლათინური ასოებით“; (**ცვლილება 2021.06.07.N245/ს)**

2. სუბიექტის განმასხვავებელ სახელებში ანონიმური სუბიექტებისა და ფსევდონიმების გამოყენება დაუშვებელია.

3. სუბიექტის სახელი და გვარი კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატში შეიტანება ინგლისურ ენაზე სააგენტოს მონაცემთა ელექტრონული ბაზის საფუძველზე.

4. სუბიექტის განმასხვავებელი სახელები უნიკალურია, რასაც უზრუნველყოფს მათში პირადი ნომრის მონაწილეობა - ერთიდაიგივე განმასხვავებელი სახელი არ მიენიჭება 2 სხვადასხვა პირს.

5. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატში ინფორმაცია სუბიექტის შესახებ არ იცვლება. სუბიექტის შესახებ სერტიფიკატში დატანილი ინფორმაციის ცვლილების შემთხვევაში, სუბიექტის სახელზე გაიცემა ახალი სერტიფიკატი შეცვლილი მონაცემებით.

6. კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატის გაცემის მიზნებისათვის, სერტიფიკატის subjectAlternativeName გაფართოებაში შეიტანება სუბიექტის სახელი და გვარი ქართულ ენაზე და პირადი ნომერი პირადობის ელექტრონული მოწმობის მიხედვით. (**ცვლილება 2021.06.07.N245/ს)**

მუხლი 18. ღია გასაღების ინფრასტრუქტურაში მონაწილე მხარეთა ვალდებულებები და პასუხისმგებლობები

1. წინამდებარე თავის მიზნებისათვის, სერტიფიცირების ცენტრი პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების გამართულ და უსაფრთხო მუშაობაზე, რაც მოიცავს:

ა) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების უსაფრთხოების უზრუნველყოფას, მათ შორის, შესაბამისი დახურული გასაღებისა და აქტივაციის მონაცემების დაცვას კომპრომეტირებისგან;
ბ) სერტიფიკატის შექმნასა და გაუქმებას და წინამდებარე დოკუმენტით განსაზღვრული ფუნქციების შესაბამისად, მარეგისტრირებელი ორგანოს მოთხოვნის დაკმაყოფილებას;
გ) წინამდებარე დოკუმენტით განსაზღვრული, სერტიფიკატის ავტომატური შემოწმების მომსახურების ხელმისაწვდომობას სუბიექტებისა და კონტრაჰენტებისათვის, ამ დოკუმენტით განსაზღვრულ ფარგლებში.
2. წინამდებარე თავის მიზნებისათვის, მარეგისტრირებელი ორგანო ვალდებულია:
ა) მიიღოს განცხადება სუბიექტის კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაცემასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;
ბ) მიიღოს განცხადება სუბიექტის კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაუქმებაზე და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;
გ) შეამოწმოს განმცხადებლის უფლებამოსილება;
დ) მიიღოს გადაწყვეტილება კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატის გაცემის ან გაუქმების შესახებ;
ე) სერტიფიცირების ცენტრს მიაწოდოს სერტიფიკატის გაცემისა და გაუქმებისათვის საჭირო სრულყოფილი და უტყუარი ინფორმაცია;
ვ) წინამდებარე დოკუმენტის შესაბამისად, საჭიროების შემთხვევაში, უზრუნველყოს პირადობის (ბინადრობის) მოწმობის ან/და მისი აქტივაციის მონაცემების უსაფრთხო მიწოდება სუბიექტისთვის;
ზ) უზრუნველყოს სუბიექტის ინფორმირება კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გამოყენების, მართვისა და უსაფრთხოების დაცვის შესახებ.

3. წინამდებარე თავის მიზნებისათვის, პერსონალიზაციის ორგანო ვალდებულია, უზრუნველყოს:
ა) პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის კრიპტოგრაფიული გასაღების წყვილების (ღია და დახურული გასაღებების) შექმნა და სერტიფიცირების ცენტრისათვის მიწოდება;
ბ) პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე იმ აქტივაციის მონაცემების მინიჭება, რომლებიც სუბიექტზე გაიცემა სერტიფიკატზე განაცხადის მიღებისას;
გ) პირადობის (ბინადრობის) ელექტრონულ მოწმობის უსაფრთხო მიწოდება წინამდებარე დოკუმენტით განსაზღვრული წესით (საფოსტო გზავნილის მეშვეობით);
დ) პირადობის (ბინადრობის) ელექტრონულ მოწმობის ვიზუალური პერსონალიზაცია.

4. წინამდებარე თავის მიზნებისათვის, სუბიექტი ან/და მისი წარმომადგენელი ვალდებულია:

ა) წარმოადგინოს პოლიტიკით ან/და შინაგანაწესით მოთხოვნილი სწორი და სრულყოფილი ინფორმაცია კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების მისაღებად, ასევე დროულად განაახლოს აღნიშნული ინფორმაცია, მისი ცვლილების შემთხვევაში;
ბ) ავთენტიფიკაციისა და კვალიფიციური ელექტრონული ხელმოწერის გასაღების წყვილები/სერტიფიკატები გამოიყენოს მხოლოდ წინამდებარე დოკუმენტით მითითებული დანიშნულებით;
გ) გაეცნოს მიღებულ კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატში მითითებულ ინფორმაციას და დროულად აცნობოს სანდო მომსახურების მიმწოდებელს გამოვლენილი უზუსტობების შესახებ;
დ) გაუფრთხილდეს საკუთარ დახურულ გასაღებს და არ დაუშვას მისი გამოყენება არაუფლებამოსილი პირების მიერ;
ე) არ ეცადოს საკუთარი დახურული გასაღების მოწყობილობიდან ამოღებას და მის მიღმა გამოყენებას ნებისმიერი დანიშნულებით;
ვ) დახურული გასაღების კომპრომიტირების შემთხვევაში, დაუყოვნებლივ დაუკავშირდეს სანდო მომსახურების მიმწოდებელს - წინამდებარე შინაგანაწესის 29-ე მუხლით განსაზღვრული წესით. აღნიშნული ასევე შეეხება აქტივაციის მონაცემების (მაგ., PIN კოდების) მოხვედრას არაუფლებამოსილი პირების ხელში;
ზ) არ გამოიყენოს კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატები და შესაბამისი დახურული გასაღებები სერტიფიკატების მოქმედების ვადის ამოწურვის, სერტიფიკატის გაუქმების ან/და სანდო მომსახურების მიმწოდებელისაგან კომპრომეტაციის თაობაზე ინფორმაციის მიღების შემთხვევაში.

5. ამ მუხლის მე-4 პუნქტის ,,ბ“ და ,,დ“ ქვეპუნქტების მოთხოვნების შესასრულებლად სუბიექტმა უნდა დაიცვას შემდეგი მოთხოვნები:

ა) თუ სუბიექტი მუშაობის პროცესში არ იყენებს თავის პერსონალურ კომპიუტერს ან/და სხვა მოწყობილობას (გარდა თავად პირადობის (ბინადრობის) ელექტრონულ მოწმობისა), იგი ვალდებულია, შეაფასოს მოქმედების მიზანშეწონილობა. შეფასებისას, სულ მცირე, ყურადღება უნდა მიექცეს იმ გარემოებას, იკრიფება თუ არა აქტივაციის მონაცემები (PIN კოდი) კომპიუტერის კლავიატურაზე, ნაცვლად სპეციალური, უსაფრთხო მოწყობილობისა;
ბ) საჯარო ადგილებში ან/და კონტრაჰენტის მიერ კონტროლირებად გარემოში აქტივაციის მონაცემები (PIN კოდი) უნდა აიკრიფოს ისეთი მოწყობილობის მეშვეობით, რომელიც უზრუნველყოფს კოდის საიდუმლოდ გადაცემას პირადობის (ბინადრობის) ელექტრონული მოწმობისათვის;
გ) კვალიფიციური ელექტრონული ხელმოწერის დასმის პროცესში გამოყენებულმა აპარატურულმა და/ან პროგრამულმა უზრუნველყოფამ კონტრაჰენტს არ უნდა შეუზღუდოს ხელმოწერის დასმამდე დოკუმენტის სრულად გაცნობის შესაძლებლობა.

მუხლი 19. პირადობის (ბინადრობის) ელექტრონული მოწმობისა და კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატის გაცემაზე განაცხადის წარდგენა და გადაწყვეტილების მიღება

1. განაცხადი, პირადობის (ბინადრობის) ელექტრონული მოწმობისა და კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების გაცემის მიზნით, წარედგინება მარეგისტრირებელ ორგანოს - სააგენტოს ტერიტორიულ სამსახურს.
2. განცხადების მიღების შემდეგ მარეგისტრირებელი ორგანო განიხილავს მას და იღებს გადაწყვეტილებას კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაცემის ან გაცემაზე უარის თქმის თაობაზე.
3. შესაბამისი გადაწყვეტილების მიღების პროცესში მარეგისტრირებელი ორგანო უზრუნველყოფს სუბიექტის იდენტიფიკაციასა და ავთენტიფიკაციას, რაც გულისხმობს მისი პიროვნების დადგენას პირადობის დამადასტურებელი მონაცემების შემოწმების საფუძველზე.
4. სუბიექტის პერსონალური მონაცემებისა და უფლებამოსილების შემოწმება შესაძლებელია როგორც დოკუმენტის წარმოდგენის, ისე სააგენტოს მონაცემთა ელექტრონულ ბაზაში პიროვნების პერსონალური მონაცემების შემოწმების გზით.
5. სუბიექტის სახელზე კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაცემის გადაწყვეტილების მიღების შემდგომ სერტიფიკატები გაიცემა ამ შინაგანაწესის 24-ე მუხლით დადგენილი წესის შესაბამისად.

მუხლი 20. კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატის განმეორებით გაცემაზე განაცხადის წარდგენა და გადაწყვეტილების მიღება

1. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატის განმეორებით გაცემის მოთხოვნა 14 წლის ასაკს მიღწეულმა სუბიექტმა შესაძლებელია წარადგინოს ტერიტორიულ სამსახურში.
2. სუბიექტს უფლება აქვს, ტერიტორიულ სამსახურში წარადგინოს კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატებთან ერთად პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების განმეორებით გაცემის მოთხოვნა.
3. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების განმეორებით გაცემის თაობაზე სააგენტოში წარდგენილ განცხადებას უნდა დაერთოს პირადობის (ბინადრობის) ელექტრონული მოწმობა, რომელზეც სერტიფიკატი განმეორებით გაიცემა.
4. განცხადების მიღების შემდეგ მარეგისტრირებელი ორგანო განიხილავს მას და იღებს გადაწყვეტილებას კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაცემის ან გაცემაზე უარის თქმის თაობაზე.
5. ამ მუხლის პირველი და მე-2 პუნქტების შესაბამისად წარდგენილ განცხადებაზე შესაბამისი გადაწყვეტილების მიღების პროცესში მარეგისტრირებელი ორგანო უზრუნველყოფს სუბიექტის იდენტიფიკაციასა და ავთენტიფიკაციას, რაც გულისხმობს მისი პიროვნების დადგენას პირადობის დამადასტურებელი მონაცემების შემოწმების საფუძველზე.
6. სუბიექტის პერსონალური მონაცემებისა და უფლებამოსილების შემოწმება შესაძლებელია წარმოდგენილი დოკუმენტის და სააგენტოს მონაცემთა ელექტრონულ ბაზაში პიროვნების პერსონალური გადამოწმების გზით.
7. პირს კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატები განმეორებით გადაეცემა გასააქტიურებელ მდგომარეობაში. ორივე სერტიფიკატი გააქტიურდება საფასურის გადახდისთანავე.
8. ამ მუხლის მე-2 პუნქტით გათვალისწინებული მომსახურების გაწევისას პირს დალუქული კონვერტით გადაეცემა აქტივაციის მონაცემები.
9. ამ მუხლის მე-8 პუნქტით გათვალისწინებული კონვერტის გადაცემის შემდეგ კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატის გაცემისთვის მოთხოვნის წარმდგენმა პირმა უნდა შექმნას კვალიფიციური ელექტრონული ხელმოწერის კოდი (PIN3) და გაიაროს ავტორიზაცია პერსონალური ავთენტიფიკაციის კოდით (PIN1).
10. მარეგისტრირებელი ორგანოს უფლებამოსილი თანამშრომლის მოთხოვნის შემდეგ სუბიექტი თავის მოწყობილობას მიუერთებს შესაბამისი პროგრამული და აპარატურული უზრუნველყოფით აღჭურვილ კომპიუტერს და შეიყვანს აქტივაციის მონაცემებს. ამის შემდეგ პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე განახლდება გასაღების წყვილი, სერტიფიკატის მოთხოვნა გაეგზავნება სერტიფიკატის გამცემ ორგანოს და პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე დაიტანება ახალი სერტიფიკატი. აუცილებელია, რომ კომპიუტერი აღჭურვილი იყოს აქტივაციის მონაცემების უსაფრთხო შეყვანის მოწყობილობით (ბარათის წამკითხველი PIN კოდის უსაფრთხო შეყვანის ფუნქციით და სხვა).
11. ამ მუხლის მე-8 პუნქტით გათვალისწინებულ აქტივაციის მონაცემებთან ერთად განმცხადებელს გადაეცემა/ეგზავნება წერილობითი ინფორმაცია პირადობის (ბინადრობის) ელექტრონული მოწმობის გამოყენებისა და შენახვის, ასევე, კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის საფუძველზე შექმნილი კვალიფიციური ელექტრონული ხელმოწერის გამოყენების წესების თაობაზე, მათ შორის, იმის თაობაზე, რომ მან კვალიფიციური ელექტრონული ხელმოწერის განსახორციელებლად უნდა გააქტიუროს კვალიფიციური ელექტრონული ხელმოწერის კოდი (PIN3).
12. ამ მუხლით გათვალისწინებული, სააგენტოს უფლებამოსილ ტერიტორიულ სამსახურში წარდგენილი განცხადების ფორმა მოცემულია #1 დანართით.

მუხლი 21. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების განმეორებით დისტანციურად გაცემის თაობაზე განცხადების დამუშავება და გადაწყვეტილების მიღება

1. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების განმეორებით გაცემის მოთხოვნა 14 წლის ასაკს მიღწეულმა სუბიექტმა შესაძლებელია წარადგინოს ტერიტორიულ სამსახურში მიუსვლელად სააგენტოს ვებგვერდიდან - www.id.ge ჩამოტვირთული შესაბამისი პროგრამული უზრუნველყოფის მეშვეობით, თუ პირს პერსონალური ავთენტიფიკაციის კოდის გამოყენებით (PIN1) შეუძლია გაიაროს იდენტიფიკაცია და გააქტიურებული აქვს კვალიფიციური ელექტრონული ხელმოწერის კოდი (PIN3).
2. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატებთან ერთად პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების განმეორებით გაცემის მოთხოვნის დისტანციურად წარდგენა დაუშვებელია.
3. დისტანციურად გაცემის თაობაზე განცხადების წარდგენა შეუძლებელია, თუ პირადობის (ბინადრობის) მოწმობა უვარგისია, რაც გულისხმობს ერთ-ერთი შემდეგი პირობის დაკმაყოფილებას:
   ა) დოკუმენტი გაუქმებულია ან შეჩერებულია;
   ბ) შეუძლებელია პირადობის (ბინადრობის) ელექტრონულ მოწმობასა და განახლებისათვის საჭირო პროგრამულ ან/და აპარატურულ უზრუნველყოფას შორის კავშირის დამყარება.

4. გასაღებების წყვილის განახლების შემდეგ ღია გასაღები მოთავსდება ელექტრონულ განაცხადში და ინტერნეტის საშუალებით ავტომატურად გადაეცემა შესაბამის სერტიფიკატის გამცემ ორგანოს.
5. მარეგისტრირებელი ორგანოს მიერ ავტომატურად მოწმდება განაცხადში უსაფრთხოების მექანიზმების და პირადობის (ბინადრობის) ელექტრონული მოწმობის სტატუსი და სერტიფიკატის მოთხოვნა ეგზავნება სერტიფიკატების გამცემ შესაბამის ორგანოს.
6. სუბიექტის სახელზე კვალიფიციური ელექტრონული ხელმწერის და ავთენტიფიკაციის სერტიფიკატების გაცემის გადაწყვეტილების მიღების შემდგომ სერტიფიკატი გაიცემა ამ შინაგანაწესის 24-ე მუხლით დადგენილი წესის შესაბამისად.
7. სერტიფიკატების გამცემი ორგანოს მიერ გაცემული სერტიფიკატი ელექტრონულად უბრუნდება მომთხოვნს და ავტომატურად დაიტანება პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე.

მუხლი 22. გასაღების წყვილის განახლება

1. პირადობის (ბინადრობის) ელექტრონული მოწმობის შეცვლის გარეშე გასაღების წყვილის განახლება შესაძლებელია მხოლოდ იმ შემთხვევაში, როდესაც მოწმობა ვარგისია. ამ შემთხვევაში გასაღების წყვილი შეიძლება განახლდეს როგორც სერტიფიკატის ვადის გასვლამდე, ისე მის შემდეგ.
2. გასაღების წყვილის განახლების მოთხოვნის უფლება აქვს, ამ თავის შესაბამისად, სერტიფიკატის მოთხოვნაზე უფლებამოსილ ნებისმიერ პირს.
3. გასაღების წყვილის განახლების შემდეგ სერტიფიკატი განმეორებით გაიცემა წინამდებარე დოკუმენტით განსაზღვრული წესით.
4. თუ სერტიფიკატი გაიცემა სუბიექტზე გაცემული წინა სერტიფიკატისგან განსხვავებული წესებით და პირობებით, მომხმარებელი ამ ინფორმაციას მიიღებს ახალი სერტიფიკატის შექმნამდე.

მუხლი 23. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის განმეორებით გაცემის საფასური

1. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის განმეორებით გაცემის საფასური განისაზღვრება ,,საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – სახელმწიფო სერვისების განვითარების სააგენტოს და დელეგირებული უფლებამოსილების ფარგლებში საკონსულო თანამდებობის პირის მიერ გაწეული მომსახურების ვადების, ამ მომსახურებისათვის დაწესებული საფასურების ოდენობების და საფასურის გადახდის წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 2011 წლის 29 დეკემბრის N508 დადგენილებით.
2. სააგენტოს უფლებამოსილ ტერიტორიულ სამსახურში განცხადების წარდგენის შემთხვევაში, კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების განმეორებით გაცემისას კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატის გასააქტიურებლად საფასური გადაიხდება სერტიფიკატის გაცემიდან 10 კალენდარული დღის ვადაში.
3. სააგენტოს ვებგვერდიდან ჩამოტვირთული შესაბამისი პროგრამული უზრუნველყოფის მეშვეობით განცხადების წარდგენისას, საფასური გადაიხდება სერტიფიკატის გაცემამდე. პირს გადაეცემა გააქტიურებული სერტიფიკატი.

მუხლი 24. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაცემა

1. მარეგისტრირებელი ორგანოს მიერ სუბიექტის სახელზე სერტიფიკატის გაცემის შესახებ გადაწყვეტილება აღსასრულებლად ეგზავნება:

ა) ამ შინაგანაწესის მე-19 მუხლით გათვალისწინებული მომსახურების მოთხოვნის შემთხვევაში, პერსონალიზაციის ორგანოს;

ბ) ამ შინაგანაწესის მე-20 და 21-ე მუხლებით გათვალისწინებული მომსახურების მოთხოვნის შემთხვევაში, სერტიფიცირების ცენტრს.

2. ამ მუხლის პირველი პუნქტის ,,ა“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე პერსონალიზაციის ორგანო უზრუნველყოფს:

ა) პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე კვალიფიციური ელექტრონული ხელმოწერის ღია და დახურული გასაღების წყვილების უსაფრთხო შექმნას;(**ცვლილება 2021.06.07.N245/ს)**

ბ) სუბიექტის სერტიფიკატის შექმნაზე მოთხოვნის ავტომატურ გადაცემას სერტიფიცირების ცენტრისთვის;

გ) პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე სერტიფიცირების ცენტრის მიერ გაცემული სერტიფიკატის დატანას;

დ) პირადობის (ბინადრობის) ელექტრონულ მოწმობისა და მისი აქტივაციის მონაცემების გადაცემას მიწოდებაზე პასუხისმგებელი მხარისათვის.

მუხლი 25. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის შექმნა

1. სერტიფიცირების ცენტრის პროგრამული უზრუნველყოფა ავტომატურად ამოწმებს, შეიქმნა თუ არა კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის ღია და დახურული გასაღების წყვილები უშუალოდ პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე და ხომ არ მომხდარა ღია გასაღებების ჩანაცვლება სერტიფიცირების ცენტრისთვის გადაცემამდე.

2. შემოწმების შედეგების შესაბამისად, სერტიფიკატის გამცემი ორგანოს საშუალებით იქმნება კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატი. სერტიფიკატის შესაქმნელად გამოიყენება ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტით განსაზღვრული „GEO Signing CA G(n)“ სერტიფიკატის გამცემი ორგანო, ხოლო ავთენტიფიკაციის სერტიფიკატის შესაქმნელად გამოიყენება ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტით განსაზღვრული „GEO Authentication CA G(n)“ სერტიფიკატის გამცემი ორგანო. (**ცვლილება 2021.06.07.N245/ს)**

3. შინაგანაწესის 24-ე მუხლის მე-2 პუნქტით გათვალისწინებული მომსახურების ფარგლებში,სერტიფიცირების ცენტრის მიერ შექმნილი სერტიფიკატი ეგზავნება პერსონალიზაციის ორგანოს.

4. პერსონალიზაციის ორგანო ამოწმებს სერტიფიცირების ცენტრიდან მიღებულ მონაცემებს და უზრუნველყოფს სერტიფიკატის დატანას პირადობის (ბინადრობის) ელექტრონულ მოწმობაზე. პერსონალიზებული მოწმობა გადაეცემა მიწოდებაზე პასუხისმგებელ მხარეს - მარეგისტრირებელ ორგანოს ან საფოსტო მომსახურების განმახორციელებელ პირს (თუ მოწყობილობა იგზავნება ფოსტით). მიწოდებაზე პასუხისმგებელ მხარეს, ასევე, გადაეცემა აქტივაციის მონაცემების შემცველი დალუქული კონვერტი. სრული პროცესი მიმდინარეობს სააგენტოში დამტკიცებული „პირადობის/ბინადრობის ელექტრონული მოწმობის წარმოების სახელმძღვანელოს“ მიერ დადგენილი პროცედურების შესაბამისად.

მუხლი 26. პირადობის (ბინადრობის) ელექტრონული მოწმობისა და მისი აქტივაციის მონაცემების მიწოდება

1. მარეგისტრირებელი ორგანო სუბიექტს გადასცემს პირადობის (ბინადრობის) ელექტრონულ მოწმობას და მისი აქტივაციის მონაცემებს. აღნიშნული პროცედურა წარიმართება „საქართველოს მოქალაქეთა და საქართველოში მცხოვრებ უცხოელთა რეგისტრაციისა და რეგისტრაციიდან მოხსნის, პირადობის (ბინადრობის) ელექტრონული მოწმობის, პასპორტის, სამგზავრო პასპორტისა და სამგზავრო დოკუმენტის გაცემის წესის დამტკიცების შესახებ“ საქართველოს იუსტიციის მინისტრის 2011 წლის 27 ივლისის N98 ბრძანებით დამტკიცებული წესის შესაბამისად.

2. მოწყობილობა 14 წლამდე არასრულწლოვანი ფიზიკური პირის შემთხვევაში მის ნაცვლად გადაეცემა სუბიექტის კანონიერ წარმომადგენელს, ხოლო 14 წლიდან 18 წლამდე ასაკი სფიზიკურ პირს - პირადად ან მის კანონიერ წარმომადგენელს.

3. საფოსტო მომსახურების განმახორციელებელი პირი სუბიექტს გზავნილს გადასცემს/მიაწვდის სააგენტოსთან დადებული მომსახურების ხელშეკრულების საფუძველზე.

4. სერტიფიკატების განმეორებით გაცემის შემთხვევაში, მისი აქტივაციის მონაცემები გადაეცემა სუბიექტს პირადად, 14 წლის ასაკიდან.

მუხლი 27. სერტიფიკატის გადაცემის დასტური

1. პირადობის (ბინადრობის) ელექტრონული მოწმობისა და მისი აქტივაციის მონაცემების მიღების ფაქტი (გარდა ფოსტის მეშვეობით გადაცემის შემთხვევისა) უნდა დადასტურდეს მოწმობის გაცემის თაობაზე განცხადება-ანკეტაზე ხელმოწერით.
2. მარეგისტრირებელ ორგანოში გამოცხადებისას კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატებთან ერთად პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების განმეორებით გაცემის შემთხვევაში აქტივაციის მონაცემების გადაცემის ფაქტთან დაკავშირებით დგება შესაბამისი მიღება-ჩაბარების აქტი.

მუხლი 28. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაუქმება

1. სანდო მომსახურების მიმწოდებელი სერტიფიკატს აუქმებს შემდეგ შემთხვევებში:

ა) გაუქმდა პირადობის (ბინადრობის) ელექტრონული მოწმობა;

ბ) პირადობის (ბინადრობის) ელექტრონული მოწმობის მოქმედება შეჩერდა;

გ) სერტიფიკატის გაუქმების თაობაზე განაცხადი წარადგინა პირადობის (ბინადრობის) ელექტრონული მოწმობის მფლობელმა პირმა;

დ) კანონმდებლობით დადგენილ ვადაში სუბიექტმა არ გადაიხადა კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გააქტიურებისთვის დადგენილი საფასური.

ე) არსებობს დასაბუთებული ვარაუდი კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების კომპრომიტირების შესახებ;

ვ) არსებობს დასაბუთებული ვარაუდი პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების კომპრომიტირების შესახებ.

2. კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების გაუქმება ავტომატურად არ იწვევს პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების გაუქმებას, გარდა ამ მუხლის პირველი პუნქტის „ვ“ ქვეპუნქტით გათვალისწინებული შემთხვევისა.

3. გაუქმებული კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების, პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების აღდგენა დაუშვებელია.

4. პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის იმავე კოდების ხელმეორედ გადაცემა დაუშვებელია.

5. ამ მუხლის პირველი პუნქტის ,,ა“, ,,ბ“ ,,დ“, ,,ე“ და ,,ვ“ ქვეპუნქტებით განსაზღვრულ შემთხვევებში სერტიფიკატი შესაძლოა გაუქმდეს სანდო მომსახურების მიმწოდებლის მიერ.

მუხლი 29. განაცხადი კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაუქმების თაობაზე

1. კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაუქმების მოთხოვნა შეუძლია სუბიექტს ან საქართველოს კანონმდებლობით დადგენილ შესაბამის უფლებამოსილ პირს.

2. შესაბამისი უფლებამოსილი პირი, კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გაუქმების მოთხოვნით მიმართავს მარეგისტრირებელ ორგანოს.

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.

მუხლი 30. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაუქმების შესახებ განცხადების დამუშავება და გადაწყვეტილების მიღება

1. შინაგანაწესის 28-ე მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში შესაბამისი განცხადების მიღების შემდეგ მარეგისტრირებელი ორგანო ან დისტანციური მომსახურების სამსახური ამოწმებს სუბიექტის ვინაობას და უფლებამოსილებას საქართველოს კანონმდებლობით დადგენილი წესით.
2. მარეგისტრირებელი ორგანო ან დისტანციური მომსახურების სამსახური განიხილავს მომართვას და იღებს გადაწყვეტილებას სერტიფიკატების გაუქმების ან გაუქმებაზე უარის თქმის თაობაზე.

მუხლი 31. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების გაუქმება

1. ამ შინაგანაწესის 29-ე მუხლის მე-2 პუნქტის შესაბამისად მიღებული განაცხადის საფუძველზე სერტიფიკატის გაუქმების გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს მარეგისტრირებელი ორგანო.

2. ამ შინაგანაწესის 29-ე მუხლის მე-3 პუნქტის შესაბამისად მიღებული მომართვის საფუძველზე სერტიფიკატის გაუქმების გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს დისტანციური მომსახურების სამსახური;

2[1]. კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის შესახებ გადაწყვეტილება გამოიცემა სუბიექტის მიერ სერტიფიკატის გაუქმების მოთხოვნის სააგენტოში წარდგენიდან არაუგვიანეს მომდევნო სამუშაო დღისა.(**ცვლილება 2021.06.07.N245/ს**)

2[2]. კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატი უქმდება ამ მუხლის მე-3 პუნქტით გათვალისწინებული გადაწყვეტილების მიღების დღეს.(**ცვლილება 2021.06.07.N245/ს**)

3. სერტიფიკატის გაუქმების შესახებ ინფორმაცია აღირიცხება ელექტრონულ ჟურნალში, რომელიც ინახება 10 წლის ვადით.

მუხლი 32. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატების შეჩერება

კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის მოქმედების შეჩერება დაუშვებელია.

მუხლი 33. კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის ღია და დახურული გასაღებების წყვილის გენერაცია და მართვა

1. სუბიექტის კვალიფიციური ელექტრონული ხელმოწერის გასაღების წყვილი იქმნება უშუალოდ პირადობის (ბინადრობის) ელექტრონული მოწმობის შიგნით.

2. გასაღების პარამეტრებია:

ა) კრიპტოგრაფიული ალგორითმი - RSA;

ბ) გასაღების სიგრძე - 2048 ბიტი.

3. მოწმობაზე ღია გასაღები სერტიფიკატის გამცემ ორგანოს გადაეცემა უსაფრთხო წესით, რაც ითვალისწინებს ინფორმაციის ავთენტურობისა და მთლიანობის დადასტურებას. მიმღები მხარე შესაბამისი მექანიზმებით ამოწმებს, მოხდა თუ არა გასაღების გენერაცია უშუალოდ მოწყობილობაზე. გასაღების წყვილის დისტანციური განახლებისას ინტერნეტკავშირი დამატებით დაცულია SSL/TLS საშუალებებით.

4. სუბიექტის დახურული გასაღების მესამე პირისთვის მიბარება და სარეზერვო ასლის შექმნა დაუშვებელია. გასაღებების წყვილი იქმნება პირადობის (ბინადრობის) ელექტრონული მოწმობაზე, ელექტრონული მატარებლიდან რამე (მათ შორის, დაშიფრული) სახით ამოკითხვის შესაძლებლობის გარეშე.

5. პირადობის (ბინადრობის) ელექტრონულ მოწმობას აქვს კვალიფიციური ხელმოწერის შექმნის მოწყობილობის სტატუსი, საქართველოს კანონმდებლობის შესაბამისად.

მუხლი 34. პირადობის (ბინადრობის) ელექტრონულ მოწმობაში არსებული სერტიფიკატის აქტივაციის მონაცემები

1. აქტივაციის მონაცემები, რომლებიც პირადობის (ბინადრობის) ელექტრონულ მოწმობასთან ერთად გაიცემა სუბიექტზე, წარმოადგენს 3 (სამ) საიდუმლო კოდს, დაბეჭდილს და დალუქულს სპეციალურ კონვერტში. ამ კოდების დანიშნულება შემდეგია:

ა) PIN 1 კოდი (4 ციფრი) - გამოიყენება პირადობის (ბინადრობის) ელექტრონულ მოწმობის მფლობელის ავთენტიფიკაციისთვის, მათ შორის გასაღების წყვილის განახლების მოთხოვნისათვის და სანდო მომსახურების მიმწოდებლისაგან მიღებული სერტიფიკატის ჩასაწერად მოწმობაზე;

ბ) PIN 2 კოდი (5 ციფრი) - გამოიყენება იმისათვის, რომ სპეციალური პროგრამული უზრუნველყოფით შეიქმნას PIN 3 კოდი’

გ) PUK კოდი (8 ციფრი) - გამოიყენება დაბლოკილი PIN კოდების განბლოკვისათვის, ასევე დავიწყებული PIN 1 კოდის აღსადგენად. PUK კოდის გამოყენება მხოლოდ 10-ჯერ არის შესაძლებელი, ამის შემდეგ ის იბლოკება.

2. აქტივაციის მონაცემები, რომლებიც ამ წესის მე-20 მუხლის მე-2 პუნქტით გათვალისწინებული მოთხოვნის წარდგენისას გადაეცემა პირს, წარმოადგენს 3 (სამ) საიდუმლო კოდს, დაბეჭდილს და დალუქულს სპეციალურ კონვერტში.
ა) განმეორებით შექმნილი პერსონალური ავთენტიფიკაციის კოდი (PIN1) - 6 სიმბოლო;
ბ) განმეორებით შექმნილი კვალიფიციური ელექტრონული ხელმოწერის აქტივაციის კოდი (PIN2) - 8 სიმბოლო;
გ) განმეორებით შექმნილი განბლოკვის კოდი (PUK) – 8 სიმბოლო.

3. სუბიექტს მხოლოდ PIN 3 კოდის (6 ციფრი) შექმნის შემდეგ შეუძლია განახორციელოს კვალიფიციური ელექტრონული ხელმოწერა პირადობის (ბინადრობის) ელექტრონული მოწმობის საშუალებით.

4. ყველა კოდი იბლოკება ზედიზედ სამი არასწორი ცდის შემდეგ.

თავი IV

კვალიფიციური ელექტრონული შტამპის სერტიფიკატების გაცემა და მომსახურება

მუხლი 35. კვალიფიციური ელექტრონული შტამპის სერტიფიკატი და სერტიფიკატის გამოყენების წესი

1. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის დანიშნულებაა ელექტრონულ დოკუმენტებზე კვალიფიციური ელექტრონული შტამპის შექმნა.
2. კვალიფიციური ელექტრონული შტამპის სერტიფიკატი გაიცემა მხოლოდ სუბიექტის სახელზე. სერტიფიკატი არ გაიცემა სუბიექტის სტრუქტურული ერთეულის სახელზე.
3. დაუშვებელია სუბიექტზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა. ასევე დაუშვებელია მისი გამოყენება სხვა სერტიფიკატების გასაცემად, მათი გაუქმების შესახებ ინფორმაციაზე ან დროის აღნიშვნის ტოკენზე ხელმოსაწერად.
4. კვალიფიციური ელექტრონული შტამპის სერტიფიკატი შესაძლებელია გაიცეს:
   ა) სუბიექტის მიერ წარმოდგენილ სუბიექტის მოწყობილობაზე;
   ბ) სუბიექტის ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე;
   გ) სააგენტოს მიერ გაცემულ სუბიექტის მოწყობილობაზე;
   დ) სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე.
5. კვალიფიციური ელექტრონული შტამპის სერტიფიკატი გაიცემა 2 წლისა და 6 თვის მოქმედების ვადით.
6. თითოეულ კვალიფიციური ელექტრონული შტამპის სერტიფიკატში შეიტანება ,,კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკის“ უნიკალური იდენტიფიკატორი, რომელიც უზრუნველყოფს სერტიფიკატის გაცემის დროისთვის წინამდებარე დოკუმენტის მოქმედი რედაქციის იდენტიფიცირების შესაძლებლობას.
7. სუბიექტის მოწყობილობას აქვს კვალიფიციური ელექტრონული შტამპის შექმნის მოწყობილობის სტატუსი, საქართველოს კანონმდებლობის შესაბამისად.
8. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. სერტიფიკატის ავტომატური შემოწმების მომსახურებები და მათი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.
9. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის პროფილი განისაზღვრება ამ შინაგანაწესის N2 დანართის შესაბამისად.

მუხლი 36. კვალიფიციური ელექტრონული შტამპის სერტიფიკატში სუბიექტის განმასხვავებელი სახელის სახელდებისა და ინტერპრეტირების წესი

1. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის მიზნებისათვის სუბიექტებს განმასხვავებელი სახელი ენიჭებათ X.509v3 ფორმატით, შემდეგი წესით:
   ა) C=GE (ქვეყნის კოდი);
   ბ) O=სუბიექტის დასახელება;
   გ) CN=სუბიექტის დასახელება (იგივე, რაც O ველი);
   დ) organizationIdentifier=სუბიექტის საიდენტიფიკაციო კოდი.
2. სუბიექტის განმასხვავებელ სახელებში ანონიმური სუბიექტებისა და ფსევდონიმების გამოყენება დაუშვებელია. ამასთან, არ მოწმდება განმასხვავებელი სახელის სუბიექტის რეგისტრირებულ სავაჭრო ნიშანთან თანხვედრა.

3. სუბიექტის საიდენტიფიკაციო კოდის ველის მნიშვნელობა განისაზღვრება „ETSI EN 319 412“ წესით და აქვს შემდეგი ფორმატი: NTRGE-XXXXXXXXX, სადაც XXXXXXXXX არის აღნიშნული ორგანიზაციის უნიკალური საიდენტიფიკაციო კოდი, რომლის მეშვეობითაც მიიღწევა სუბიექტის განმასხვავებელი სახელის უნიკალურობა.

4. სუბიექტის დასახელება კვალიფიციური ელექტრონული შტამპის სერტიფიკატის განმასხვავებელ სახელში შეიტანება ინგლისურ ენაზე.

5. სუბიექტის სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემისათვის სუბიექტის დასახელება და საიდენტიფიკაციო კოდი განისაზღვრება სსიპ - საჯარო რეესტრის ეროვნულ სააგენტოში არსებული ინფორმაციის მიხედვით, ხოლო ასეთის არარსებობის შემთხვევაში, სსიპ - შემოსავლების სამსახურის გადამხდელთა რეესტრის მიხედვით.

6. ამ მუხლის მე-5 პუნქტის შესაბამისად განსაზღვრულ რეესტრებში სუბიექტის ინგლისური დასახელების არარსებობის შემთხვევაში, სუბიექტს ინგლისური დასახელება ენიჭება ამ შინაგანაწესის 38-ე მუხლის შესაბამისად, სუბიექტის განცხადებაში მითითებული ინგლისური დასახელების შესაბამისად.

7. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის მიზნებისათვის, სერტიფიკატის subjectAlternativeName გაფართოებაში შეიტანება სუბიექტის დასახელება ქართულ ენაზე. სუბიექტის სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემისათვის სუბიექტის ქართულ ენაზე დასახელება განისაზღვრება სსიპ - საჯარო რეესტრის ეროვნულ სააგენტოში არსებული ინფორმაციის მიხედვით, ხოლო ასეთის არარსებობის შემთხვევაში, სსიპ - შემოსავლების სამსახურის გადამხდელთა რეესტრის მიხედვით.**(ცვლილება 2021.06.07.N245/ს)**

8. კვალიფიციური ელექტრონული შტამპის სერტიფიკატში სუბიექტის ინფორმაციის ცვლილება დაუშვებელია. სერტიფიკატში ასახული სუბიექტის შესახებ ინფორმაციის ცვლილების შემთხვევაში, სუბიექტის სახელზე გაიცემა ახალი სერტიფიკატი შეცვლილი მონაცემებით.

9. სერტიფიკატში ასახული სუბიექტის განმასხვავებელი სახელის ცვლილების დროს, იმ შემთხვევაში, თუ აღნიშნული სახელის რომელიმე კომპონენტი ვიზუალურად დატანილია სააგენტოს მიერ გაცემულ სუბიექტის მოწყობილობაზე, ახალი სერტიფიკატის გაცემის დროს აუცილებელია მოწყობილობის შეცვლა.

მუხლი 37. ღია გასაღების ინფრასტრუქტურაში მონაწილე მხარეთა ვალდებულებები და პასუხისმგებლობები

1. წინამდებარე თავის მიზნებისათვის, სერტიფიცირების ცენტრი პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების გამართულ და უსაფრთხო მუშაობაზე, რაც მოიცავს:

   ა) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების უსაფრთხოების უზრუნველყოფას, მათ შორის, შესაბამისი დახურული გასაღებისა და აქტივაციის მონაცემების დაცვას კომპრომეტირებისგან;
   ბ) სერტიფიკატის შექმნას, გაუქმებასა და წინამდებარე დოკუმენტით განსაზღვრული ფუნქციების შესაბამისად მარეგისტრირებელი ორგანოს მოთხოვნის დაკმაყოფილებას;
   გ) სუბიექტებისა და კონტრაჰენტებისათვის წინამდებარე დოკუმენტით განსაზღვრული, სერტიფიკატის ავტომატური შემოწმების მომსახურების ხელმისაწვდომობას.

2. წინამდებარე თავის მიზნებისათვის, მარეგისტრირებელი ორგანო ვალდებულია:

   ა) მიიღოს განცხადება სუბიექტის კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია, ავთენტიფიკაცია;
   ბ) მიიღოს განცხადება სუბიექტის კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმებაზე და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;
   გ) შეამოწმოს განმცხადებლის უფლებამოსილება;
   დ) მიიღოს გადაწყვეტილება კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემასა ან გაუქმებასთან დაკავშირებით;
   ე) სერტიფიცირების ცენტრს მიაწოდოს სერტიფიკატის გაცემისა და გაუქმებისათვის საჭირო სრულყოფილი და უტყუარი ინფორმაცია;
   ვ) წინამდებარე დოკუმენტის შესაბამისად, საჭიროების შემთხვევაში, უზრუნველყოს სუბიექტის მოწყობილობის ან/და სუბიექტის მოწყობილობის აქტივაციის მონაცემების უსაფრთხო მიწოდება სუბიექტისთვის;
   ზ) უზრუნველყოს სუბიექტის ინფორმირება კვალიფიციური ელექტრონული შტამპის სერტიფიკატების გამოყენების, მართვისა და უსაფრთხოების დაცვის შესახებ.

3. წინამდებარე თავის მიზნებისათვის, პერსონალიზაციის ორგანო ვალდებულია, უზრუნველყოს:

   ა) სუბიექტის მოწყობილობაზე კვალიფიციური ელექტრონული შტამპის კრიპტოგრაფიული გასაღების წყვილის (ღია და დახურული გასაღებების) შექმნა და სერტიფიცირების ცენტრისათვის მიწოდება;

ბ) სუბიექტის მოწყობილობისათვის იმ აქტივაციის მონაცემების მინიჭება, რომლებიც სუბიექტზე გაიცემა სერტიფიკატზე განცხადების მიღებისას;

გ) სუბიექტის მოწყობილობის უსაფრთხო მიწოდება წინამდებარე დოკუმენტით განსაზღვრული წესით (საფოსტო გზავნილის მეშვეობით);

დ) სააგენტოს მიერ გაცემული სუბიექტის მოწყობილობის ვიზუალური პერსონალიზაცია.

4. წინამდებარე თავის მიზნებისათვის, სუბიექტი ან/და წარმომადგენელი ვალდებულია:

ა) წარმოადგინოს ამ შინაგანაწესით მოთხოვნილი სწორი და სრულყოფილი ინფორმაცია კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მისაღებად;

ბ) სერტიფიკატში ასახული სუბიექტის ინფორმაციის ცვლილების შემთხვევაში, დროულად მიაწოდოს ინფორმაცია სააგენტოს;

გ) გასაღების წყვილი/კვალიფიციური ელექტრონული შტამპის სერტიფიკატი გამოიყენოს მხოლოდ წინამდებარე დოკუმენტით მითითებული დანიშნულებით;

დ) გაეცნოს მიღებულ კვალიფიციური ელექტრონული შტამპის სერტიფიკატში მითითებულ ინფორმაციას და დროულად აცნობოს სააგენტოს გამოვლენილი უზუსტობების შესახებ;

ე) გაუფრთხილდეს საკუთარ დახურულ გასაღებს და არ დაუშვას მისი გამოყენება არაუფლებამოსილი პირების მიერ;

ვ) არ ეცადოს საკუთარი დახურული გასაღების მოწყობილობიდან ამოღებას და გამოყენებას მის მიღმა, ნებისმიერი დანიშნულებით;

ზ) დახურული გასაღების არასანქცირებული გამოყენების, ან გამოყენებაზე საფუძვლიანი ეჭვის შემთხვევაში, დაუყოვნებლივ დაუკავშირდეს სააგენტოს მიმწოდებელს - წინამდებარე შინაგანაწესის 43-ე მუხლით განსაზღვრული წესით. აღნიშნული ასევე შეეხება აქტივაციის მონაცემების (მაგ.: PIN კოდების) მოხვედრას არაუფლებამოსილი პირების ხელში;

თ) არ გამოიყენოს კვალიფიციური ელექტრონული შტამპის სერტიფიკატები და შესაბამისი დახურული გასაღებები სერტიფიკატების მოქმედების ვადის ამოწურვის, სერტიფიკატის გაუქმების ან/და იმ შემთხვევაში, თუ სააგენტო აცნობებს კომპრომეტაციის თაობაზე;

ი) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შესაბამისი დახურული გასაღები გამოიყენოს მხოლოდ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების მისივე კონტროლქვეშ არსებობის პირობებში;

კ) სუბიექტის ლიკვიდაციის ან სხვა სუბიექტთან შერწყმის შეთხვევაში, დაუყოვნებლივ მიაწოდოს ინფორმაცია სააგენტოს;

ლ) შინაგანაწესის 44-ე მუხლის პირველი პუნქტის შესაბამისად, მის სახელზე გაცემული სერტიფიკატის გაუქმების საფუძვლების არსებობის შემთხვევაში, დაუყოვნებლივ დაუკავშირდეს სააგენტოს - წინამდებარე შინაგანაწესის 43-ე მუხლით განსაზღვრული წესით.

5. ამ მუხლის მე-4 პუნქტის „ე“ და „ზ“ ქვეპუნქტების მოთხოვნების შესასრულებლად სუბიექტმა და მისმა წარმომადგენელმა უნდა დაიცვან შემდეგი მოთხოვნები:

ა) კვალიფიციური ელექტრონული შტამპის დასმის პროცესში გამოყენებულმა აპარატურულმა და/ან პროგრამულმა უზრუნველყოფამ მის მომხმარებელს არ უნდა შეუზღუდოს შტამპის დასმამდე დოკუმენტის სრულად გაცნობის შესაძლებლობა;

ბ) თუ სუბიექტი მუშაობის პროცესში არ იყენებს თავის პერსონალურ კომპიუტერს ან/და სხვა მოწყობილობას (გარდა თავად სუბიექტის მოწყობილობისა), იგი ვალდებულია, შეაფასოს მოქმედების განხორციელების მიზანშეწონილობა. შეფასებისას, სულ მცირე, ყურადღება უნდა მიექცეს იმ გარემოებას, იკრიფება თუ არა აქტივაციის მონაცემები (PIN კოდი) კომპიუტერის კლავიატურაზე, ნაცვლად სპეციალური, უსაფრთხო მოწყობილობისა;

გ) საჯარო ადგილებში ან/და კონტრაჰენტის მიერ კონტროლირებად გარემოში აქტივაციის მონაცემები (PIN კოდი) უნდა აიკრიფოს ისეთი მოწყობილობის მეშვეობით, რომელიც უზრუნველყოფს კოდის საიდუმლოდ გადაცემას სუბიექტის მოწყობილობისათვის.

6. წინამდებარე თავის მიზნებისათვის, კონტრაჰენტი ვალდებულია, შეამოწმოს მიღებული სერტიფიკატის სტატუსი, რომლის საშუალებითაც ჩატარებულია შესაბამისი ოპერაცია და გაეცნოს შესაბამისი სერტიფიკატის გამოყენების პირობებს, დადგენილს მოქმედი კანონმდებლობითა და წინამდებარე შინაგანაწესით.

მუხლი 38. განცხადება კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემაზე

1. სუბიექტი კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის მოთხოვნით განცხადებით მიმართავს სააგენტოს. განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) მოთხოვნას კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შესახებ;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) სააგენტოში განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

2. სააგენტოში წარდგენილ განცხადებას უნდა დაერთოს:

ა) სუბიექტის მიერ წარმოდგენილ სუბიექტის მოწყობილობაზე სერტიფიკატის გაცემის შემთხვევაში, ამ შინაგანაწესის N3 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;

ბ) სუბიექტის ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე სერტიფიკატის გაცემის შემთხვევაში, ამ შინაგანაწესის N4 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;

გ) სააგენტოს მიერ გაცემულ სუბიექტის მოწყობილობაზე სერტიფიკატის გაცემის შემთხვევაში, ამ შინაგანაწესის N5 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;

დ) სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე სერტიფიკატის გაცემის შემთხვევაში ამ შინაგანაწესის N6 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;

ე) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი;

ვ) ამ წესის 35-ე მუხლის მე-4 პუნქტის „ა“ და „ბ“ ქვეპუნქტებით განსაზღვრული მომსახურების მოთხოვნის შემთხვევაში, კვალიფიციური ელექტრონული შტამპის მოწყობილობის კანონმდებლობით გათვალისწინებული, სტანდარტებთან შესაბამისობის დამადასტურებელი დოკუმენტაცია;

ზ) ამ წესის 35-ე მუხლის მე-4 პუნქტის „ბ“ ქვეპუნქტით განსაზღვრული მომსახურების მოთხოვნის შემთხვევაში, კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების განთავსების ადგილის მართლზომიერი მფლობელობის დამადასტურებელი დოკუმენტაცია.

3. ამ მუხლის მე-2 პუნქტის „ა“-„დ“ ქვეპუნქტებით განსაზღვრული დანართი სუბიექტის მიერ ივსება სააგენტოს ვებგვერდზე - www.sda.gov.ge - და მას შექმნისთანავე ენიჭება უნიკალური იდენტიფიკატორი. დანართის შექმნის შემდეგ მისი შინაარსის შეცვლა დაუშვებელია. აღნიშნული დანართის სააგენტოში წარდგენა შესაძლებელია მისი შექმნიდან ერთი თვის განმავლობაში.

4. მატერიალური ფორმით კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

5. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“, „ბ“ ან „გ“ ქვეპუნქტებით განსაზღვრული მომსახურების მოთხოვნის შემთხვევაში, სუბიექტმა უნდა წარმოადგინოს საფასურის გადახდის დამადასტურებელი დოკუმენტი არაუგვიანეს განცხადების შეტანის დღისა.

6. ამ მუხლის მე-5 პუნქტით განსაზღვრული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ სუბიექტმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტაცია.

7. სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შემთხვევაში, განაცხადს წარმოადგენს სააგენტოს თავმჯდომარის მიერ გამოცემული ბრძანება, რომლის საფუძველზეც განისაზღვრება სერტიფიკატის მიმღები პირი.

8. სუბიექტის წარმომადგენლობა სააგენტოში გულისხმობს შემდეგი ფუნქციების განხორციელებაზე უფლებამოსილების მინიჭებას:

ა) ამ შინაგანაწესის დანართი N3-ის შემთხვევაში:

ა.ა) გამოცხადდეს სააგენტოში და წარმოადგინოს შტამპის შექმნის საშუალება;

ა.ბ) ხელი მოაწეროს გაწეული მომსახურების მიღება-ჩაბარების აქტს.

ბ) ამ შინაგანაწესის დანართი N4-ის შემთხვევაში:

ბ.ა) დაესწროს სერტიფიკატის გენერაციის ცერემონიას;

ბ.ბ) ხელი მოაწეროს გაწეული მომსახურების მიღება-ჩაბარების აქტს.

გ) ამ შინაგანაწესის დანართი N5-ის შემთხვევაში:

გ.ა) მიიღოს კვალიფიციური ელექტრონული შტამპის შექმნის საშუალება და მისი აქტივაციის მონაცემები;

გ.ბ) ხელი მოაწეროს გაწეული მომსახურების მიღება-ჩაბარების აქტს.

დ) ამ შინაგანაწესის დანართი N6-ის შემთხვევაში:

დ.ა) გამოცხადდეს სააგენტოში კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის პროცედურაში მონაწილეობის მისაღებად;

დ.ბ) ხელი მოაწეროს გაწეული მომსახურების მიღება-ჩაბარების აქტს.

მუხლი 39. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის განცხადების დამუშავება და გადაწყვეტილების მიღება

1. განცხადების მიღებიდან არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესითა და საქართველოს მოქმედი კანონმდებლობით დადგენილ მოთხოვნებთან.

2. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო ახორციელებს სუბიექტის (მისი წარმომადგენლის) იდენტიფიკაციას და უფლებამოსილების შემოწმებას საქართველოს კანონმდებლობით დადგენილი წესით. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს და დაამუშაოს შემდეგი ინფორმაცია:

   ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;
   ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან;
   გ) უძრავი ქონების რეგისტრაციის შესახებ მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 38-ე მუხლით დადგენილ მოთხოვნებს, გარდა 38-ე მუხლის პირველი პუნქტის ,,დ“ ქვეპუნქტისა;
   ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება საქართველოს კანონმდებლობისა და ამ შინაგანაწესით დადგენილ მოთხოვნებს;
   გ) ამ მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. ამავე მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 20 სამუშაო დღეს. მარეგისტრირებელი ორგანოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

5. შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული მომსახურების მოთხოვნის შემთხვევაში, მარეგისტრირებელი ორგანო სუბიექტს უგზავნის წერილობით შეტყობინებას კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების წარმოდგენის თაობაზე. შეტყობინებაში მიეთითება კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების წარმოდგენის დრო და ადგილი. სუბიექტი ვალდებულია, გამოცხადდეს სააგენტოს მიერ წინასწარ წერილობით განსაზღვრულ დროსა და ადგილას და წარმოადგინოს კვალიფიციური ელექტრონული შტამპის შექმნის საშუალება.

6. თუ ამავე მუხლის მე-5 პუნქტით განსაზღვრულ შემთხვევაში, სუბიექტის წარმომადგენელი არ გამოცხადდა სააგენტოში, განცხადება რჩება განუხილველი.

7. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ბ“ ქვეპუნქტით განსაზღვრული მომსახურების მოთხოვნის შემთხვევაში, მარეგისტრირებელი ორგანო განმცხადებელს უგზავნის წერილობით შეტყობინებას და აცნობებს თარიღს, როდესაც შემოწმდება განმცხადებლის ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალება.

8. ამ მუხლის მე-7 პუნქტით გათვალისწინებულ შემთხვევაში, სუბიექტი ვალდებულია, სააგენტოს უფლებამოსილი პირი ფიზიკურად დაუშვას თავისი ინფრასტრუქტურის განთავსების ადგილზე. წინააღმდეგ შემთხვევაში, განცხადება რჩება განუხილველი.

9. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებულ შემთხვევაში, სერტიფიცირების ცენტრი, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, ადგენს ელექტრონული შტამპის შექმნის საშუალების სტანდარტებთან შესაბამისობას და შემოწმების შედეგს აწვდის მარეგისტრირებელ ორგანოს.

10. ამ მუხლის მე-5 და მე-7 პუნქტებით განსაზღვრულ შემთხვევებში, შტამპის სერტიფიკატის გაცემის შეუძლებლობისას, მარეგისტრირებელი ორგანო უფლებამოსილია, დამატებით განსაზღვროს გამოვლენილი ხარვეზის აღმოფხვრის ვადა, გარდა ამავე მუხლის მე-6 და მე-8 პუნქტებით გათვალისწინებული შემთხვევებისა.

11. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტით განსაზღვრული მომსახურების შემთხვევაში, სუბიექტს ეგზავნება წერილობითი შეტყობინება, რომელშიც მითითებულია სააგენტოს უფლებამოსილი პირის საკონტაქტო მონაცემები, სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებასთან წვდომის მიზნით წარმოსადგენი ინფორმაცია და მომსახურების საფასური..

12. ამ მუხლის მე-11 პუნქტით განსაზღვრული შეტყობინების ჩაბარებიდან 3 სამუშაო დღის ვადაში სუბიექტი ვალდებულია:

ა) გადაიხადოს კანონმდებლობით დადგენილი მომსახურების საფასური და გადახდის დამადასტურებელი დოკუმენტი წარუდგინოს სააგენტოს;

ბ) ამ მუხლის მე-11 პუნქტით გათვალისწინებული შეტყობინებით განსაზღვრული ინსტურუქციის შესაბამისად, შექმნას სააგენტოს ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებასთან წვდომისათვის საჭირო კრიპტოგრაფიული გასაღების სერტიფიკატი - ავთენტიფიკაციის სერტიფიკატი და მიაწოდოს ამავე შეტყობინებით განსაზღვრულ სააგენტოს უფლებამოსილ პირს.

13. ამ მუხლის მე-12 პუნქტით განსაზღვრული მომსახურების საფასურის გადახდის დამადასტურებელი დოკუმენტის წარდგენისა და შტამპის შექმნის საშუალებასთან წვდომისათვის საჭირო ავთენტიფიკაციის სერტიფიკატის შექმნის შემთხვევაში:

ა) სუბიექტი უკავშირდება სააგენტოს, რის შემდეგაც მხარეები 5 სამუშაო დღის ვადაში ერთობლივად უზრუნველყოფენ დახურული კერძო ქსელის (VPN) კონფიგურირებას (გამართვას);

ბ) დახურული კერძო ქსელის გამართვის შემდგომ სააგენტო სუბიექტს უგზავნის წერილობით შეტყობინებას კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის პროცესში მონაწილეობის მიღებასთან დაკავშირებით. შეტყობინებაში მიეთითება სერტიფიკატის გაცემის დრო და ადგილი;

გ) სააგენტო გასცემს კვალიფიციური ელექტრონული შტამპის სერტიფიკატს.

14. ამ მუხლის მე-12 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ სუბიექტმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

15. ამ მუხლის მე-12 და მე-13 პუნქტებით გათვალისწინებულ შემთხვევაში, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, სერტიფიცირებ ის ცენტრი ამოწმებს სუბიექტის მიერ მოწოდებულ შტამპის შექმნის საშუალებასთან წვდომისათვის საჭირო ავთენტიფიკაციის სერტიფიკატს, სუბიექტის წარმომადგენელთან დაკავშირების შემდეგ სააგენტოს მხარეს უზრუნველყოფს დახურული კერძო ქსელის (VPN) კონფიგურირებას (გამართვას) და შედეგების შესახებ ინფორმაციას აწვდის მარეგისტრირებელ ორგანოს.

16. სუბიექტის სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატი გაიცემა ამ შინაგანაწესის მე-40 მუხლით დადგენილი წესის შესაბამისად.

17. სუბიექტს შეიძლება უარი ეთქვას კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემაზე თუ:

ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები ამ შინაგანაწესის 38-ე მუხლის პირველი პუნქტის ,,დ“ ქვეპუნქტის მოთხოვნების შესაბამისად ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა;

ბ) განცხადების დანართი წარდგენილია ამ შინაგანაწესის 38-ე მუხლის მე-3 პუნქტით დადგენილი მოთხოვნების დარღვევით;

გ) სუბიექტმა სააგენტოს მიერ განსაზღვრულ ვადაში ვერ აღმოფხვრა ამ მუხლის მე-10 პუნქტით გათვალისწინებული ხარვეზი;

დ) დარღვეულია ამ მუხლის მე-12 პუნქტით განსაზღვრული მოთხოვნები;

ე) დარღვეულია ამ მუხლის მე-13 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული მოთხოვნები.

მუხლი 40. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემა

1. მარეგისტრირებელი ორგანოს მიერ სუბიექტის სახელზე სერტიფიკატის გაცემის შესახებ გადაწყვეტილება აღსასრულებლად ეგზავნება:

ა) ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“, „ბ“ და „დ“ ქვეპუნქტებით გათვალისწინებული მომსახურების მოთხოვნის შემთხვევაში, სერტიფიცირების ცენტრს;

ბ) ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული მომსახურების მოთხოვნის შემთხვევაში, პერსონალიზაციის ორგანოს.

2. მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, პერსონალიზაციის ორგანო უზრუნველყოფს:

ა) სუბიექტის მოწყობილობაზე კვალიფიციური ელექტრონული შტამპის ღია და დახურული გასაღების წყვილების უსაფრთხო შექმნას;

ბ) სუბიექტის სერტიფიკატის შექმნაზე მოთხოვნის ავტომატურ გადაცემას სერტიფიცირების ცენტრისთვის;

გ) სუბიექტის მოწყობილობაზე შესაბამისი ვიზუალური აღნიშვნების დატანას, სუბიექტის იდენტიფიცირებისა და სუბიექტისადმი მისი კუთვნილების დადასტურების მიზნით;

დ) სუბიექტის მოწყობილობაზე სერტიფიცირების ცენტრის მიერ გაცემული სერტიფიკატის დატანას;

ე) სუბიექტის მოწყობილობისა და მისი აქტივაციის მონაცემების სუბიექტისთვის მიწოდებას ამ შინაგანაწესის 42-ე მუხლით გათვალისწინებული წესით.

3. სააგენტოს მიერ გაცემული სუბიექტის მოწყობილობის (რომელზეც ერთხელ უკვე გაიცა სააგენტოს მიერ შესაბამისი სერტიფიკატი) იმავე მიზნით ხელმეორედ გამოყენება დაუშვებელია.

4. სერტიფიცირების ცენტრი, ამ მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტის შესაბამისად პერსონალიზაციის ორგანოს მიერ სუბიექტის სერტიფიკატის შექმნაზე მოთხოვნის მიღების შემთხვევაში, უზრუნველყოფს სუბიექტის სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შექმნას და პერსონალიზაციის ორგანოსთვის უსაფრთხო მიწოდებას.

5. სერტიფიცირების ცენტრი, ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე უზრუნველყოფს:

ა) მოთხოვნის განხილვას და სუბიექტის მოწყობილობის განთავსების ადგილზე კვალიფიციური ელექტრონული შტამპის შექმნისა და შემოწმების მონაცემების, ღია და დახურული გასაღებების წყვილის უსაფრთხო შექმნის პროცესის საკონტროლო წერტილების დადგენას ან შეფასებას, თუ ამგვარი საკონტროლო წერტილები უკვე დადგენილია;

ბ) შეთანხმებულ დროსა და ადგილზე სერტიფიცირების ცენტრის და, საჭიროების შემთხვევაში, სააგენტოს სხვა უფლებამოსილი პირების გაგზავნას გასაღების წყვილების შექმნის პროცესში (ცერემონია) მონაწილეობის მისაღებად;

გ) სუბიექტის მოწყობილობის შესაბამის სტანდარტებთან და სუბიექტის მიერ წარმოდგენილ დოკუმენტაციასთან შესაბამისობის დადგენას;

დ) სერტიფიკატის შექმნას ამ შინაგანაწესის 41-ე მუხლით გათვალისწინებული წესით.

6. სერტიფიცირების ცენტრი, ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, სუბიექტის უფლებამოსილი წარმომადგენლის თანდასწრებით უზრუნველყოფს:

ა) სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე წვდომის კოდების შექმნას და სუბიექტის წარმომადგენლისათვის უსაფრთხო მიწოდებას;

ბ) სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე წვდომისათვის საჭირო სხვა დამატებითი ინფორმაციის სუბიექტის წარმომადგენლისთვის მიწოდებას (ასეთის საჭიროების შემთხვევაში);

გ) სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის ღია და დახურული გასაღების წყვილების უსაფრთხო შექმნას;

დ) სუბიექტის სახელზე ამ შინაგანაწესის 41-ე მუხლით გათვალისწინებული წესით სერტიფიკატის შექმნას და ჩაწერას სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე.

მუხლი 41. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შექმნა

1. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“ და „ბ“ ქვეპუნქტებით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ მოწმდება სერტიფიკატის შექმნის მოთხოვნა (მისი მიღების შემდეგ) იმ ფაქტის დასადგენად, შეიქმნა თუ არა კვალიფიციური ელექტრონული შტამპის ღია და დახურული გასაღებების წყვილები უშუალოდ სუბიექტის მოწყობილობაზე და ხომ არ მომხდარა ღია გასაღებების ჩანაცვლება განცხადების სერტიფიცირების ცენტრისთვის გადაცემამდე.

2. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის პროგრამული უზრუნველყოფა ავტომატურად ამოწმებს, შეიქმნა თუ არა კვალიფიციური ელექტრონული შტამპის ღია და დახურული გასაღების წყვილი უშუალოდ სუბიექტის მოწყობილობაზე და ხომ არ მომხდარა ღია გასაღებების ჩანაცვლება სერტიფიცირების ცენტრისთვის გადაცემამდე.

3. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შექმნის მოთხოვნა მოწმდება (მისი მიღების შემდეგ) იმ ფაქტის დასადგენად, შეიქმნა თუ არა კვალიფიციური ელექტრონული შტამპის სერტიფიკატის ღია და დახურული გასაღებების წყვილები უშუალოდ სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე და ხომ არ მომხდარა ღია გასაღებების ჩანაცვლება განცხადების სერტიფიცირების ცენტრისთვის გადაცემამდე.

4. შემოწმების შედეგების შესაბამისად, სერტიფიკატის გამცემი ორგანოს საშუალებით იქმნება კვალიფიციური ელექტრონული შტამპის სერტიფიკატი. სერტიფიკატის შესაქმნელად გამოიყენება ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტით განსაზღვრული „GEO ESeal CA G(n)“ სერტიფიკატის გამცემი ორგანო. **(ცვლილება 2021.06.07.N245/ს)**

5. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ შექმნილი სერტიფიკატი სერტიფიცირების ცენტრის მიერ დაიტანება სუბიექტის მიერ წარმოდგენილ მოწყობილობაზე.

6. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ შექმნილი სერტიფიკატი ეგზავნება თავად სუბიექტს.

7. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ შექმნილი სერტიფიკატი ეგზავნება პერსონალიზაციის ორგანოს, რომელიც ამოწმებს მიღებულ მონაცემებს და უზრუნველყოფს სერტიფიკატის დატანას სააგენტოს მიერ გაცემულ სუბიექტის მოწყობილობაზე.

8. ამ შინაგანაწესის 35-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტით გათვალისწინებული მომსახურების ფარგლებში, სერტიფიცირების ცენტრის მიერ კვალიფიციური ელექტრონული შტამპის სერტიფიკატი დაიტანება სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე.

მუხლი 42. სუბიექტის მოწყობილობისა და მისი აქტივაციის მონაცემების მიწოდება

1. დაუშვებელია, სუბიექტის მოწყობილობის აქტივაციის მონაცემების სუბიექტისათვის მიწოდება სუბიექტის მოწყობილობასთან ან სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე წვდომისათვის საჭირო ინფორმაციასთან ერთად, გარდა უშუალოდ სუბიექტის წარმომადგენლისთვის პირადად გადაცემის შემთხვევისა.

2. სუბიექტის მოწყობილობის, აქტივაციის მონაცემების, ან სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ სუბიექტის მოწყობილობაზე წვდომისათვის საჭირო ინფორმაციის უშუალოდ სუბიექტის წარმომადგენლისთვის გადაცემის შემთხვევაში (გარდა ფოსტის მეშვეობით გადაცემის შემთხვევისა), დგება შესაბამისი მიღება-ჩაბარების აქტი.

მუხლი 43. კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან დაკავშირებული მომსახურების შეწყვეტა

1. კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან დაკავშირებული მომსახურება წყდება:
   ა) ამ შინაგანაწესით დადგენილი სერტიფიკატებისა და მასთან დაკავშირებული ინფორმაციის შენახვის ვადის ამოწურვის შემთხვევაში;
   ბ) სააგენტოს მიერ მომსახურების შეწყვეტის შემთხვევაში;
   გ) სააგენტოს ლიკვიდაციის შემთხვევაში.

3. ამ მუხლის პირველი პუნქტის „ბ“ და „გ“ ქვეპუნქტების შესაბამისად განსაზღვრული, სერტიფიკატთან დაკავშირებული მომსახურების შეწყვეტის შედეგები და ვალდებულებები რეგულირდება საქართველოს კანონმდებლობის შესაბამისად.

მუხლი 44. განცხადება კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმებაზე

1. სერტიფიკატი შესაძლოა გაუქმდეს შემდეგ შემთხვევებში:
   ა) თუ კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმება მოითხოვა უფლებამოსილმა პირმა;
   ბ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატში მითითებული ინფორმაციის ცვლილების შემთხვევაში;
   გ) თუ არსებობს დასაბუთებული ვარაუდი კვალიფიციური ელექტრონული შტამპის კომპრომეტირების შესახებ;
   დ) თუ დადგინდა, რომ კვალიფიციური ელექტრონული შტამპის შექმნის მოწყობილობა გამოსაყენებლად უვარგისია;
   ე) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის ვადის გასვლის შემთხვევაში (გაუქმდება ავტომატურად);

ვ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მფლობელი იურიდიული პირის ლიკვიდაციის შემთხვევაში;

ზ) თუ კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემისას სააგენტომ დაუშვა შეცდომა, რის შედეგადაც შეუძლებელია სერტიფიკატის გამოყენება, ან/და სერტიფიკატში დატანილია არასწორი ინფორმაცია;

თ) საქართველოს კანონმდებლობით დადგენილ სხვა შემთხვევებში.

2. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების მოთხოვნა შეუძლია სუბიექტის უფლებამოსილ წარმომადგენელს ან საქართველოს კანონმდებლობით დადგენილ შესაბამის უფლებამოსილ პირს.

3. შესაბამისი უფლებამოსილი პირი, კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების მოთხოვნით განცხადებით მიმართავს სააგენტოს. განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების შესახებ მოთხოვნას;

ბ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების მიზეზს;

ე) სუბიექტის სახელზე გაცემული კონკრეტული სერტიფიკატის გაუქმების საჭიროების შემთხვევაში, გასაუქმებელი კვალიფიციური ელექტრონული შტამპის სერტიფიკატის იდენტიფიკაციისთვის აუცილებელ ინფორმაციას (სერტიფიკატის სერიული ნომერი, სერტიფიკატის გაცემის თარიღი, სააგენტოს მიერ გაცემული სუბიექტის მოწყობილობის სერიული ნომერი);

ვ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

4. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

5. მატერიალური ფორმით წარდგენილი კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

6. სუბიექტს შეუძლია სააგენტოს დისტანციური მომსახურების სამსახურში ელექტრონული ფორმით წარადგინოს კვალიფიციური ელექტრონული შტამპის 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.

7. ამ მუხლის პირველი პუნქტის „გ“-„ზ“ ქვეპუნქტებით განსაზღვრულ შემთხვევებში, სერტიფიკატის გაუქმება შეიძლება მოითხოვოს სანდო მომსახურების მიმწოდებელმა.

მუხლი 45. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების შესახებ განცხადების განხილვა და გადაწყვეტილების მიღება

1. ამ შინაგანაწესის 44-ე მუხლის მე-2 და მე-7 პუნქტებით გათვალისწინებულ შემთხვევაში, შესაბამისი მოთხოვნის მიღების შემდეგ მარეგისტრირებელი ორგანო განიხილავს მას და იღებს გადაწყვეტილებას სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის თაობაზე.

2. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო ახორციელებს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაციას. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 44-ე მუხლის მე-3 და მე-4 პუნქტებით დადგენილ მოთხოვნებს, გარდა 44-ე მუხლის მე-3 პუნქტის ,,ვ“ ქვეპუნქტისა;

ბ) ამ მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 5 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

5. ამ შინაგანაწესის 44-ე მუხლის მე-6 პუნქტით გათვალისწინებულ შემთხვევაში მოთხოვნის მიღების შემდეგ დისტანციური მომსახურების სამსახური განიხილავს მას და იღებს გადაწყვეტილებას სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის თაობაზე.

6. დისტანციური მომსახურების სამსახური ახდენს სუბიექტის უფლებამოსილი წარმომადგენლის იდენტიფიკაციას, ავთენტიფიკაციას და უფლებამოსილების დადგენას საქართველოს კანონმდებლობით დადგენილი წესით.

7. სუბიექტს შეიძლება უარი ეთქვას კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმებაზე, თუ:

ა) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი ვადაგასულია;

ბ) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი უკვე გაუქმებულია;

გ) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი არ არის გაცემული სააგენტოს მიერ;

დ) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები ამ შინაგანაწესის 44-ე მუხლის მე-3 პუნქტის ,,ვ“ ქვეპუნქტის მოთხოვნების შესაბამისად ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა.

8. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის შესახებ გადაწყვეტილება გამოიცემა სუბიექტის მიერ სერტიფიკატის გაუქმების მოთხოვნის სააგენტოში წარდგენიდან არაუგვიანეს მომდევნო სამუშაო დღისა.**(ცვლილება 2021.06.07.N245/ს)**

9. კვალიფიციური ელექტრონული შტამპის სერტიფიკატი უქმდება ამ მუხლის მე-8 პუნქტით გათვალისწინებული გადაწყვეტილების მიღების დღეს.**(ცვლილება 2021.06.07.N245/ს)**

მუხლი 46. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმება

1. ამ შინაგანაწესის 44-ე მუხლის მე-2 და მე-5 პუნქტების შესაბამისად მიღებული მოთხოვნის საფუძველზე სერტიფიკატის გაუქმებასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს მარეგისტრირებელი ორგანო.

2. ამ შინაგანაწესის 44-ე მუხლის მე-6 პუნქტის შესაბამისად მიღებული მომართვის საფუძველზე სერტიფიკატის გაუქმებასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს დისტანციური მომსახურების სამსახური.

3. ამ მუხლის პირველი და მეორე პუნქტის შესაბამისად განსაზღვრული პირების მიერ სერტიფიკატის გაუქმების მოთხოვნა, ასევე, შესაძლებელია გადაეგზავნოს სერტიფიცირების ცენტრს, რომელიც, თავის მხრივ, ამ შინაგანაწესით დადგენილი წესის შესაბამისად აუქმებს სერტიფიკატს.

4. იმ შემთხვევაში, თუ კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის მომენტისათვის ფიქსირდება სხვაობა ამ შინაგანაწესის 38-ე მუხლის მე-2 პუნქტის შესაბამისად სუბიექტის მიერ კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემასთან დაკავშირებით მიღებულ განცხადებასა და სერტიფიკატის გაცემის მომენტისათვის სუბიექტის სახელზე გაცემული აქტიური სტატუსის მქონე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის ამ შინაგანაწესის 36-ე მუხლის პირველი პუნქტით განსაზღვრულ მონაცემებს შორის, მარეგისტრირებელი ორგანო აუქმებს განსხვავებული მონაცემებით არსებულ აქტიურ სერტიფიკატს ახალი სერტიფიკატის გაცემასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების დღეს.

5. სერტიფიკატის გაუქმების შესახებ ინფორმაცია აღირიცხება ელექტრონულ ჟურნალში არანაკლებ 10 წლის ვადით.

6. სერტიფიკატის შესახებ ინფორმაცია ხელმისაწვდომია სერტიფიკატის გაუქმების შესახებ შესაბამისი გადაწყვეტილების მიღებიდან არაუგვიანეს 60 წუთისა.

7. გაუქმებული სერტიფიკატის ხელახლა ამოქმედება დაუშვებელია.

მუხლი 47. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შეჩერება

კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მოქმედების შეჩერება დაუშვებელია.

მუხლი 48. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნება

1. სუბიექტის სახელზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატი ქვეყნდება ამავე სუბიექტის წერილობითი თანხმობის საფუძველზე.

2. სუბიექტის სახელზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნება გულისხმობს სანდო მომსახურების მიმწოდებლის მიერ ამავე მუხლის მე-3 პუნქტის შესაბამისად სუბიექტის წერილობით მოთხოვნაში მითითებული სერტიფიკატის ვებგვერდზე https://id.ge გამოქვეყნებას და გამოქვეყნებული სერტიფიკატის საჯაროდ ხელმისაწვდომობის უზრუნველყოფას.

3. სუბიექტი მის სახელზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნების მოთხოვნით განცხადებით მიმართავს სააგენტოს.

4. სუბიექტის სახელზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნების მოთხოვნა უნდა მოიცავდეს:

ა) კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნების შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) გამოსაქვეყნებელი კვალიფიციური ელექტრონული შტამპის სერტიფიკატის სერიულ ნომერს;

ე) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

5. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

6. კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნების მოთხოვნა, წარმოდგენილი მატერიალური ფორმით, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

7 განცხადების მიღებიდან 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო განიხილავს მას და იღებს გადაწყვეტილებას სუბიექტის სახელზე გაცემული კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გამოქვეყნების ან გამოქვეყნებაზე უარის თქმის თაობაზე.

8. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო ახორციელებს სუბიექტის (მისი წარმომადგენლის) იდენტიფიკაციას. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

9. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ მუხლის მე-4 და მე-5 პუნქტებით დადგენილ მოთხოვნებს, გარდა მე-4 მუხლის ,,ე“ ქვეპუნქტისა;

ბ) ამ მუხლის მე-8 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

10. ამ მუხლის მე-9 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 5 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

11. განმცხადებელს შეიძლება უარი ეთქვას კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმებაზე, თუ განმცხადებლის მიერ მოთხოვნილი გამოსაქვეყნებელი სერტიფიკატი არ არის გაცემული სააგენტოს მიერ ან განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები ამ მუხლის მე-4 პუნქტის ,,ე“ ქვეპუნქტის მოთხოვნების შესაბამისად ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა.

12. სერტიფიცირების ცენტრი მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე აქვეყნებს კვალიფიციური ელექტრონული შტამპის სერტიფიკატს.

მუხლი 49. კვალიფიციური ელექტრონული შტამპის ღია და დახურული გასაღებების წყვილის გენერაცია და მართვა

1. სუბიექტის კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გასაღების წყვილი იქმნება უშუალოდ სუბიექტის მოწყობილობის შიგნით.

2. გასაღების პარამეტრებია:

   ა) კრიპტოგრაფიული ალგორითმი - RSA;

   ბ) გასაღების სიგრძე - 2048 ბიტი.

3. სუბიექტის მოწყობილობაზე გენერირებული ღია გასაღები სერტიფიკატის გამცემ ორგანოს გადაეცემა უსაფრთხო წესით, რაც ითვალისწინებს ინფორმაციის ავთენტურობისა და მთლიანობის დადასტურებას. მიმღები მხარე შესაბამისი მექანიზმებით ამოწმებს, მოხდა თუ არა გასაღების გენერაცია უშუალოდ მოწყობილობაზე.

4. სუბიექტის დახურული გასაღების მესამე პირისთვის მიბარება და სარეზერვო ასლის შექმნა დაუშვებელია. გასაღებების წყვილი იქმნება სუბიექტის მოწყობილობაზე, მოწყობილობიდან რამე სახით (მათ შორის, დაშიფრული) ინფორმაციის ამოკითხვის შესაძლებლობის გარეშე.

5. სააგენტოს მიერ გაცემული კვალიფიციური ელექტრონული შტამპის შექმნის და სააგენტოს ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებით კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის დახურული გასაღებების აქტივაციის მონაცემების გამოყენება შესაძლებელია შემდეგი პირობებით:

   ა) კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის დახურული გასაღებების გამოყენება - მხოლოდ შესაბამისი აქტივაციის მონაცემის (PIN კოდის) შეყვანისას;

   ბ) PIN კოდი არ შეიძლება იყოს 4 ციფრზე ნაკლები. თუ სუბიექტის მოწყობილობა ამის საშუალებას იძლევა, ციფრებთან ერთად დასაშვებია დამატებითი სიმბოლოების გამოყენება;

   გ) PIN კოდი უნდა იბლოკებოდეს არაუმეტეს 5 არასწორი ცდის შემდეგ.

6. სააგენტოს ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებით კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის დახურული გასაღებების გამოყენება დასაშვებია მხოლოდ სუბიექტის კონტროლქვეშ.

7. სუბიექტის მიერ წარმოდგენილი და სუბიექტის ინფრასტრუქტურაში ინტეგრირებული სუბიექტის მოწყობილობების და ორგანიზაციის ავთენტიფიკაციის დახურული გასაღებების აქტივაციის მონაცემების უსაფრთხოების სტანდარტების დაცვის უზრუნველყოფაზე პასუხისმგებელია თავად სუბიექტი.

8. სუბიექტის მოწყობილობის რომელიმე პროგრამულ უზრუნველყოფაში ინტეგრაციისას, სუბიექტი თავადაა ვალდებული, შეაფასოს აქტივაციის მონაცემების პროგრამულ უზრუნველყოფაში ინტეგრაციის რისკები. კერძოდ, ყურადღება უნდა მიექცეს იმ გარემოებას, რომ აქტივაციის მონაცემების სერვერის ფაილურ სისტემაში ან სხვა მსგავს, ადვილად ხელმისაწვდომ ადგილზე შენახვა გაზრდის გასაღების კომპრომეტაციის რისკს. გამოყენებული უნდა იყოს გასაღების დინამიკური აქტივაცია პასუხისმგებელი პირების მონაწილეობით (სერვერის ყოველი გადატვირთვისას შესაბამისი პირები მექანიკურად შეიყვანენ აქტივაციის მონაცემებს, რის შემდეგადაც გააქტიურდება სუბიექტის მოწყობილობაში მოთავსებული დახურული გასაღები შესაბამისი ოპერაციების ჩასატარებლად) ან სხვა უსაფრთხო მეთოდი.

9. სუბიექტის სახელზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის დროს გენერირებულ გასაღების წყვილზე ახალი სერტიფიკატი არ გაიცემა.

თავი V

იურიდიული პირის ავთენტიფიკაციის სერტიფიკატების გაცემა და მომსახურება

მუხლი 50. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატი და სერტიფიკატის გამოყენების წესი

1. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატის დანიშნულებაა ელექტრონულ სისტემებში სუბიექტის რწმუნების მაღალი ხარისხით იდენტიფიკაცია და ავთენტიფიკაცია, მასთან უსაფრთხო კავშირის დამყარების და ინფორმაციის უსაფრთხოდ გაცვლის უზრუნველყოფის მიზნით.

2. დაუშვებელია სუბიექტზე გაცემული ავთენტიფიკაციის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა. ასევე დაუშვებელია მისი გამოყენება სხვა სერტიფიკატების გასაცემად, მათი გაუქმების შესახებ ინფორმაციაზე ან დროის აღნიშვნის ტოკენზე ხელმოსაწერად.

3. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატი გაიცემა 2 წლისა და 6 თვის მოქმედების ვადით.

4. თითოეული იურიდიული პირის ავთენტიფიკაციის სერტიფიკატში შეიტანება „კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკის“ უნიკალური იდენტიფიკატორი, რომელიც უზრუნველყოფს სერტიფიკატის გაცემის დროისთვის წინამდებარე დოკუმენტის მოქმედი რედაქციის იდენტიფიცირების შესაძლებლობას.

5. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. სერტიფიკატის ავტომატური შემოწმების მომსახურებები და მათი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.

6. სერტიფიკატის შესაქმნელად გამოიყენება ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ზ“ ქვეპუნქტით განსაზღვრული „GEO Organizational Authentication CA G(n)“ სერტიფიკატის გამცემი დაქვემდებარებული ორგანო. **(ცვლილება 2021.06.07.N245/ს)**

7. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატის პროფილი განისაზღვრება ამ შინაგანაწესის N2 დანართის შესაბამისად.

8. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატი გაიცემა კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან ერთად. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატის მოთხოვნა კვალიფიციური ელექტრონული შტამპის სერტიფიკატისაგან დამოუკიდებლად დაუშვებელია.

9. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატი უქმდება კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან ერთად. იურიდიული პირის ავთენტიფიკაციის სერტიფიკატის გაუქმების მოთხოვნა კვალიფიციური ელექტრონული შტამპის სერტიფიკატისაგან დამოუკიდებლად დაუშვებელია.

თავი VI ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემისა და მომსახურების წესი

მუხლი 51. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი და სერტიფიკატის გამოყენების წესი

1. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემა არის კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის მომსახურება, რომელიც გულისხმობს სუბიექტისთვის, ელექტრონული ხელმოწერის დეშიფრაციის ინსტრუმენტის სააგენტოსთვის გადაცემის პირობით, ღია და დახურული გასაღების წყვილისა და ღია გასაღებზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შექმნას. აღნიშნული სერტიფიკატის გაცემა მოიცავს:
   ა) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების აღრიცხვას;
   ბ) ელექტრონული ხელმოწერის ბიომეტრიული შიფრაციის სერტიფიკატის არაუფლებამოსილი პირის მიერ გამოყენების ან/და გამოყენების საფრთხის შემთხვევაში მის გაუქმებას;
   გ) გაუქმებული სერტიფიკატების სიის გამოქვეყნების გზით გაუქმებული ელექტრონული ბიომეტრიული შიფრაციის სერტიფიკატის შესახებ ინფორმაციის საჯარო ხელმისაწვდომობას.

2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის დანიშნულებაა ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაცია.

3. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი სააგენტოს მიერ გაიცემა 2 წლისა და 6 თვის მოქმედების ვადით.

4. თითოეულ ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატში შეიტანება ,,ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გაცემისა და მომსახურების

პოლიტიკის“ უნიკალური იდენტიფიკატორი, რომელიც უზრუნველყოფს სერტიფიკატის გაცემის დროისთვის წინამდებარე დოკუმენტის მოქმედი რედაქციის იდენტიფიცირების შესაძლებლობას.

5. სუბიექტის ღია და დახურული გასაღების წყვილი იქმნება უშუალოდ იმ მოწყობილობაზე, რომელიც განკუთვნილია მისი შემდგომი შენახვისათვის.

6. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტისთვის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი გაიცემა სააგენტოს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაში ინტეგრირებულ, ბიომეტრიული მონაცემების დეშიფრაციის დახურული გასაღების უსაფრთხო სანახზე.

7. ბიომეტრიული მონაცემების მიმღები სუბიექტისთვის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი გაიცემა სუბიექტის მიერ წარმოდგენილ ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალურ მოწყობილობაზე.

8. ელექტრონული ხელმოწერის დეშიფრაციის ინსტრუმენტის სააგენტოსთვის მიწოდება არ მოეთხოვება ბიომეტრიული მონაცემების მიმღებ სუბიექტს

9. სუბიექტის დახურული გასაღების დანიშნულებაა დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაცია.

10. დაუშვებელია სუბიექტზე გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გამოყენება ყველა სხვა დანიშნულებით, გარდა წინამდებარე მუხლში მითითებულისა.

11. სუბიექტის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატები ინახება სააგენტოს მონაცემთა ელექტრონულ ბაზაში და ისინი არ ქვეყნდება.

მუხლი 52. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატში სუბიექტის განმასხვავებელი სახელის სახელდებისა და ინტერპრეტირების წესი

1. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მიზნებისათვის, სუბიექტებს განმასხვავებელი სახელი ენიჭებათ X.509v3 ფორმატით, რომელიც ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ დადგენილი RFC (Request for Comments) 5280 სტანდარტითაა განსაზღვრული შემდეგი წესით:
   ა) C=GE (ქვეყნის კოდი);
   ბ) O=სუბიექტის დასახელება (იურიდიული პირის შემთხვევაში, ცარიელია ფიზიკური პირის შემთხვევაში);
   გ) CN=სუბიექტის სახელი და გვარი (ფიზიკური პირის შემთხვევაში) ან სუბიექტის დასახელება (იურიდიული პირის შემთხვევაში);
   დ) UID =სუბიექტის საიდენტიფიკაციო კოდი;
   ე) SERIALNUMBER = გაცემული სერტიფიკატის რიგითი ნომერი.

2. სუბიექტის განმასხვავებელ სახელებში ანონიმური მომხმარებლისა და ფსევდონიმების გამოყენება დაუშვებელია. ამასთან, არ მოწმდება განმასხვავებელი სახელის სუბიექტის რეგისტრირებულ სავაჭრო ნიშანთან თანხვედრა.

3. გაცემული სერტიფიკატის რიგითი ნომერი (SERIALNUMBER ობიექტის იდენტიფიკატორი 2.5.4.5) აღნიშნავს ამ სუბიექტზე გაცემული სერტიფიკატის რიგით ნომერს.

4. სუბიექტის დასახელება, სახელი და გვარი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატში შეიტანება ინგლისურ ენაზე.

5. იურიდიული პირის შემთხვევაში, სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემისათვის მომხმარებლის დასახელება და საიდენტიფიკაციო კოდი განისაზღვრება სსიპ - საჯარო რეესტრის ეროვნული სააგენტოში არსებული ინფორმაციის მიხედვით, ხოლო ასეთის არარსებობის შემთხვევაში, სსიპ - შემოსავლების სამსახურის გადამხდელთა რეესტრის მიხედვით .

6. ამოღებულია. **(ცვლილება 2021.06.07.N245/ს)**

7. ამ მუხლის მე-5 პუნქტის შესაბამისად განსაზღვრულ რეესტრებში სუბიექტის ინგლისური დასახელების არარსებობის შემთხვევაში, სუბიექტს ინგლისური დასახელება ენიჭება ამ შინაგანაწესის 54-ე მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული მომხმარებლის ინგლისური დასახელების შესაბამისად.

8. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატში სუბიექტის ინფორმაციის ცვლილება დაუშვებელია. სერტიფიკატში დატანილი სუბიექტის ინფორმაციის ცვლილების შემთხვევაში, სუბიექტის სახელზე გაიცემა ახალი სერტიფიკატი შეცვლილი მონაცემებით.

მუხლი 53. ღია გასაღების ინფრასტრუქტურაში მონაწილე მხარეთა ვალდებულებები და პასუხისმგებლობები

1. წინამდებარე თავის მიზნებისათვის, სერტიფიცირების ცენტრი პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების გამართულ და უსაფრთხო მუშაობაზე, რაც მოიცავს:

   ა) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების უსაფრთხოების უზრუნველყოფას, მათ შორის, შესაბამისი დახურული გასაღებისა და აქტივაციის მონაცემების დაცვას კომპრომეტირებისგან;
   ბ) სერტიფიკატის შექმნისა და გაუქმების უზრუნველყოფასა და წინამდებარე დოკუმენტით განსაზღვრული ფუნქციების შესაბამისად, მარეგისტრირებელი ორგანოს მოთხოვნის დაკმაყოფილებას;
   გ) წინამდებარე დოკუმენტით განსაზღვრული გაუქმებული სერტიფიკატების სიის ხელმისაწვდომობას მომხმარებლისა და კონტრაჰენტებისათვის;
   დ) დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის პროცესების უსაფრთხოების უზრუნველყოფას ამ შინაგანაწესით დადგენილი წესის შესაბამისად.

2. წინამდებარე თავის მიზნებისათვის, მარეგისტრირებელი ორგანო ვალდებულია:

   ა) მიიღოს განცხადება სუბიექტის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;
   ბ) მიიღოს განცხადება სუბიექტის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმებაზე და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;
   გ) შეამოწმოს განმცხადებლის უფლებამოსილება;
   დ) მიიღოს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის ან გაუქმების გადაწყვეტილება;
   ე) სერტიფიცირების ცენტრს მიაწოდოს სერტიფიკატის გაცემისა და გაუქმებისათვის საჭირო სრულყოფილი და უტყუარი ინფორმაცია;
   ვ) უზრუნველყოს სუბიექტის ინფორმირება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გამოყენების, მართვისა და უსაფრთხოების დაცვის შესახებ.

3. წინამდებარე თავის მიზნებისათვის, ბიომეტრიული მონაცემების შემგროვებელი სუბიექტი ვალდებულია:

   ა) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მიზნებისთვის, სააგენტოს მიაწოდოს ელექტრონული ხელმოწერის შექმნისა და შიფრაციის მოწყობილობის შესახებ ინფორმაცია;
   ბ) სააგენტოს მიაწოდოს ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტი და უზრუნველყოს აღნიშნული ინსტრუმენტის გამართულად ფუნქციონირების მხარდაჭერა ამ შინაგანაწესით დადგენილი წესის შესაბამისად;
   გ) შეინახოს ელექტრონული ხელმომწერის დაშიფრული ბიომეტრიული მონაცემები ელექტრონული ხელმოწერის შედეგად შექმნილ დოკუმენტში ისე, რომ შესაძლებელი იყოს შიფრაციის სერტიფიკატის იდენტიფიცირება;
   დ) ამ შინაგანაწესის მე-60 მუხლის პირველი პუნქტის შესაბამისად მის სახელზე გაცემული სერტიფიკატის გაუქმების საფუძვლების არსებობის შემთხვევაში, დაუყოვნებლივ დაუკავშირდეს სააგენტოს.

4. წინამდებარე თავის მიზნებისათვის, კონტრაჰენტი ვალდებულია, შეამოწმოს მიღებული სერტიფიკატის სტატუსი, რომლის საშუალებითაც ჩატარებულია შესაბამისი ოპერაცია და გაეცნოს შესაბამისი სერტიფიკატის მოქმედი კანონმდებლობითა და წინამდებარე შინაგანაწესით დადგენილ გამოყენების პირობებს;

მუხლი 54. განცხადება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემასთან დაკავშირებით

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მოთხოვნით განცხადებით მიმართავს სააგენტოს.

2. სუბიექტის მიერ წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

   ა) მოთხოვნას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის შესახებ;
   ბ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
   გ) ხელმოწერის თარიღს;
   დ) სააგენტოში განცხადების მატერიალური ფორმით წარდგენის შემთხვევაში, განცხადების წარდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

3. სააგენტოში წარდგენილ განცხადებას უნდა დაერთოს შემდეგი დოკუმენტები:

   ა) ამ შინაგანაწესის N7 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;

ბ) სუბიექტის უფლებამოსილების დამადასტურებელი დოკუმენტი.

4. სუბიექტი, ამ შინაგანაწესის N8 დანართით განსაზღვრული მოთხოვნების შესაბამისად, უზრუნველყოფს დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის სააგენტოსთვის მიწოდებას განცხადების წარდგენიდან არაუგვიანეს 5 სამუშაო დღეში.

5. ამ მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული დანართი სუბიექტის მიერ ივსება სააგენტოს ვებგვერდზე (www.sda.gov.ge) და მას შექმნისთანავე ენიჭება უნიკალური იდენტიფიკატორი. დანართის შექმნის შემდეგ მისი შინაარსის შეცვლა დაუშვებელია. აღნიშნული დანართის სააგენტოში წარდგენა შესაძლებელია მისი შექმნიდან ერთი თვის განმავლობაში.

6. მატერიალური ფორმით ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით. ამ შინაგანაწესის N6 დანართით განსაზღვრული სუბიექტის წარმომადგენლობა სააგენტოში გულისხმობს მომსახურების მიღება-ჩაბარების აქტზე ხელმოწერის განხორციელებაზე უფლებამოსილების მინიჭებას.

მუხლი 55. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის განცხადების განხილვა და გადაწყვეტილების მიღება

1. განცხადების მიღებისა და ამ შინაგანაწესის 54-ე მუხლის მე-4 პუნქტით განსაზღვრული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის წარდგენის ვადის გასვლიდან არაუმეტეს 10 სამუშაო დღეში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების ამ შინაგანაწესითა და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობას.

2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო:

   ა) ამოწმებს სუბიექტის მონაცემებს სსიპ - საჯარო რეესტრის ეროვნული სააგენტოში არსებული ინფორმაციის მიხედვით, ხოლო ასეთის არარსებობის შემთხვევაში, სსიპ - შემოსავლების სამსახურის გადამხდელთა რეესტრის მიხედვით;

   ბ) ამოწმებს სუბიექტის წარმომადგენლის ვინაობასა და უფლებამოსილებას საქართველოს კანონმდებლობით დადგენილი წესით;

   გ) სერტიფიცირების ცენტრს აწვდის სუბიექტის მიერ წარმოდგენილი დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტს, ამ შინაგანაწესის N8 დანართით განსაზღვრულ მოთხოვნებთან შესაბამისობის დადგენის მიზნით.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 54-ე მუხლით დადგენილ მოთხოვნებს, გარდა 54-ე მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტისა;

   ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება საქართველოს კანონმდებლობისა და ამ შინაგანაწესით დადგენილ მოთხოვნებს;

   გ) ამ მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, სერტიფიცირების ცენტრი ადგენს ამ მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის შესაბამისად მიღებული ინფორმაციის/მოწყობილობის ამ შინაგანაწესით განსაზღვრულ მოთხოვნებთან შესაბამისობას და შედეგს აწვდის მარეგისტრირებელ ორგანოს.

5. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 20 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

6. სუბიექტის მიერ წარმოდგენილი დოკუმენტების შესაბამისობის დადგენის შემდეგ სუბიექტს ეგზავნება შეტყობინება სერტიფიკატის საფასურის გადახდის თაობაზე. შეტყობინების ჩაბარებიდან 3 სამუშაო დღის ვადაში სუბიექტი ვალდებულია, გადაიხადოს კანონმდებლობით დადგენილი მომსახურების საფასური. აღნიშნულ ვადაში მომსახურების საფასურის გადახდის დამადასტურებელი დოკუმენტის წარდგენის შემთხვევაში, სააგენტო, ამ შინაგანაწესის 56-ე მუხლით დადგენილი წესის შესაბამისად, გასცემს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატს.

7. ბიომეტრიული მონაცემების შემგროვებელ სუბიექტს საფასურის გადახდის დამადასტურებელი ინფორმაციის წარდგენა არ მოეთხოვება, თუ სუბიექტმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

8. ბიომეტრიული მონაცემების შემგროვებელ სუბიექტზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი გაიცემა მხოლოდ იმ შემთხვევაში, თუ აღნიშნულ სუბიექტს სააგენტო უწევს ამ წესის VII თავით განსაზღვრულ, ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურებას.

9. ბიომეტრიული მონაცემების შემგროვებელ სუბიექტს შეიძლება უარი ეთქვას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემაზე, თუ:

ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 54-ე მუხლის მე-2 პუნქტის ,,დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა;

ბ) სუბიექტმა ამ მუხლის მე-6 პუნქტით დადგენილ ვადაში არ გადაიხადა კანონმდებლობით დადგენილი მომსახურების საფასური;

გ) განცხადების დანართი წარდგენილია ამ შინაგანაწესის 54-ე მუხლის მე-5 პუნქტით დადგენილი მოთხოვნების დარღვევით.

მუხლი 56. სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემა

1. მარეგისტრირებელი ორგანოს მიერ სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის შესახებ გადაწყვეტილება აღსასრულებლად ეგზავნება სერტიფიცირების ცენტრს.

2. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემასთან დაკავშირებით მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, სერტიფიცირების ცენტრი უზრუნველყოფს:

   ა) სააგენტოს ინფრასტრუქტურაში ინტეგრირებული ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახში ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის ღია და დახურული გასაღების წყვილის უსაფრთხო შექმნას;

   ბ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მოთხოვნის შექმნას;

   გ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემას და ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახში ჩაწერას;

   დ) მარეგისტრირებელი ორგანოსთვის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შესახებ ინფორმაციისა და სერტიფიკატის საკონტროლო ჯამის მიწოდებას.

3. ბიომეტრიული მონაცემების შემგროვებელ სუბიექტს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი მიეწოდება ამ შინაგანაწესის 57-ე მუხლით დადგენილი წესით.

4. სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შესაქმნელად გამოიყენება ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტით განსაზღვრული „**Biometric Encryption CA** “ სერტიფიკატის გამცემი ორგანო.

5. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის ღია და დახურული გასაღების წყვილის შექმნა, სერტიფიკატის გაცემა და შესაბამის მოწყობილობაზე დატანა ხორციელდება სააგენტოს მიერ დამტკიცებული “მექანიკურ რეჟიმში გასაღების წყვილის შექმნისა და სერტიფიკატის გაცემის პროცედურის“ მიხედვით.

6. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის სახელზე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის შემდეგ მარეგისტრირებელი ორგანო სუბიექტს წერილობით უგზავნის ინფორმაციას გაცემული სერტიფიკატის შესახებ, სადაც მითითებულია ამ მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტის შესაბამისად განსაზღვრული სერტიფიკატის საკონტროლო ჯამი.

მუხლი 57. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტისთვის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის მიწოდება

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტისთვის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გადაცემა, სუბიექტის მოთხოვნის საფუძველზე, შესაძლებელია:

   ა) ამ შინაგანაწესის N7 დანართის შესაბამისად დამტკიცებულ განცხადების დანართში მითითებული სუბიექტის უფლებამოსილი პირის სააგენტოში გამოცხადების შემდეგ მისთვის უშუალოდ გადაცემის გზით;

   ბ) ამ შინაგანაწესის N7 დანართის შესაბამისად დამტკიცებულ განცხადების დანართში მითითებული სუბიექტის უფლებამოსილი პირის ელექტრონული ფოსტის მისამართზე გაგზავნის გზით.

2. ამ მუხლის პირველი პუნქტის შესაბამისად სუბიექტისთვის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გადაცემის შემდგომ სუბიექტისა და მარეგისტრირებელი ორგანოს უფლებამოსილ პირებს შორის ფორმდება სერტიფიკატის გადაცემის შესახებ მიღება-ჩაბარების აქტი.

მუხლი 58. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის ღია და დახურული გასაღებების წყვილის გენერაცია და მართვა

1. ამ შინაგანაწესის 51-ე მუხლის მე-6 და მე-7 პუნქტების შესაბამისად განსაზღვრული სუბიექტის ტიპის მიხედვით ღია და დახურული გასაღების წყვილის შექმნისა და შენახვისათვის გამოიყენება:

   ა) ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის შემთხვევაში, სანდო მომსახურების მიმწოდებლის ინფრასტრუქტურაში ინტეგრირებული ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახი;

   ბ) ბიომეტრიული მონაცემების მიმღები სუბიექტის შემთხვევაში, სუბიექტის ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობა.

2. ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახი მოთავსებულია სანდო მომსახურების მიმწოდებლის მონაცემთა დამუშავების ცენტრში.

3. გასაღების წყვილის შექმნისათვის საჭირო პროცედურები ტარდება დაცულ საოფისე ზონაში, სანდო მომსახურების მიმწოდებლის ავტორიზებული პერსონალის მიერ. სუბიექტის ღია და დახურული გასაღების წყვილის შექმნის ოპერაციაში აუცილებელია მინიმუმ ორი ავტორიზებული პირის მონაწილეობა, სააგენტოს მიერ დამტკიცებული „მექანიკურ რეჟიმში გასაღების წყვილის შექმნისა და სერტიფიკატის გაცემის პროცედურის“ შესაბამისად.

4. გასაღების პარამეტრებია:

   ა) კრიპტოგრაფიული ალგორითმი - RSA;

   ბ) გასაღების სიგრძე - 2048 ბიტი.

5. სუბიექტის ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობა და სანდო მომსახურების მიმწოდებლის ინფრასტრუქტურაში ინტეგრირებული ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახი უნდა აკმაყოფილებდნენ შემდეგ მოთხოვნებს :

   ა) ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობა სერტიფიცირებულია არანაკლებ Common Criteria EAL 4+ ან/და არანაკლებ FIPS 140-2 Level 2 სტანდარტის მიხედვით;

   ბ) ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახი სერტიფიცირებულია FIPS 140-2 Level 3 სტანდარტის მიხედვით.

6. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღების ამოღება (ექსპორტირება) ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახიდან დასაშვებია მხოლოდ დაშიფრული ფორმით. გასაღების ამოღებას ან/და ნებისმიერ სხვა პროცედურას, რომლის შედეგადაც მიღებული იქნება გასაღები, ესაჭიროება სააგენტოს არანაკლებ ორი ავტორიზებული თანამშრომლის მონაწილეობა.

7. ბიომეტრიულ მონაცემთა შემგროვებლის დახურული გასაღები, პროგრამული უზრუნველყოფის ტექნიკური შეზღუდვების გამო, შესაძლებელია წარმოდგენილი იყოს ღია სახით. ამ შემთხვევაში გასაღების დაცვა კომპრომეტაციისგან უნდა მოხდეს ორგანიზაციული ღონისძიებების გამოყენებით, რაც მინიმუმ მოიცავს:

   ა) გასაღების არსებობა ღია სახით დასაშვებია მხოლოდ განცალკევებული და სპეციალურად ამ მიზნისთვის გამოყოფილი კომპიუტერის ოპერატიულ მეხსიერებაში;

   ბ) კომპიუტერი აღჭურვილი უნდა იყოს მუდმივად განახლებადი ანტივირუსული პროგრამული უზრუნველყოფით;

გ) დახურული გასაღები ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახიდან ამოღებული უნდა იყოს დაშიფრული ფორმით;

დ) კომპიუტერი უნდა ჩაირთოს უშუალოდ დეშიფრაციის პროცესის წინ და გამოირთოს პროცესის დასრულებისთანავე.

8. თუ ბიომეტრიული მონაცემების შემგროვებლის გასაღების წყვილი წარმოდგენილია ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახს გარეთ (მაგ., მატერიალური ფორმით), ის დაშიფრული უნდა იყოს 3TDEA, AES-128 (ან უფრო მაღალი) ან ეკვივალენტური სიძლიერის სიმეტრიული კრიპტოგრაფიული გასაღების გამოყენებით. აღნიშნული გასაღები უნდა გაიყოს რამდენიმე პირს შორის ისე, რომ დაცული იყოს წინამდებარე დოკუმენტით განსაზღვრული მონაწილე პირების აუცილებელი რაოდენობა.

9. ბიომეტრიული მონაცემების შემგროვებლის გასაღების წყვილის აქტივაციის მონაცემების სახეობა განისაზღვრება ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახის მწარმოებლის მიერ. აღნიშნული მონაცემები გაიცემა სააგენტოს უფლებამოსილ თანამშრომლებზე უსაფრთხოების აპარატურული მოდულის, მისი კონკრეტული უსაფრთხო სეგმენტის ან/და გამცემი შიფრაციის გასაღების წყვილის შექმნისას.

10. აქტივაციის მონაცემები იქმნება და ინახება ამ შინაგანაწესით და „მექანიკურ რეჟიმში გასაღების წყვილის შექმნისა და სერტიფიკატის გაცემის პროცედურის“ მოთხოვნების დაცვით.

11. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღების სარეზერვო ასლის შექმნა და შენახვა შესაძლებელია სანდო მომსახურების მიმწოდებლის ინფრასტრუქტურაში. სარეზერვო ასლი ინახება ძირითადი გასაღებისგან მოშორებით, რათა უზრუნველყოფილი იყოს მისი ხელმისაწვდომობა ორიგინალის დაზიანების შემთხვევაში.

12. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღების სარეზერვო ასლის შენახვა შეიძლება უსაფრთხოების აპარატურულ მოდულში, რომელიც განთავსებულია სააგენტოს მონაცემთა დამუშავების ცენტრში და სერტიფიცირებულია უსაფრთხოების იმავე ან უფრო მაღალი სტანდარტით, რაც წინამდებარე დოკუმენტით განისაზღვრება ბიომეტრიული მონაცემების დეშიფრაციის გასაღების უსაფრთხო სანახისათვის.

13. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღების სარეზერვო ასლი ასევე შესაძლებელია ინახებოდეს სანდო მომსახურების მიმწოდებლის დაცულ გარემოში განთავსებულ სეიფებში. ამ შემთხვევაში გასაღების შენახვა შეიძლება როგორც FIPS 140-2 Level 2 ან Common Criteria EAL 4+ სტანდარტით სერტიფიცირებულ გადასატან მატარებლებზე, ისე მატერიალური (ქაღალდზე დაბეჭდილი და დალუქულ კონვერტში მოთავსებული) ფორმით. მატერიალური ფორმით შენახვისას აუცილებელია გასაღების შიფრაცია იმგვარად, რომ მისი გამოყენება შესაძლებელი იყოს მხოლოდ წინამდებარე დოკუმენტით დადგენილი ტიპის აქტივაციის მონაცემების გამოყენებით.

14. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღების მიბარება მესამე პირისთვის შეიძლება მასთან დადებული ხელშეკრულების შესაბამისად, იმ პირობის დაცვით, რომ დახურული გასაღების ღია სახით მიღება (აღდგენა) შესაძლებელი იქნება მხოლოდ სანდო მომსახურების მიმწოდებლის არანაკლებ ორი ავტორიზებული თანამშრომლის მონაწილეობით.

15. ბიომეტრიული მონაცემების შემგროვებლის დახურული გასაღები მესამე პირს გადაეცემა ამ შინაგანაწესის 73-ე მუხლით დადგენილი წესით.

16. ბიომეტრიული მონაცემების შემგროვებლის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღები გადაეცემა მხოლოდ მესამე პირი არის კვალიფიციური სანდო მომსახურების მიმწოდებელი ან სერტიფიცირებულია სსტ ენ ისო/იეკ 27001:2017 / 2017, სსტ ისო/იეკ 27001:2013 / 2015 ან ISO/IEC 27001:2013 სტანდარტის მიხედვით.

17. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის დახურული გასაღების ბიომეტრიული მონაცემების შემგროვებელი სუბიექტისთვის გადაცემა დაუშვებელია.

18. დაუშვებელია ბიომეტრიული მონაცემების მიმღების დახურული გასაღების სარეზერვო ასლის მიღება ან/და მესამე პირისათვის მიბარება.

მუხლი 59. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების სერტიფიკატთან დაკავშირებული მომსახურების შეწყვეტა

1. სააგენტოს მიერ ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების სერტიფიკატთან დაკავშირებული მომსახურება წყდება:

   ა) სუბიექტის გარდაცვალებისას (ფიზიკური პირის შემთხვევაში);

   ბ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების სერტიფიკატების შენახვის მომსახურების შეწყვეტისა და დახურული გასაღების მესამე პირისთვის გადაცემასთან დაკავშირებით მომხმარებლის მოთხოვნის საფუძველზე;

გ) ამ შინაგანაწესით დადგენილი სერტიფიკატებისა და მასთან დაკავშირებული ინფორმაციის შენახვის ვადის ამოწურვის შემთხვევაში;

დ) სააგენტოს მიერ მომსახურების შეწყვეტის შემთხვევაში;

ე) სააგენტოს ლიკვიდაციის შემთხვევაში.

2. ამ მუხლის პირველი პუნქტის „დ“ და „ე“ ქვეპუნქტების შესაბამისად განსაზღვრული, სერტიფიკატთან დაკავშირებული მომსახურების შეწყვეტის შედეგები და ვალდებულებები დარეგულირდება საქართველოს კანონმდებლობის შესაბამისად.

მუხლი 60. განცხადება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმებაზე

1. სერტიფიკატი შესაძლოა გაუქმდეს:

ა) სუბიექტის განცხადების საფუძველზე;

ბ) სუბიექტის მოწყობილობის უვარგისად მიჩნევის შემთხვევაში;

გ) სერტიფიკატის ვადის გასვლის შემთხვევაში (უქმდება ავტომატურად);

დ) სერტიფიკატის მფლობელი იურიდიული პირის ლიკვიდაციის შემთხვევაში;

ე) სუბიექტის (ფიზიკური პირის) გარდაცვალების შემთხვევაში;

ვ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატში მითითებული ინფორმაციის ცვლილების შემთხვევაში;

ზ) თუ არსებობს სერტიფიკატის დახურული გასაღების კომპრომეტაციის საშიშროება ან ეჭვი;

თ) თუ სერტიფიკატის გაცემისას სააგენტომ დაუშვა შეცდომა, რის შედეგადაც შეუძლებელი ხდება სერტიფიკატის გამოყენება, ან/და სერტიფიკატში დატანილია არასწორი ინფორმაცია;

ი) ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის დახურული გასაღები გადაეცა მესამე პირს;

კ) საქართველოს კანონმდებლობით დადგენილ სხვა შემთხვევებში.

2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების მოთხოვნა შეუძლია სუბიექტს, სუბიექტის უფლებამოსილ წარმომადგენელს ან საქართველოს კანონმდებლობით დადგენილ შესაბამის უფლებამოსილ პირს.

3. შესაბამისი უფლებამოსილი პირი, ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების მოთხოვნით განცხადებით მიმართავს სააგენტოს. განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების შესახებ მოთხოვნას;

ბ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების მიზეზს;

ე) სუბიექტის სახელზე გაცემული კონკრეტული ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების საჭიროების შემთხვევაში, გასაუქმებელი სერტიფიკატის იდენტიფიკაციისთვის აუცილებელ ინფორმაციას (სერტიფიკატის სერიული ნომერი, სერტიფიკატის გაცემის თარიღი).

ვ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

4. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

5. მატერიალური ფორმით წარდგენილი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების სერტიფიკატის გაუქმების მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

6. სუბიექტს შეუძლია სააგენტოს დისტანციური მომსახურების სამსახურში ელექტრონული ფორმით წარადგინოს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის 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.

7. ამ მუხლის პირველი პუნქტის „დ“-„ი“ ქვეპუნქტებით განსაზღვრულ შემთხვევებში სერტიფიკატის გაუქმება შეიძლება მოითხოვოს სანდო მომსახურების მიმწოდებელმა.

მუხლი 61. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების შესახებ განცხადების განხილვა და გადაწყვეტილების მიღება

1. ამ შინაგანაწესის მე-60 მუხლის მე-2 და მე-7 პუნქტებით გათვალისწინებულ შემთხვევაში შესაბამისი განცხადების მიღების შემდეგ მარეგისტრირებელი ორგანო განიხილავს მას და იღებს გადაწყვეტილებას სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის თაობაზე.

2. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო ახორციელებს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაციას. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

   ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

   ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის მე-60 მუხლის მე-3 და მე-4 პუნქტებით დადგენილ მოთხოვნებს, გარდა მე-3 პუნქტის ,,ვ“ ქვეპუნქტისა;

   ბ) ამ მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 5 სამუშაო დღეს. სანდო მომსახურების მიმწოდებლის მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

5. ამ შინაგანაწესის მე-60 მუხლის მე-6 პუნქტით გათვალისწინებულ შემთხვევაში განცხადების მიღების შემდეგ დისტანციური მომსახურების სამსახური განიხილავს მას და იღებს გადაწყვეტილებას სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის თაობაზე.

6. დისტანციური მომსახურების სამსახური ახდენს სუბიექტის უფლებამოსილი წარმომადგენლის იდენტიფიკაციას და ავთენტიფიკაციას, სუბიექტის წარმომადგენლის (ასეთის არსებობის შემთხვევაში) ვინაობის და უფლებამოსილების შემოწმებას საქართველოს კანონმდებლობით დადგენილი წესით.

7. სუბიექტს შეიძლება უარი ეთქვას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმებაზე, თუ:

   ა) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი ვადაგასულია;

   ბ) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი უკვე გაუქმებულია;

   გ) სუბიექტის მიერ მოთხოვნილი გასაუქმებელი სერტიფიკატი არ არის გაცემული სააგენტოს მიერ;

   დ) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები ამ შინაგანაწესის მე-60 მუხლის მე-3 პუნქტის ,,ვ“ ქვეპუნქტის მოთხოვნების შესაბამისად ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა.

8. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმების ან გაუქმებაზე უარის თქმის შესახებ გადაწყვეტილება გამოიცემა სუბიექტის მიერ სერტიფიკატის გაუქმების მოთხოვნის სააგენტოში წარდგენიდან არაუგვიანეს მომდევნო სამუშაო დღისა.(ცვლილება 2021.06.07.N245/ს)

9. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი უქმდება ამ მუხლის მე-8 პუნქტით გათვალისწინებული გადაწყვეტილების მიღების დღეს.(ცვლილება 2021.06.07.N245/ს)

მუხლი 62. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაუქმება

1. ამ შინაგანაწესის მე-60 მუხლის მე-3 და მე-7 პუნქტების შესაბამისად მიღებული განცხადების საფუძველზე სერტიფიკატის გაუქმებასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს მარეგისტრირებელი ორგანო.

2. ამ შინაგანაწესის მე-60 მუხლის მე-6 პუნქტის შესაბამისად მიღებული განცხადების საფუძველზე სერტიფიკატის გაუქმებასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების შემთხვევაში, სერტიფიკატს აუქმებს დისტანციური მომსახურების სამსახური.

3. ამ მუხლის პირველი და მეორე პუნქტის შესაბამისად განსაზღვრული პირების მიერ სერტიფიკატის გაუქმების მოთხოვნა შესაძლებელია გადაეგზავნოს სერტიფიცირების ცენტრს, რომელიც, თავის მხრივ, ამ შინაგანაწესით დადგენილი წესის შესაბამისად აუქმებს სერტიფიკატს.

4. თუ ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის მომენტისათვის ფიქსირდება სხვაობა ამ შინაგანაწესის 54-ე მუხლის მე-2 და მე-3 პუნქტების შესაბამისად სუბიექტის მიერ მიღებულ განცხადებასა და სერტიფიკატის გაცემის მომენტისათვის სუბიექტის სახელზე გაცემული აქტიური სტატუსის მქონე ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის ამავე შინაგანაწესის 52-ე მუხლის პირველი პუნქტით განსაზღვრულ მონაცემებში, მაშინ მარეგისტრირებელი ორგანო აუქმებს განსხვავებული მონაცემებით არსებულ აქტიურ სერტიფიკატს ახალი სერტიფიკატის გაცემასთან დაკავშირებით დადებითი გადაწყვეტილების მიღების დღეს.

5. სერტიფიკატის გაუქმების შესახებ ინფორმაცია აღირიცხება ელექტრონულ ჟურნალში არანაკლებ 10 წლის ვადით.

6. სერტიფიკატის გაუქმების შესახებ ინფორმაცია ხელმისაწვდომია სერტიფიკატის გაუქმების შესახებ გადაწყვეტილების მიღებიდან არაუგვიანეს 60 წუთისა.

7. სერტიფიკატის გაუქმების შემდეგ მისი ხელახლა ამოქმედება დაუშვებელია.

მუხლი 63. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შეჩერება

ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის მოქმედების შეჩერება დაუშვებელია.

თავი VII

ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების წესი

მუხლი 64. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის სახელზე გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების და შესაბამისი სერტიფიკატის სააგენტოს ინფრასტრუქტურაში შენახვა გულისხმობს:
   ა) არაუფლებამოსილი პირის მიერ გამოყენების ან/და გამოყენების საფრთხისაგან დახურული გასაღების დაცვას, შესაბამისი აპარატურული, პროგრამული და/ან ორგანიზაციული მეთოდების გამოყენებით;
   ბ) დახურული გასაღების სარეზერვო ასლის შექმნას, დედნისაგან განცალკევებით შენახვას და არაუფლებამოსილი პირის მიერ გამოყენების ან/და გამოყენების საფრთხისაგან დაცვას, შესაბამისი აპარატურული, პროგრამული და/ან ორგანიზაციული მეთოდების გამოყენებით.
2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების და სერტიფიკატის შენახვის ერთი მომსახურების და, შესაბამისად, მისთვის დადგენილი ერთი საფასურის ფარგლებში, შესაძლებელია სააგენტოს მიერ გაცემული ნებისმიერი რაოდენობის სერტიფიკატების შენახვა.
3. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება ბიომეტრიული მონაცემების მიმღები სუბიექტის მოთხოვნის შემთხვევაში, გულისხმობს მოთხოვნილი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციას და შედეგად მიღებული ინფორმაციის მისთვის გადაცემას.

4. სანდო მომსახურების მიმწოდებელი დაშიფრული ბიომეტრიული მონაცემის დეშიფრაციას ახორციელებს მიუხედავად ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის სტატუსისა და კომპრომეტაციისა.

5. სანდო მომსახურების მიმწოდებელი დაშიფრული ბიომეტრიული მონაცემის დეშიფრაციას ახორციელებს ბიომეტრიული მონაცემების შემგროვებელი მომხმარებლის მიერ, ამ შინაგანაწესის N8 დანართის შესაბამისად, მოწოდებული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის საშუალებით.

6. ბიომეტრიული მონაცემების შემგროვებელი უზრუნველყოფს სანდო მომსახურების მიმწოდებლისთვის გადაცემული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის გამართული ფუნქციონირების მხარდაჭერას;

7. დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის გამოყენების პროცესში დეშიფრაციის ინსტრუმენტის გაუმართაობის შემთხვევაში, რაც შეიძლება გამოწვეული იყოს დეშიფრაციის ინსტრუმენტში გამოყენებულ ბიბლიოთეკებში (ბიომეტრიული მონაცემების დეშიფრაციის პროცესში გამოყენებული ელექტრონული ხელმოწერის შექმნის მოწყობილობის მწარმოებლის პროგრამული პაკეტები API Libraries) აღმოჩენილი ხარვეზებით და/ან გამოყენებული ბიბლიოთეკის არსებულ სისტემებთან შეუთავსებლობით და საჭიროებს ელექტრონული ხელმოწერის შექმნის მოწყობილობის მწარმოებლისგან ბიბლიოთეკების მიღებას (განახლების ჩათვლით) ან/და ლიცენზირებას, ბიომეტრიული მონაცემების შემგროვებელი სუბიექტი ვალდებულია, სააგენტოს წერილობითი მოთხოვნის შემთხვევაში, სადაც აღწერილი იქნება შეფერხების მიზეზი, მიაწოდოს მას შეფერხების აღმოფხვრისათვის მოთხოვნილი ინფორმაცია და ხარვეზის აღმოფხვრისთვის საჭირო საშუალებები.

8. დაშიფრული ბიომეტრიული მონაცემის დეშიფრაცია ხორციელდება ამ შინაგანაწესის 68-ე მუხლით განსაზღვრული წესის შესაბამისად.

9. ექსპერტიზის მიზნებისთვის, განსაკუთრებული კატეგორიის (ელექტრონული ხელმოწერის ბიომეტრიული მონაცემები) პერსონალური მონაცემების საქართველოს ფარგლებს გარეთ ექსპერტის ან/და საექსპერტო დაწესებულებისთვის მიწოდება დასაშვებია მხოლოდ „პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნების ნუსხის დამტკიცების თაობაზე“ პერსონალურ მონაცემთა დაცვის ინსპექტორის 2014 წლის 16 სექტემბრის N1 ბრძანების დანართით განსაზღვრულ, პერსონალურ მონაცემთა დაცვის სათანადო გარანტიების მქონე ქვეყნებში.

მუხლი 65. განცხადება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვასა და ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღებასთან დაკავშირებით

1. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვაზე და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღებაზე უფლებამოსილი პირია - იურიდიული პირი, რომელიც თავისი ფუნქციების შესრულებისას აგროვებს და დაშიფრული სახით ინახავს ბიომეტრიულ მონაცემებს, ამ დოკუმენტის საფუძველზე გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გამოყენებით.

2. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და სერტიფიკატის შენახვის და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღების მოთხოვნით განცხადებით მიმართავს სააგენტოს.

3. სუბიექტის მიერ წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

   ა) ამ შინაგანაწესის 64-ე მუხლით განსაზღვრული მომსახურებების მიღების შესახებ მოთხოვნას;
   ბ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
   გ) ხელმოწერის თარიღს;
   დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

4. წარდგენილ განცხადებას უნდა დაერთოს შემდეგი დოკუმენტები:

   ა) ამ შინაგანაწესის N9 დანართის შესაბამისად დამტკიცებული განცხადების დანართი;
   ბ) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

5. თუ სააგენტოს მიერ სუბიექტის სახელზე არ არის გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი, სუბიექტმა სერტიფიკატის გაცემასთან დაკავშირებული განცხადება უნდა წარადგინოს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების და შესაბამისი

სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღებასთან დაკავშირებით განცხადების წარდგენიდან 5 სამუშაო დღეში.

6. ამ მუხლის მე-4 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული დანართი სუბიექტის მიერ ივსება სააგენტოს ვებგვერდზე (www.sda.gov.ge) და მას შექმნისთანავე ენიჭება უნიკალური იდენტიფიკატორი. დანართის შექმნის შემდეგ მისი შინაარსის შეცვლა დაუშვებელია. აღნიშნული დანართის სააგენტოში წარდგენა შესაძლებელია მისი შექმნიდან ერთი თვის განმავლობაში.

7. მატერიალური ფორმით ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვაზე და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღებაზე მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

8. სუბიექტის წარმომადგენლობა სააგენტოში გულისხმობს მომსახურების მიღება-ჩაბარების აქტზე ხელმოწერის განხორციელებაზე უფლებამოსილების მინიჭებას.

მუხლი 66. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვაზე და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღებაზე განცხადების განხილვა და გადაწყვეტილების მიღება

1. თუ სააგენტოს მიერ სუბიექტის სახელზე გაცემულია ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი, განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების ამ შინაგანაწესით და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობას.

2. თუ სააგენტოს მიერ სუბიექტის სახელზე არ არის გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი, განცხადების მიღებისა და ამ შინაგანაწესის 64-ე მუხლის მე-5 პუნქტით განსაზღვრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემასთან დაკავშირებული განცხადების წარდგენის ვადის გასვლიდან არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების ამ შინაგანაწესით და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობას.

3. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო ახორციელებს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაციას. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:
   ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;
   ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

4. ამ მუხლის პირველი და მე-2 პუნქტებით განსაზღვრულ შემთხვევებში, მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას, თუ:
   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 65-ე მუხლით დადგენილ მოთხოვნებს, გარდა 65-ე მუხლის მე-3 პუნქტის ,,დ“ ქვეპუნქტისა;
   ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესით დადგენილ მოთხოვნებს;
   გ) ამ მუხლის მე-3 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

5. ამ მუხლის მე-4 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

6. სუბიექტს ეგზავნება შეტყობინება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვის და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების თანხის გადახდის თაობაზე. შეტყობინების ჩაბარებიდან 3 სამუშაო დღეში სუბიექტი ვალდებულია, გადაიხადოს კანონმდებლობით დადგენილი მომსახურების საფასური. აღნიშნულ ვადაში მომსახურების საფასურის გადახდის დამადასტურებელი დოკუმენტაციის წარდგენის შემთხვევაში, სააგენტო სუბიექტს აწვდის შესაბამის მომსახურებას.

7. ამ მუხლის მე-6 პუნქტით განსაზღვრული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ სუბიექტმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის

გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

8. ამ წესის 65-ე მუხლის მე-5 პუნქტით განსაზღვრულ შემთხვევაში, ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის, ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების და შესაბამისი სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების გაწევის გადაწყვეტილებები მიიღება ერთად.

9. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის ღია და დახურული გასაღების წყვილის შენახვა და მართვა ხორციელდება ამ შინაგანაწესით დადგენილი წესის შესაბამისად, ხოლო ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება ხორციელდება ამ შინაგანაწესის 67-ე და 68-ე მუხლებით დადგენილი წესის შესაბამისად.

10. სუბიექტს შეიძლება უარი ეთქვას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიწოდებაზე, თუ:
    ა) განცხადების დანართი წარდგენილია ამ შინაგანაწესის 65-ე მუხლის მე-6 პუნქტით დადგენილი მოთხოვნების დარღვევით;
    ბ) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 65-ე მუხლის მე-3 პუნქტის „დ“ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა;
    გ) სააგენტოს მიერ სუბიექტის სახელზე არ არის გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი, ამ წესის VI თავის შესაბამისად, არ მიმდინარეობს შიფრაციის სერტიფიკატის გაცემის საქმისწარმოება;
    დ) სუბიექტმა ამ მუხლის მე-6 პუნქტით დადგენილ ვადაში არ გადაიხადა საქართველოს კანონმდებლობით განსაზღვრული მომსახურების საფასური.

მუხლი 67. განცხადება ელექტრონული ხელმოწერის დაშიფრული ბიომეტრიული მონაცემების დეშიფრაციაზე

1. დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მოთხოვნა შეუძლია ბიომეტრიული მონაცემების მიმღებ სუბიექტს, რომელსაც, საქართველოს კანონმდებლობის შესაბამისად, გავლილი აქვს აკრედიტაცია სსტ ისო/იეკ 17025:2017 / 2017 ან ISO/IEC 17025:2017 სტანდარტის შესაბამისად და მისი აკრედიტაციის სფეროში შედის ხელნაწერი ტექსტები, ხელწერის საფუძველზე პიროვნების იდენტიფიკაცია.

2. ბიომეტრიული მონაცემების მიმღები სუბიექტი დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მოთხოვნის განცხადებით მიმართავს სააგენტოს. განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

    ა) დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის შესახებ მოთხოვნას;
    ბ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის მიღების შესახებ მოთხოვნას იმ შემთხვევაში, თუ სუბიექტზე არ არის გაცემული აქტიური სტატუსის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი;
    გ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
    დ) ხელმოწერის თარიღს;
    ე) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი);

    ვ) ექსპერტის ან/და საექსპერტო დაწესებულების უფლებამოსილი პირის საკონტაქტო ინფორმაციას (სახელი, გვარი, პირადი ნომერი, თანამდებობა, ელექტრონული ფოსტა და ტელეფონის ნომერი);

    ზ) იმ ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის უნიკალურ იდენტიფიკატორს (CA და SN), რომელიც გამოყენებული იყო გასაშიფრი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დროს ან იმ სუბიექტის დასახელებას, რომელმაც განახორციელა ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაცია და ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის კონკრეტულ თარიღსა და დროს.

3. წარდგენილ განცხადებას უნდა დაერთოს შემდეგი დოკუმენტები:

    ა) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი;
    ბ) ელექტრონული დოკუმენტიდან შესაბამისი პროგრამული უზრუნველყოფის საშუალებით ამოღებული, მხოლოდ დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემები;

გ) სუბიექტის მიერ შესაბამის სფეროში ექსპერტიზის განხორციელების უფლებამოსილების დამადასტურებელი ინფორმაცია და დოკუმენტაცია;

დ) სუბიექტის ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის ამ შინაგანაწესით გათვალისწინებული, სტანდარტებთან შესაბამისობის დამადასტურებელი დოკუმენტაცია იმ შემთხვევაში, თუ განმცხადებელზე არ არის გაცემული აქტიური სტატუსის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი.

4. მატერიალური ფორმით წარდგენილი დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის, მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, სუბიექტის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

მუხლი 68. განცხადების განხილვა და ელექტრონული ხელმოწერის დაშიფრული ბიომეტრიული მონაცემების დეშიფრაცია

1. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება ხორციელდება განცხადების წარდგენიდან 30 სამუშაო დღის ვადაში.

2. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების ამ შინაგანაწესით და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობას.

3. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო:
   ა) ამოწმებს სუბიექტის სარეგისტრაციო/საიდენტიფიკაციო მონაცემებს შესაბამის ორგანოებში;
   ბ) ამოწმებს სუბიექტის/სუბიექტის წარმომადგენლის ვინაობას და უფლებამოსილებას საქართველოს კანონმდებლობით დადგენილი წესით;
   გ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის შესაძლებლობის დადგენის მიზნით, ამ შინაგანაწესის 67-ე მუხლის მე-3 პუნქტის „ბ“ ქვეპუნქტის შესაბამისად, სუბიექტის მიერ მოწოდებულ ინფორმაციას აწვდის/უგზავნის სერტიფიკაციის ცენტრს;
   დ) ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის ამ შინაგანეწესით დადგენილ მოთხოვნებთან შესაბამისობის დადგენის მიზნით, ამ შინაგანაწესის 67-ე მუხლის მე-3 პუნქტის „დ“ ქვეპუნქტის შესაბამისად, სუბიექტის მიერ მოწოდებულ ინფორმაციას აწვდის/უგზავნის სერტიფიცირების ცენტრს.

4. მარეგისტრირებელი ორგანოდან, ამ მუხლის მე-3 პუნქტის „გ“ და „დ“ ქვეპუნქტების შესაბამისად მიღებული მოთხოვნის საფუძველზე, სერტიფიცირების ცენტრი ამოწმებს მიღებულ ინფორმაციას/მონაცემებს, ადგენს დაშიფრული ბიომეტრიული მონაცემების დეშიფრაციის შესაძლებლობისა და სუბიექტის ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის ამ შინაგანაწესით დადგენილ მოთხოვნებთან შესაბამისობას და მიღებულ შედეგსუგზავნის/აწვდის მარეგისტრირებელ ორგანოს.

5. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას, თუ:

   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 67-ე მუხლით დადგენილ მოთხოვნებს, გარდა 67-ე მუხლის მეორე პუნქტის ,,ე“ ქვეპუნქტისა;
   ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება საქართველოს კანონმდებლობისა და ამ შინაგანაწესით დადგენილ მოთხოვნებს.

6. ამ მუხლის მე-5 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

7. თუ ბიომეტრიული მონაცემების მიმღები სუბიექტის სახელზე არ არის გაცემული აქტიური სტატუსის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატი:

   ა) მარეგისტრირებელი ორგანო სუბიექტს უგზავნის წერილობით შეტყობინებას ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის წარმოდგენის თაობაზე. შეტყობინებაში მიეთითება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის წარმოდგენის დრო და ადგილი;
   ბ) სუბიექტი ვალდებულია, გამოცხადდეს სააგენტოს მიერ წინასწარ წერილობით განსაზღვრულ დროსა და ადგილას და წარმოადგინოს ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობა;
   გ) სერტიფიცირების ცენტრი ადგენს ბიომეტრიული მონაცემების დეშიფრაციის ინდივიდუალური მოწყობილობის განმცხადებლის მიერ სააგენტოში წარმოდგენილ დოკუმენტებთან შესაბამისობას და გასცემს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის სერტიფიკატს.

8. ამავე მუხლის მე-7 პუნქტით განსაზღვრული მომსახურების შემთხვევაში, თუ სუბიექტი არ გამოცხადდა სააგენტოში, განცხადება რჩება განუხილველი.

9. ამ მუხლის მე-7 პუნქტით განსაზღვრულ შემთხვევებში, ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის შეუძლებლობის დროს, სააგენტო უფლებამოსილია, დამატებით განსაზღვროს გამოვლენილი ხარვეზის აღმოფხვრის ვადა, გარდა ამ მუხლის მე-8 პუნქტით გათვალისწინებული შემთხვევისა. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში განცხადება რჩება განუხილველი.

10. ბიომეტრიული მონაცემების მიმღებ სუბიექტს დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემები მიეწოდება სანდო მომსახურების მიმწოდებლის მონაცემთა გაცვლის სერვერის მეშვეობით. მონაცემთა გაცვლის სერვერთან კომუნიკაცია ხორციელდება დახურული კერძო ქსელის (VPN) მეშვეობით.

11. მარეგისტრირებელი ორგანოს მიერ ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის შესახებ გადაწყვეტილება აღსასრულებლად ეგზავნება სერტიფიცირების ცენტრს, რომელიც უზრუნველყოფს:

    ა) სააგენტოს მონაცემთა გაცვლის სერვერზე სუბიექტისთვის სპეციალური საქაღალდის შექმნას და მონაცემთა გაცვლის სერვერთან დაკავშირებისათვის საჭირო ინფორმაციის სუბიექტისთვის მიწოდებას;

    ბ) დაშიფრული ბიომეტრიული მონაცემების დეშიფრაციას;

    გ) ბიომეტრიული მონაცემების მიმღებ სუბიექტზე გაცემული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის აქტიური სერტიფიკატის მეშვეობით დაშიფრვას;

    დ) გაშიფრული და დაშიფრული ბიომეტრიული მონაცემების SHA256 საკონტროლო ჯამის გენერაციას ისე, რომ შესაძლებელი იყოს კონკრეტული ბიომეტრიული მონაცემების დეშიფრაციის პროცესის და მიწოდების დადასტურება;

    ე) გაშიფრული და დაშიფრული ბიომეტრიული მონაცემების განადგურებას;

    ვ) ამ პუნქტის „გ“ ქვეპუნქტის შესაბამისად მიღებული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების მონაცემთა გაცვლის სერვერზე სუბიექტისთვის გამოყოფილ სპეციალურ საქაღალდეში განთავსებას;

    ზ) ამ პუნქტის „დ“ ქვეპუნქტის შესაბამისად მიღებული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების საკონტროლო ჯამის ელექტრონული ფოსტის მეშვეობით ამ შინაგანაწესის 67-ე მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტის შესაბამისად, სუბიექტის მიერ მითითებულ ელექტრონული ფოსტის მისამართზე მიწოდებას.

12. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემის დეშიფრაციისა და დეშიფრირებული ბიომეტრიული მონაცემების მიმღები სუბიექტისთვის მიწოდებასთან დაკავშირებით დგება მიღება-ჩაბარების აქტი, რომელსაც ხელს აწერს ამ შინაგანაწესის 67-ე მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტით განსაზღვრული პირი.

მუხლი 69. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მოთხოვნაზე უარის თქმის საფუძვლები

ბიომეტრიული მონაცემების შემგროვებელ სუბიექტს შეიძლება უარი ეთქვას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციაზე, თუ:

ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 67-ე მუხლის მე-2 პუნქტის ,,ე“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმდგენი პირის მონაცემები სხვადასხვაა;

ბ) შეუძლებელია სუბიექტის მიერ წარმოდგენილი, ელექტრონული დოკუმენტიდან ამოღებული, დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების გაშიფვრა.

მუხლი 70. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და სერტიფიკატის შენახვის და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტა

1. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის დახურული გასაღების შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურება წყდება:

    ა) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების გაწევის შეწყვეტისა და სუბიექტის სახელზე გაცემული შიფრაციის სერტიფიკატის დახურული გასაღების მესამე პირისთვის გადაცემის ან განადგურების შესახებ უფლებამოსილი პირის განცხადების საფუძველზე;

ბ) ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატებისა და მასთან დაკავშირებული ინფორმაციის შენახვის ვადის ამოწურვიდან 15 წლის გასვლის შემდეგ;
გ) სააგენტოს მიერ მომსახურების შეწყვეტის შემთხვევაში;
დ) სააგენტოს ლიკვიდაციის შემთხვევაში.

2. ამ მუხლის პირველი პუნქტის „გ“ და „დ“ ქვეპუნქტების შესაბამისად განსაზღვრული, სერტიფიკატთან დაკავშირებული მომსახურების შეწყვეტის წესები და პირობები განისაზღვრება „კვალიფიციური სანდო მომსახურების მიმწოდებლისთვის სავალდებულო ტექნიკური რეგლამენტის დამტკიცების შესახებ“ საქართველოს მთავრობის 2018 წლის 28 ივნისის N343 დადგენილების შესაბამისად.

მუხლი 71. განცხადება ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და სერტიფიკატის შენახვის და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტასთან დაკავშირებით

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტი ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტის მოთხოვნის განცხადებით მიმართავს სააგენტოს. განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტისა და სუბიექტის სახელზე გაცემული შიფრაციის სერტიფიკატის დახურული გასაღების მესამე პირისთვის გადაცემის ან განადგურების შესახებ მოთხოვნას;
ბ) სუბიექტის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
გ) ხელმოწერის თარიღს;
დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი);
ე) მესამე პირზე გადასაცემი ან გასანადგურებელი ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის სერიულ ნომერსა და სერტიფიკატის გაცემის თარიღს.

2. წარდგენილ განცხადებას უნდა დაერთოს შემდეგი დოკუმენტები:

ა) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი;
ბ) ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემის შემთხვევაში, მესამე პირის მიერ ამ შინაგანაწესის 58-ე მუხლის მე-16 პუნქტით განსაზღვრულ მოთხოვნებთან შესაბამისობის დამადასტურებელი ინფორმაცია და დოკუმენტაცია;
გ) ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემის შემთხვევაში, მესამე პირის მიერ სუბიექტის სახელზე შედგენილ წერილობით მიმართვას, რომელიც უნდა შეიცავდეს:
გ.ა) თანხმობას სუბიექტის სახელზე გაცემული ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მიბარებასთან/შენახვასთან დაკავშირებით;
გ.ბ) მესამე პირის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
გ.გ) ხელმოწერის თარიღს;
გ.დ) დაშიფრული სახით დახურული გასაღების ტრანსპორტირების მიზნით, სატრანსპორტო გასაღების პირველი ნაწილის მეურვე ფიზიკური პირის საიდენტიფიკაციო მონაცემებს (პირადი ნომერი, გვარი, სახელი და ელექტრონული ფოსტის მისამართი);
გ.ე) დაშიფრული სახით დახურული გასაღების ტრანსპორტირების მიზნით, სატრანსპორტო გასაღების მეორე ნაწილის მეურვე ფიზიკური პირის საიდენტიფიკაციო მონაცემებს (პირადი ნომერი, გვარი, სახელი და ელექტრონული ფოსტის მისამართი);
გ.ვ) დაშიფრული სახით დახურული გასაღების მიღების მიზნით, ფიზიკური პირის საიდენტიფიკაციო მონაცემებს (პირადი ნომერი, გვარი, სახელი და ელექტრონული ფოსტის მისამართი).

მუხლი 72. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და სერტიფიკატის შენახვის და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტასთან დაკავშირებით განცხადების განხილვა და გადაწყვეტილების მიღება

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტა და სუბიექტის სახელზე გაცემული შიფრაციის სერტიფიკატის დახურული გასაღების მესამე პირისთვის გადაცემა ან განადგურება ხორციელდება განცხადების წარდგენიდან 30 სამუშაო დღის ვადაში.

2. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების ამ შინაგანაწესით და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან შესაბამისობას.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას, თუ განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესითა და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს, გარდა შინაგანაწესის 71-ე მუხლის პირველი პუნქტის ,,დ“ ქვეპუნქტისა;

4. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში განცხადება რჩება განუხილველი.

5. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემის მოთხოვნის შემთხვევაში, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, სერტიფიცირების ცენტრი უზრუნველყოფს ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემის მიზნით 2 ნაწილად გაყოფილ AES ან 3DES სატრანსპორტო გასაღების გენერაციას.

6. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემის მიზნით:

   ა) მარეგისტრირებელი ორგანო ამ შინაგანაწესის 71-ე მუხლის მე-2 პუნქტის „გ.დ“ და „გ.ე“ ქვეპუნქტებით განსაზღვრული მესამე პირის უფლებამოსილ წარმომადგენლებს ცალ-ცალკე უგზავნის წერილობით შეტყობინებას ამ მუხლის მე-5 პუნქტის შესაბამისად შექმნილი სატრანსპორტო გასაღების გადაცემის თაობაზე. შეტყობინებაში მიეთითება სატრანსპორტო გასაღების გადაცემის დრო და ადგილი;

   ბ) მესამე პირის უფლებამოსილი წარმომადგენელი ვალდებულია, გამოცხადდეს სააგენტოს მიერ წინასწარ წერილობით განსაზღვრულ დროსა და ადგილას;

   გ) სერტიფიცირების ცენტრი ამ შინაგანაწესის 71-ე მუხლის მე-2 პუნქტის „გ.დ“ და „გ.ე“ ქვეპუნქტებით განსაზღვრული მესამე პირის უფლებამოსილ წარმომადგენლებს, გადასცემს სატრანსპორტო გასაღების შესაბამის ნაწილს და აფორმებს მიღება-ჩაბარების აქტს;

   დ) ამ მუხლის მე-6 პუნქტის „გ“ ქვეპუნქტში მითითებული მიღება-ჩაბარების აქტების გაფორმების შემდეგ ამ შინაგანაწესის 71-ე მუხლის მე-2 პუნქტის „გ.ვ“ ქვეპუნქტით განსაზღვრული მესამე პირის უფლებამოსილ წარმომადგენლებს უგზავნის წერილობით შეტყობინებას დაშიფრული სახით დახურული გასაღების გადაცემის თაობაზე. შეტყობინებაში მიეთითება დახურული გასაღების გადაცემის დრო და ადგილი;

   ე) ამ მუხლის მე-6 პუნქტის „გ“ ქვეპუნქტით განსაზღვრული მესამე პირის უფლებამოსილი წარმომადგენელი ვალდებულია, გამოცხადდეს სააგენტოს მიერ წინასწარ წერილობით განსაზღვრულ დროსა და ადგილას;

   ვ) სააგენტო ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურულ გასაღებს მესამე პირს გადასცემს ამ შინაგანაწესის 73-ე მუხლით დადგენილი წესის შესაბამისად;

   ზ) მარეგისტრირებელი ორგანო იღებს გადაწყვეტილებას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტის შესახებ და სუბიექტს წერილობითი შეტყობინების სახით უგზავნის მესამე პირზე დახურული გასაღების გადაცემის შესახებ ამ შინაგანაწესის 73-ე მუხლის მე-10 პუნქტის შესაბამისად გაფორმებულ მიღება-ჩაბარების აქტს.

7. ამ მუხლის მე-6 პუნქტით განსაზღვრულ შემთხვევაში, თუ მესამე პირის უფლებამოსილი წარმომადგენელი(ები) არ გამოცხადდა სააგენტოში, განცხადება რჩება განუხილველი.

8. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის მოთხოვნის შესაბამისად, მარეგისტრირებელი ორგანო იღებს გადაწყვეტილებას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტისა და სუბიექტის სახელზე გაცემული შიფრაციის სერტიფიკატის დახურული გასაღების განადგურების შესახებ.

9. სერტიფიცირების ცენტრი ამ მუხლის მე-8 პუნქტის შესაბამისად მიღებული გადაწყვეტილების მიღების შემდეგ აუქმებს სერტიფიკატს (საჭიროების შემთხვევაში) და ანადგურებს დახურულ გასაღებს როგორც სანახში, ისე მატერიალური ფორმით.

10. სუბიექტს შეიძლება უარი ეთქვას ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის შენახვისა და ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების შეწყვეტასა და სუბიექტის სახელზე გაცემული შიფრაციის სერტიფიკატის დახურული გასაღების მესამე პირისთვის გადაცემაზე ან განადგურებაზე, თუ:

    ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 71-ე მუხლის პირველი პუნქტის ,,დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმომდგენი პირის მონაცემები სხვადასხვაა;

ბ) სააგენტოს მიერ სუბიექტის სახელზე არ არის გაცემული სერტიფიკატი ან სააგენტო არ ახორციელებს იმ ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის მომსახურებას, რომლის მესამე პირზე გადაცემაც ან განადგურებაც მოითხოვა სუბიექტმა.

მუხლი 73. ბიომეტრიული მონაცემების დახურული გასაღების მესამე პირისთვის გადაცემა

1. მარეგისტრირებელი ორგანო სერტიფიცირების ცენტრს უგზავნის წერილობით შეტყობინებას ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირზე გადაცემასთან დაკავშირებით.

2. სერტიფიცირების ცენტრი ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების უსაფრთხო სანახიდან განახორციელებს სუბიექტის სახელზე გაცემული ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და სერტიფიკატის ამოღებას, რომელიც დაშიფრული იქნება ამ შინაგანაწესის 72-ე მუხლის მე-5 პუნქტით განსაზღვრული სატრანსპორტო გასაღების წყვილის მეშვეობით.

3. სერტიფიცირების ცენტრი ამ მუხლის მე-2 პუნქტით შესაბამისად მიღებულ სერტიფიკატსა და გასაღებს გადასცემს ამ შინაგანაწესის 72-ე მუხლის მე-2 პუნქტის „გ.ვ“ ქვეპუნქტით განსაზღვრული მესამე პირის უფლებამოსილ წარმომადგენელს.

4. სერტიფიკაციის ცენტრი აუქმებს სერტიფიკატს (საჭიროების შემთხვევაში) და ანადგურებს დახურულ გასაღებს როგორც სანახში, ისე მატერიალური ფორმით.

5. სუბიექტის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღების მესამე პირისთვის გადაცემასთან დაკავშირებით ფორმდება მიღება-ჩაბარების აქტი.

თავი VIII

დროის კვალიფიციური აღნიშვნის მომსახურების გაცემისა და მომსახურების წესი

მუხლი 74. დროის კვალიფიციური აღნიშვნის მომსახურების პირობები და გამოყენების წესი

1. დროის კვალიფიციური აღნიშვნა არის „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონით განსაზღვრული მომსახურება, რომელიც შეესაბამება ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ დადგენილ RFC 1361 სტანდარტს.

2. დროის კვალიფიციური აღნიშვნის მომსახურება, შეზღუდული წარმადობის პირობით, მუდმივად და უსასყიდლოდ ხელმისაწვდომია ნებისმიერი პირისთვის მისამართზე - http://tsa.cra.ge/signserver/tsa?workerName=qtsa - შემდეგი პირობებით:
   ა) დროის კვალიფიციური აღნიშვნის მომსახურებაზე მიმართვა არ მოითხოვს მომხმარებლების ავთენტიფიკაციას;
   ბ) დროის კვალიფიციური აღნიშვნის მომსახურება ხელმისაწვდომია RSA-2048 ტიპის გასაღებით;
   გ) ერთი მომხმარებლის მიერ ხუთ წამში ერთზე მეტი მოთხოვნის გამოგზავნის შემთხვევაში, სააგენტო უფლებას იტოვებს, შეზღუდოს ან სხვაგვარად შეაფერხოს მომსახურების მიწოდება.

3. იურიდიული პირებისათვის კვალიფიციური დროის აღნიშვნის მომსახურების გარანტირებული წარმადობით მიღება, ამ მუხლის მეორე პუნქტისგან განსხვავებული პირობებით, შესაძლებელია ამ შინაგანაწესის 76-ე მუხლით დადგენილი წესის შესაბამისად.

4. დროის კვალიფიციური აღმნიშვნელი თითოეული ერთეული დროის აღნიშვნის ტოკენს ხელს აწერს უნიკალური დახურული გასაღებით, რომელიც მხოლოდ ამ მიზნისთვის (დროის აღნიშვნის ტოკენზე ხელმოსაწერად) გამოიყენება. დროის კონკრეტულ მომენტში თითოეულ ერთეულზე აქტიურია მხოლოდ ერთი გასაღები.

5. დროის აღმნიშვნელი ერთეულის გასაღები და სერტიფიკატი იცვლება წელიწადში ერთხელ. დროის აღმნიშვნელი ერთეულის სერტიფიკატის მოქმედების ვადა შეადგენს 8 წელს. მოქმედი სერტიფიკატის გაცემის თარიღიდან 1 წლის განმავლობაში, არაუადრეს აღნიშნული ვადის ამოწურვამდე 21 დღისა, გენერირდება ახალი გასაღების წყვილი და მასზე გაიცემა სერტიფიკატი. დროის აღმნიშვნელი ერთეული დაუყოვნებლივ გადაირთვება ახალ სერტიფიკატზე/ახალ დახურულ გასაღებზე. პროცესი სრულდება წინა სერტიფიკატის შესაბამისი დახურული გასაღების უსაფრთხო განადგურებით, ამ შინაგანაწესის 78-ე მუხლის შესაბამისად.

6. დროის აღმნიშვნელი ერთეულების სერტიფიკატები გაიცემა სააგენტოს მიერ მართული, სპეციალურად ამ მიზნისთვის გამოყენებული ამ შინაგანაწესის მე-8 მუხლის მე-2 პუნქტის „ვ“ ქვეპუნქტით განსაზღვრული, სერტიფიკატის გამცემი დაქვემდებარებული ორგანოს მიერ. აღნიშნული ორგანო სერტიფიკატებს გასცემს მხოლოდ სააგენტოს მიერ მართულ დროის აღმნიშვნელ ერთეულებზე.

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 TSA <ნომერი>, სადაც <ნომერი> არის 01, 02 ... NN და წარმოადგენს დროის აღმნიშვნელი ერთეულის ნომერს.

8. დროის კვალიფიციური აღნიშვნის საერთაშორისო კოორდინირებული დროიდან (UTC) დასაშვები გადახრა შეადგენს მაქსიმუმ 1 წამს. გაცემული დროის აღნიშვნის ტოკენები ინახება შესაბამის ჟურნალში სააგენტოში დამტკიცებული "ღია გასაღების ინფრასტრუქტურის მედიის (ინფორმაციის მატარებლის) მართვის პროცედურის" შესაბამისად, რათა უზრუნველყოფილი იყოს ტოკენის სისწორის დადასტურება სანდო მომსახურების მიმწოდებლის მიერ.

9. დროის კვალიფიციური აღნიშვნის მომსახურება უნდა შეესაბამებოდეს ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ დადგენილ RFC 1361 სტანდარტს. მომსახურების მიღების დროს სასურველ ინფორმაციაზე დროის აღნიშვნის ტოკენის მისაღებად მომხმარებელი ვალდებულია, გამოიყენოს SHA-256 ალგორითმი ამ ინფორმაციის ჰეშირებისთვის.

10. დროის აღმნიშვნელი თითოეული ერთეული იყენებს მხოლოდ აქტიური სტატუსის მქონე სერტიფიკატებს.

11. მომსახურების უწყვეტობის მიზნით, სანდო მომსახურების მიმწოდებელი უზრუნველყოფს დროის კვალიფიციური აღმნიშვნელი 2 ან მეტი ერთეულის ფუნქციონირებას. დროის აღმნიშვნელი ერთეულები იყენებენ უნიკალურ გასაღებებს და მათი იდენტიფიცირება შესაძლებელია დროის აღნიშვნის ტოკენის განვითარებული ელექტრონული ხელმოწერისათვის გამოყენებული სერტიფიკატის მეშვეობით.

12. სააგენტო არ არის პასუხისმგებელი:
    ა) იმ პროგრამული ან/და აპარატურული სისტემების გაუმართავი მუშაობით გამოწვეულ ზიანზე, რომლებსაც მომხმარებლები ან/და კონტრაჰენტები გამოიყენებენ ტოკენის მოთხოვნის გასაგზავნად ან მიღებული ტოკენის სისწორის შესამოწმებლად;
    ბ) იმ მონაცემების შინაარსზე, რომლებიც შეიძლება მომხმარებელმა გამოგზავნოს მათზე დროის აღნიშვნის ტოკენის მიღების მიზნით;
    გ) დროის აღნიშვნის ტოკენის გაცემაზე იმ შემთხვევაში, თუ მოთხოვნა შემოსულია წინამდებარე დოკუმენტით დადგენილი ტექნიკური სტანდარტის დარღვევით;
    დ) ზიანზე, რომელიც მიადგა მხარეს იმ შემთხვევაში, თუ მან დროის აღნიშვნის ტოკენზე დაყრდნობამდე არ გადაამოწმა მისი სისწორე ამ მუხლის მე-13 პუნქტით განსაზღვრული წესით.

13. დროის აღმნიშვნელი ერთეულის ღია გასაღების გავრცელების მიზნით, შესაბამისი სერტიფიკატები ქვეყნდება ვებგვერდზე - www.id.ge. ისინი ასევე ხელმისაწვდომია დროის აღნიშვნის ტოკენის მეშვეობით.

14. დროის აღმნიშვნელი თითოეული ერთეულის ხელმოწერის სერტიფიკატის გაუქმების თაობაზე ინფორმაციის მიღება შესაძლებელია გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის ავტომატური შემოწმების მომსახურების მეშვეობით. სერტიფიკატის ავტომატური შემოწმების მომსახურება და მისი გამოყენების პირობები განისაზღვრება ამ შინაგანაწესის IX თავით დადგენილი წესის შესაბამისად.

მუხლი 75. ღია გასაღების ინფრასტრუქტურაში მონაწილე მხარეთა ვალდებულებები და პასუხისმგებლობები

1. წინამდებარე თავის მიზნებისათვის, სერტიფიცირების ცენტრი პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების გამართულ და უსაფრთხო მუშაობაზე, რაც მოიცავს:

    ა) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების უსაფრთხოებას, მათ შორის, შესაბამისი დახურული გასაღებისა და აქტივაციის მონაცემების დაცვას კომპრომეტირებისგან;
    ბ) დროის აღმნიშვნელი ორგანოს გამართულ და უსაფრთხო ფუნქციონირებას და წინამდებარე დოკუმენტით განსაზღვრული ფუნქციების შესაბამისად მარეგისტრირებელი ორგანოს მოთხოვნის დაკმაყოფილებას;
    გ) წინამდებარე დოკუმენტით განსაზღვრული სერტიფიკატის ავტომატური შემოწმების მომსახურების ხელმისაწვდომობას მომხმარებლისა და კონტრაჰენტებისათვის;
    დ) დროის აღმნიშვნელი ორგანოს მიერ დროის აღნიშვნის ტოკენზე ხელმოწერის ალგორითმების კრიპტოგრაფიული მდგრადობის მუდმივ მონიტორინგს. მათ დასუსტებაზე ეჭვის არსებობის შემთხვევაში, სერტიფიცირების ცენტრი მიმართავს შესაბამის ღონისძიებებს, რომლებიც სხვა მოქმედებებთან ერთად გულისხმობს უფრო მძლავრ კრიპტოგრაფიულ ალგორითმებზე გადასვლასაც.

2. წინამდებარე თავის მიზნებისათვის, მარეგისტრირებელი ორგანო ვალდებულია:

    ა) მიიღოს განცხადება მომხმარებლისთვის ამ შინაგანაწესის 74-ე მუხლის მე-3 პუნქტით გათვალისწინებული დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდებასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;

ბ) მიიღოს განცხადება მომხმარებლისთვის დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით შეწყვეტასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;

გ) შეამოწმოს განმცხადებლის უფლებამოსილება;

დ) მიიღოს გადაწყვეტილება მომხმარებლისთვის დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდებასთან ან შეწყვეტასთან დაკავშირებით;

ე) მიაწოდოს სერტიფიცირების ცენტრს მომხმარებლისთვის დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდებისა და შეწყვეტისათვის საჭირო სრულყოფილი და უტყუარი ინფორმაცია;

ვ) უზრუნველყოს მომხმარებლის ინფორმირება მისთვის დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით გამოყენების, მართვისა და უსაფრთხოების დაცვის შესახებ.

3. მომხმარებელი ვალდებულია, წინამდებარე შინაგანაწესის 76-ე მუხლის შესაბამისად დროის აღნიშვნის მომსახურების განარტირებული წარმადობით მიღების მიზნით, წარმოადგინოს შესაბამისი პოლიტიკით ან/და შინაგანაწესით მოთხოვნილი სწორი და სრულყოფილი ინფორმაცია, ასევე, დროულად განაახლოს აღნიშნული ინფორმაცია მისი ცვლილების შემთხვევაში.

4. წინამდებარე თავის მიზნებისათვის, მომხმარებელს უფლება აქვს, დროის აღნიშვნის მომსახურების მისაღებად გამოიყენოს ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც თავსებადია წინამდებარე დოკუმენტით განსაზღვრულ ტექნიკურ სტანდარტებთან.

5. წინამდებარე თავის მიზნებისათვის კონტრაჰენტი ვალდებულია, შეამოწმოს მიღებული დროის აღნიშვნის ტოკენი და გაეცნოს შესაბამისი სერტიფიკატის მოქმედი კანონმდებლობითა და წინამდებარე შინაგანაწესით დადგენილ გამოყენების პირობებს.

6. წინამდებარე თავის მიზნებისათვის, კონტრაჰენტი უფლებამოსილია:

ა) დროის აღნიშვნის ტოკენის სისწორის ავტომატურად დადასტურების მიზნით გამოიყენოს ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც თავსებადია წინამდებარე დოკუმენტით განსაზღვრულ ტექნიკურ სტანდარტებთან;

ბ) თუ დროის აღნიშვნის ტოკენზე არსებული კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის ვადის გასვლის და/ან კომპრომეტირების გამო ვერ ხერხდება დროის აღნიშვნის ტოკენის სისწორის დადასტურება ავტომატურ რეჟიმში, კონტრაჰენტს უფლება აქვს, აღნიშნული მომსახურების მისაღებად მიმართოს სააგენტოს.

მუხლი 76. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობები

1. დროის კვალიფიციური აღნიშვნის მომსახურება გარანტირებული წარმადობით განკუთვნილია მომხმარებლისთვის და მისი გამოყენება შესაძლებელია ნებისმიერი მიზნით, მომხმარებლის შეხედულებისამებრ.

2. დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდება ხდება შემდეგი პირობებით:

ა) მისამართი - http://tsa.cra.ge/signserver/tsa?workerName=qtsa;

ბ) დროის აღნიშვნის მომსახურება ხელმისაწვდომია RSA-2048 ტიპის გასაღებით;

გ) ერთ წამში მინიმალური გარანტირებული წარმადობაა 1 მოთხოვნა;

დ) კალენდარული დღის განმავლობაში სხვადასხვა გარანტირებული წარმადობა შესაძლებელია შეირჩეს დღის არაუმეტეს 3 მონაკვეთში, რომელთა ჯამიც უნდა შეადგენდეს 24 საათს;

ე) მომსახურების პერიოდში, მომხმარებლის მიერ კალენდარული კვირის განმავლობაში, ორშაბათიდან პარასკევის ჩათვლით, შერჩეული თითოეული დღის გარანტირებული წარმადობის კონფიგურაცია უნდა იყოს იდენტური, ხოლო შაბათსა და კვირას შესაძლებელია განსხვავებული კონფიგურაციით დღეების წარმადობების შერჩევა;

ვ) წინამდებარე პუნქტის „ე“ ქვეპუნქტში შერჩეული კალენდარული კვირის გარანტირებული წარმადობის კონფიგურაცია უცვლელი უნდა რჩებოდეს მომსახურების მთელი პერიოდის განმავლობაში;

ზ) მომსახურების ერთჯერადად მიღების მინიმალურ პერიოდს წარმოადგენს 30 კალენდარული დღე;

თ) დღის შერჩეული მონაკვეთის გარანტირებული წარმადობის მინიმალური პერიოდი შეადგენს 1 საათს;

ი) დროის კვალიფიციური აღნიშვნის მომსახურების 1 წამში მაქსიმალური გარანტირებული წარმადობაა 100 მოთხოვნა;

კ) ამ შინაგანაწესის 77-ე მუხლის მე-10 პუნქტით განსაზღვრულ გადაწყვეტილებაში მითითებული მომხმარებლის IP მისამართიდან;

ლ) მომსახურების პერიოდი განისაზღვრება გადახდილი თანხის ოდენობის შესაბამისად.

მუხლი 77. დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდების წესი

1. დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიღების მიზნით მომხმარებელი განცხადებით მიმართავს სააგენტოს. წარმოდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიღების შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
გ) ხელმოწერის თარიღს.

2. განცხადებას უნდა დაერთოს:
ა) ამ შინაგანაწესის N10 დანართით დამტკიცებული განცხადების დანართი;
ბ) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

3. მომხმარებელმა უნდა წარმოადგინოს საფასურის გადახდის დამადასტურებელი დოკუმენტი არაუგვიანეს განცხადების შეტანის დღისა.

4. ამ მუხლის მესამე პუნქტით განსაზღვრული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ მომხმარებელმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

5. ამ მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული დანართი მომხმარებლის მიერ ივსება სააგენტოს ვებგვერდზე (www.sda.gov.ge) და მას შექმნისთანავე ენიჭება უნიკალური იდენტიფიკატორი. დანართის შექმნის შემდეგ მისი შინაარსის შეცვლა დაუშვებელია. აღნიშნული დანართის სააგენტოში წარდგენა შესაძლებელია მისი შექმნიდან ერთი თვის განმავლობაში.

6. განცხადების მიღების შემდეგ არაუმეტეს 15 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესითა და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან.

7. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო ახორციელებს სუბიექტის (მისი წარმომადგენლის) იდენტიფიკაციას და ამოწმებს მის უფლებამოსილებას საქართველოს კანონმდებლობით დადგენილი წესით. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს და დაამუშაოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;
ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

8. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ მუხლის პირველი და მე-2 პუნქტებით დადგენილ მოთხოვნებს;
ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესითა და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებს;
გ) ამ მუხლის მე-7 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

9. ამ მუხლის მე-8 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. მარეგისტრირებელი ორგანოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

10. მომხმარებლის განცხადების შესაბამისობის დადგენის შემდგომ მარეგისტრირებელი ორგანო იღებს გადაწყვეტილებას დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით ხელმისაწვდომობის შესახებ, რომელიც უნდა შეიცავდეს, სულ მცირე:

ა) მომხმარებლის მიერ გადახდილი თანხის ოდენობას;
ბ) მომსახურების წარმადობის კონფიგურაციას;
გ) მომხმარებლის IP მისამართს, საიდანაც ხელმისაწვდომია მომსახურება;
დ) სააგენტოს ინტერნეტ მისამართს, რომელზეც ხელმისაწვდომია მომსახურება;
ე) მომსახურების დაწყების თარიღს;
ვ) მომსახურების დასრულების თარიღს.

11. ინფორმაციული ტექნოლოგიების მხარდაჭერის სამსახური, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, უზრუნველყოფს მომხმარებლის განცხადების შესაბამისად გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების მომხმარებლისთვის ხელმისაწვდომობას და დროის აღნიშვნის მომსახურებაზე მომხმარებლის წვდომისათვის საჭირო ინფორმაციის მარეგისტრირებელი ორგანოსთვის მიწოდებას (საჭიროების შემთხვევაში).

12. სააგენტო დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით ხელმისაწვდომობას უზრუნველყოფს ამ მუხლის მე-10 პუნქტით გათვალისწინებული გადაწყვეტილების გამოცემიდან 10 სამუშაო დღის ვადაში, განმცხადებლის მიერ გადახდილი მომსახურების საფასურის ოდენობის შესაბამისი პერიოდით.

13. მომხმარებელს შეიძლება უარი ეთქვას დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით გაწევაზე, თუ განცხადების დანართი წარდგენილია ამ მუხლის მე-5 პუნქტით დადგენილი მოთხოვნების დარღვევით.

14. შინაგანაწესის N10 დანართით განსაზღვრული სუბიექტის წარმომადგენლობა სააგენტოში გულისხმობს მომსახურების მიღება-ჩაბარების აქტზე ხელმოწერის უფლებამოსილების მინიჭებას.

მუხლი 78. დროის აღმნიშვნელი ერთეულის გასაღების წყვილის სასიცოცხლო ციკლი

1. დროის აღმნიშვნელი თითოეული ერთეულის გასაღების წყვილის გენერირება ხორციელდება „გასაღების წყვილის შექმნისა და სერტიფიკატის მექანიკურ რეჟიმში გაცემის პროცედურის“ შესაბამისად. გასაღების წყვილის გენერირება ხორციელდება უსაფრთხოების იმავე აპარატურული მოდულის საშუალებით, რომელსაც უშუალოდ იყენებს დროის აღმნიშვნელი ერთეული.

2. პირველი პუნქტით განსაზღვრული უსაფრთხოების აპარატურული მოდული სერტიფიცირებულია FIPS 140-2 Level 3 სტანდარტის მიხედვით.

3. დახურული გასაღები დაცულია არაავტორიზებული წვდომისგან. დახურული გასაღების სარეზერვო ასლის აღება ან მისი სხვაგვარად ექსპორტირება უსაფრთხოების აპარატურული მოდულიდან დაუშვებელია.

4. გასაღების წყვილის გენერირების დროს გამოიყენება ამ შინაგანაწესის 74-ე მუხლის მე-2 პუნქტის „ბ“ ქვეპუნქტით განსაზღვრული კრიპტოგრაფიული პარამეტრები.

5. დროის აღმნიშვნელი ერთეულის გასაღების წყვილის სასიცოცხლო ციკლის დასრულების შემდეგ აღნიშნული წყვილი უსაფრთხოდ ნადგურდება უსაფრთხოების აპარატურულ მოდულში.

მუხლი 79. დროის აღმნიშვნელ ერთეულთან დაკავშირებული უსაფრთხოების მოდულის სასიცოცხლო ციკლის მართვა

1. უსაფრთხოების აპარატურული მოდულის მოწოდებისა და შემდგომ ყოველდღიური ოპერირებისას პერიოდულად მოწმდება მწარმოებლის მიერ დადებული ლუქების მთლიანობა და ავთენტურობა.

2. უსაფრთხოების აპარატურული მოდულები განთავსებულია დაცულ, უსაფრთხო გარემოში და მათი ადმინისტრირება ხორციელდება ავტორიზებული პერსონალის მიერ.

3. უსაფრთხოების აპარატურული მოდულების საწარმო გარემოდან მოხსნის შემდეგ მასში არსებული ყველა გასაღები ნადგურდება მწარმოებლის ინსტრუქციების მიხედვით.

მუხლი 80. დროის აღნიშვნის ტოკენი

1. სანდო მომსახურების მიმწოდებელს გააჩნია ტექნიკური და ორგანიზაციული საშუალებები დროის აღნიშვნის ტოკენის უსაფრთხოდ გაცემისა და მასში ზუსტი დროის მითითებისათვის. წინამდებარე დოკუმენტით განსაზღვრული ზოგადი მოთხოვნების დასაკმაყოფილებლად თითოეული დროის აღნიშვნის ტოკენი იქმნება ETSI EN 319 422 სტანდარტის შესაბამისად და შეიცავს, სულ მცირე, შემდეგ ინფორმაციას:

    ა) მომხმარებლის მიერ მოწოდებულ მონაცემს (ჰეშკოდი), რომლისთვისაც გაიცემა დროის აღნიშვნა;
    ბ) დროის აღნიშვნის ტოკენის სერიულ ნომერს, რომელიც უნიკალურია, სულ მცირე, დროის აღმნიშვნელი ერთეულისათვის;
    გ) წინამდებარე დოკუმენტით განსაზღვრული BTSP პროფილის იდენტიფიკატორს;
    დ) დროს, არაუმეტეს 1 წამის სიზუსტით UTC-ს მიმართ, რომელიც დადგენილია, სულ მცირე, ერთი UTC(k) წყაროს მეშვეობით;
    ე) დროის აღმნიშვნელი ერთეულის მიერ განხორციელებულ კვალიფიციურ ელექტრონულ ხელმოწერას, შესრულებულს ექსკლუზიურად დროის აღნიშვნის ტოკენისათვის მის მიერ დროის აღნიშვნის მომსახურების გასაწევად შექმნილი დახურული გასაღებით;
    ვ) დროის აღნიშვნის მომსახურების გამცემი ორგანოს და დროის აღმნიშვნელი ერთეულის იდენტიფიკატორ(ებ)ს.

2. დროის აღნიშვნის ტოკენს სერიული ნომერი ენიჭება რიგითობის მიხედვით. თუმცა გარანტირებული არ არის ერთდროულად (ან პრაქტიკულად ერთდროულად) გაცემული დროის აღნიშვნის ტოკენების სერიული ნომრების რიგითობის დაცვა.

მუხლი 81. საათის სინქრონიზაცია UTC -სთან

1. დროის აღმნიშვნელი თითოეული ერთეულის საათი გასწორებულია UTC-სთან, არაუმეტეს 1 წამის ცდომილებით. სინქრონიზაცია ხორციელდება, სულ მცირე, ორი ალტერნატიული წყაროდან, მათ შორის, GPS-ის გამოყენებით. დროის აღმნიშველ ერთეულებზე საათი სწორდება ყოველდღიურად, დღეში 2-ჯერ მაინც. სინქრონიზაციის თითოეული ოპერაცია აღირიცხება შესაბამის ელექტრონულ ჟურნალში და მოგვიანებით არქივდება „ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“ შესაბამისად. დროის აღმნიშველი ერთეულის საათზე დროის ცვლილება შესაძლებელია მხოლოდ ორი ან მეტი ავტორიზებული პირის ერთდროული მონაწილეობით.

2. დროის აღმნიშველ თითოეულ ერთეულზე მიმდინარეობს დროის მუდმივი მონიტორინგი. UTC-ს მიმართ ამ პოლიტიკით დაშვებულზე მეტ ცდომილებას ავტომატურად აღმოაჩენს მონიტორინგის სისტემა და დროის აღნიშვნების გაცემა შეწყდება იმ დრომდე, სანამ დროის სიზუსტე არ აღდგება.

3. უფლებამოსილი ორგანოებისგან/ორგანიზაციებისგან მიღებული შეტყობინების საფუძველზე, დროის აღმნიშველი ორგანო თვალყურს ადევნებს ნაკიანი წამების გამოჩენას და რწმუნდება, რომ აღნიშნული ცვლილების შემთხვევაში, დროის სინქრონიზაცია UTC-სთან შენარჩუნებული იქნება ამ შინაგანაწესით განსაზღვრული დასაშვები სიზუსტით.

მუხლი 82. დროის აღმნიშველი ორგანოს კომპრომეტირება

1. დროის აღმნიშველი ორგანოს კომპრომეტირების შემთხვევაში, მომსახურების შეთანხმებული ხარისხით მიწოდება ხორციელდება სააგენტოს “ბიზნეს უწყვეტობის გეგმის“ შესაბამისად.

2. დროის აღმნიშველი ორგანოს კომპრომეტირების შემთხვევაში, სერტიფიცირების ცენტრი დაუყოვნებლივ აუქმებს დროის აღმნიშველი ორგანოს სერტიფიკატს.

მუხლი 83. დროის აღნიშვნის მომსახურების ინფორმაციის შენახვა

დროის აღნიშვნის მომსახურების ჩანაწერები ინახება სააგენტოში დამტკიცებული “ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“ მიხედვით. ჩანაწერები ინახება დაცულ გარემოში და ექვემდებარება პერიოდულ არქივირებას. აღნიშნული ჩანაწერები წარმოადგენს კონფიდენციალურ ინფორმაციას და მოიცავს შემდეგ მონაცემებს:

ა) დროის აღნიშვნის მოთხოვნებსა და შექმნილ დროის აღნიშვნის ტოკენებს;
ბ) დროის აღნიშვნის მომსახურებასთან დაკავშირებულ ხდომილებებს;
გ) დროის აღნიშვნის ერთეულის გასაღებებთან და სერტიფიკატებთან დაკავშირებულ ხდომილებებს.

მუხლი 84. დროის კვალიფიციური აღნიშვნის მომსახურების შეჩერება და შეწყვეტა

1. ამ შინაგანაწესის 74-ე მუხლის მე-2 პუნქტით გათვალისწინებული მომსახურება შეიძლება დროებით შეჩერდეს ან შეიზღუდოს:

ა) თუ მომსახურებაზე განხორციელდა კიბერშეტევა;

ბ) სააგენტოს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაში ადგილი აქვს ისეთ ტექნიკურ გაუმართაობას, რომელიც შეუძლებელს ხდის მომსახურების მიწოდებას.

2. ამ შინაგანაწესის 74-ე მუხლის მე-3 პუნქტით გათვალისწინებული მომსახურება შეიძლება დროებით შეჩერდეს, თუ მომსახურებაზე განხორციელდა კიბერშეტევა.

3. ამ შინაგანაწესის 74-ე მუხლის მე-3 პუნქტით გათვალისწინებული მომსახურება წყდება:

ა) უფლებამოსილი პირის განცხადების საფუძველზე;

ბ) მომსახურების ვადის ამოწურვის შემთხვევაში;

გ) საქართველოს კანონმდებლობით დადგენილ სხვა შემთხვევებში.

4. დროის კვალიფიციური აღნიშვნის მომსახურება წყდება სააგენტოს მიერ მომსახურების შეწყვეტის ან სააგენტოს ლიკვიდაციის შემთხვევაში. დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის შედეგები და ვალდებულებები დარეგულირდება საქართველოს კანონმდებლობის შესაბამისად.

5. მომხმარებლის მოთხოვნით გარანტირებული წარმადობით დროის კვალიფიციური აღნიშნვის მომსახურების შეჩერება დაუშვებელია.

მუხლი 85. განცხადება დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით შეწყვეტაზე

1. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის მოთხოვნა შეუძლია მომხმარებელს ან საქართველოს კანონმდებლობით დადგენილ უფლებამოსილ პირს.

2. შესაბამისი უფლებამოსილი პირი, გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის მოთხოვნით განცხადებით მიმართავს სააგენტოს.

3. სააგენტოში წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით შეწყვეტის შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

4. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

5. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის მატერიალური ფორმით მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, მომხმარებლის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

მუხლი 86. დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდების შეწყვეტა

1. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესის მოთხოვნებთან.

2. განცხადების განხილვის ფარგლებში მარეგისტრირებელი ორგანო უფლებამოსილია, განახორციელოს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაცია. მარეგისტრირებელი ორგანო, ასევე, უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 85-ე მუხლის მე-3 და მე-4 პუნქტებით დადგენილ მოთხოვნებს, გარდა 85-ე მუხლის მე-3 პუნქტის „დ“ ქვეპუნტისა;

ბ) ამ მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

5. განმცხადებელს შეიძლება უარი ეთქვას გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტაზე, თუ:

ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 85-ე მუხლის მე-3 პუნქტის „დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან

განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმომდგენი პირის მონაცემები სხვადასხვაა;

ბ) სააგენტო არ აწვდის განმცხადებელს შესაბამის მომსახურებას.

6. მომხმარებლისთვის დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიწოდება წყდება მარეგისტრირებელი ორგანოს მიერ შესაბამის გადაწყვეტილებაში მითითებული თარიღიდან, რომელიც არ უნდა აღემატებოდეს გადაწყვეტილების მიღებიდან 2 სამუშაო დღეს.

7. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის შემთხვევაში მომხმარებელი უფლებამოსილია, ხელახლა მიმართოს სააგენტოს შესაბამისი მომსახურების მიღების შესახებ განცხადებით.

მუხლი 87. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობების ცვლილება

1. დასაშვებია, შეიცვალოს გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შემდეგი პირობები:

ა) მომსახურების წარმადობის კონფიგურაცია;

ბ) მომხმარებლის IP მისამართი, რომლიდანაც ხელმისაწვდომია მომსახურება;

გ) მომსახურების ვადის გაგრძელება.

2. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობების ცვლილების მოთხოვნა შეუძლია იმ მომხმარებლის უფლებამოსილ წარმომადგენელს, რომელსაც სააგენტო უწევს შესაბამის მომსახურებას.

3. შესაბამისი უფლებამოსილი პირი, გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობების ცვლილების მოთხოვნით განცხადებით მიმართავს სააგენტოს.

4. სააგენტოში წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობების ცვლილების შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

5. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

6. ამ მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული პირობის ცვლილების შემთხვევაში, განმცხადებელმა უნდა წარმოადგინოს საფასურის გადახდის დამადასტურებელი დოკუმენტი არაუგვიანეს განცხადების შეტანის დღისა. აღნიშნული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ განმცხადებელმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

7. გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების შეწყვეტის მატერიალური ფორმით მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, მომხმარებლის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

8. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესის მოთხოვნებთან.

9. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო უფლებამოსილია, განახორციელოს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაცია. მარეგისტრირებელი ორგანო, ასევე, უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

10. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ მუხლის მე-4 პუნქტით დადგენილ მოთხოვნებს, ამ მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტისა;

ბ) ამ მუხლის მე-9 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

11. ამ მუხლის მე-10 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

12. განმცხადებელს შეიძლება უარი ეთქვას გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის მომსახურების პირობების ცვლილებაზე, თუ:

ა) სააგენტო არ აწვდის განმცხადებელს შესაბამის მომსახურებას;

ბ) ამ მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული პირობის ცვლილების შემთხვევაში, განმცხადებელმა არ გადაიხადა მომსახურების საფასური;

გ) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმომდგენი პირის მონაცემები სხვადასხვაა.

13. მომხმარებლისთვის გარანტირებული წარმადობით დროის კვალიფიციური აღნიშვნის შეცვლილი პირობებით მომსახურება ხორციელდება მარეგისტრირებელი ორგანოს მიერ შესაბამის გადაწყვეტილებაში მითითებული თარიღიდან, რომელიც არ უნდა აღემატებოდეს გადაწყვეტილების მიღებიდან 2 სამუშაო დღეს.

თავი IX

გაუქმებული სერტიფიკატების სიის ხელმისაწვდომობა და სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურება

მუხლი 88. გაუქმებული სერტიფიკატების სიის ხელმისაწვდომობის პირობები და გამოყენების წესი

1. გაუქმებული სერტიფიკატების სია ხელმისაწვდომია ნებისმიერი პირისთვის და მისი გამოყენება შესაძლებელია ნებისმიერი მიზნით, მომხმარებლის შეხედულებისამებრ.
2. გაუქმებული სერტიფიკატების სია, ამ შინაგანაწესით განსაზღვრული პირობებით, ხელმისაწვდომია მუდმივად და უსასყიდლოდ.
3. გაუქმებული სერტიფიკატების სია შექმნილია ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ დადგენილი RFC 5280 სტანდარტის მიხედვით და სერტიფიკატების გამცემი ორგანოების მიხედვით ქვეყნდება შემდეგ მისამართებზე:

ა) სერტიფიკატის გამცემი ძირითადი ორგანო „GEO Root CA“ - http://crl.cra.ge/georootca.crl;

ბ) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „GEO Signing CA G(n)“ - http://crl.cra.ge/geosigningcag(n).crl;

გ) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „GEO Authentication CA G(n)“- http://crl.cra.ge/geoauthenticationcag(n).crl;

დ) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „Biometric Encryption CA“ - http://crl.cra.ge/geobioencca.crl

ე)სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „SDA Time Stamping CA“ –

http://crl.cra.ge/sdatimestampingca.crl;

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

ზ) სერტიფიკატის გამცემი დაქვემდებარებული ორგანო „GEO Organizational Authentication CA G(n)“ – http://crl.cra.ge/geoorganizationalauthenticationcag(n).crl.“.

(ცვლილება 2021.06.07.N245/ს)

4. გამოქვეყნებული გაუქმებული სერტიფიკატების სიაში მითითებულია მომდევნო სიის გამოქვეყნების თარიღი, გარდა შესაბამისი სერტიფიკატების გამცემი ორგანოს მიერ გაუქმებული სერტიფიკატების სიის ბოლო გამოქვეყნების თარიღისა.

5. თუ სანდო მომსახურების მიმწოდებელი აუქმებს დროის კვალიფიციური აღნიშვნის, კვალიფიციური ელექტრონული ხელმოწერისა ან კვალიფიციური ელექტრონული შტამპის შესაბამისი სერტიფიკატების გამცემ ორგანოს, ამავე ორგანოების შესაბამისი გაუქმებული სერტიფიკატების ბოლო სიას შემდგომი გამოქვეყნების თარიღად მიეთითება მნიშვნელობა „99991231235959Z“ და ამით სიის გამოქვეყნების პროცესი სრულდება. სერტიფიკატების გამცემი ორგანოს ბოლო სიის გამოქვეყნება დასაშვებია მხოლოდ მის მიერ გაცემული ყველა სერტიფიკატის ვადის გასვლის ან გაუქმების შემდეგ. **(ცვლილება 2021.06.07.N245/ს)**

6. გაუქმებული სერტიფიკატების სია, გარდა ამ მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებული შემთხვევისა, ქვეყნდება ყოველდღიურად, წინა სიის გამოქვეყნებიდან არაუგვიანეს 24 საათისა. **(ცვლილება 2021.06.07.N245/ს)**

7. ამ მუხლის მე-3 პუნქტის „ა“ ქვეპუნქტით გათვალისწინებულ შემთხვევაში, გაუქმებული სერტიფიკატების სია ქვეყნდება ყოველ 4 თვეში ერთხელ, წინა სიის გამოქვეყნებიდან არაუგვიანეს 4 კალენდარული თვისა. **(ცვლილება 2021.06.07.N245/ს)**

8. გაუქმებული სერტიფიკატების სიის გამოქვეყნება შესაძლებელია ამ მუხლის მე-4 პუნქტით განსაზღვრული მისი შემდგომი გამოქვეყნების თარიღამდე.

9. გაუქმებული სერტიფიკატების სია ციფრულად ხელმოწერილია უშუალოდ სერტიფიკატების გამცემი ორგანოს მიერ.

10. ამ მუხლის მე-3 პუნქტის „ბ“, „ე“ და „ვ“ ქვეპუნქტით მითითებული სერტიფიკატების გამცემი ორგანოების შესაბამისი გაუქმებული სერტიფიკატების სიები შეიცავს ინფორმაციას ყველა იმ სერტიფიკატის შესახებ, რომლებიც გაიცა ამ ორგანოების მიერ და გაუქმდა მათი ვადის გასვლამდე, ხოლო დანარჩენი ორგანოების გაუქმებული სერტიფიკატების შესახებ ინფორმაცია სიიდან ამოიშლება მისი ვადის გასვლის შემდგომ.

11.გაუქმებული სერტიფიკატების სია ხელმისაწვდომია შემდეგი პირობების დაცვით:

ა) კალენდარული თვის განმავლობაში უზრუნველყოფილია მომსახურების უწყვეტობა არანაკლებ 99%-ით;

ბ) ერთი და იმავე ქსელური მისამართიდან დასაშვებია გაუქმებული სერტიფიკატების სიის ფაილის ჩამოტვირთვა წუთში ერთხელ;

გ) კალენდარული თვის განმავლობაში მომსახურების შეფერხების მაქსიმალური დასაშვები რაოდენობა შეადგენს შვიდს;

დ) ამ პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული შეფერხების მაქსიმალური ხანგრძლივობაა 90 წუთი. **(ცვლილება 2021.06.07.N245/ს)**

12. სააგენტო არ არის პასუხისმგებელი:
    ა) იმ პროგრამული ან/და აპარატურული სისტემების გაუმართავი მუშაობით მიყენებულ ზიანზე, რომლებსაც მომხმარებლები ან/და კონტრაჰენტები გამოიყენებენ გაუქმებული სერტიფიკატების სიის მისაღებად;
    ბ) ზიანზე, რომელიც მიადგა მხარეს იმ შემთხვევაში, თუ მან გაუქმებული სერტიფიკატების სიაზე დაყრდნობამდე არ გადაამოწმა ხელმოწერის ნამდვილობა.

მუხლი 89. სერტიფიკატის ავტომატური შემოწმების მომსახურების პირობები და გამოყენების წესი

1. სერტიფიკატის ავტომატური შემოწმების მომსახურება წარმოადგენს ინტერნეტის საინჟინრო სამუშაო ჯგუფის (Internet Engineering Task Force, IETF) მიერ დადგენილი RFC (Request for Comments) 6960 სტანდარტის მიხედვით შექმნილ მომსახურებას, რომელიც მოთხოვნის საფუძველზე გასცემს ინფორმაციას ელექტრონული ხელმოწერის, ავთენტიფიკაციისა და კრიპტოგრაფიული გასაღების სერტიფიკატების სტატუსის შესახებ, გარდა ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატისა.

2. ინფორმაცია სერტიფიკატის სტატუსის შესახებ ციფრულადაა ხელმოწერილი შესაბამისი სერტიფიკატის გამცემი ორგანოს მიერ საამისოდ გაცემული სპეციალური სერტიფიკატების მეშვეობით. ყველა ამ სერტიფიკატს, გარდა სერტიფიკატების გამცემი ძირითადი ორგანოს მიერ გაცემული სერტიფიკატისა, გააჩნია id-pkix-ocsp-nocheck გაფართოება. სერტიფიკატის გამცემი ძირითადი ორგანოს სერტიფიკატის სტატუსის გადამოწმება შესაძლებელია გაუქმებული სერტიფიკატების სიის მეშვეობით.

3. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურება განკუთვნილია ნებისმიერი პირისთვის და მისი გამოყენება შესაძლებელია ნებისმიერი მიზნით, მომხმარებლის შეხედულებისამებრ.

4. სერტიფიკატის ავტომატური შემოწმების მომსახურების მიღება, შეზღუდული წარმადობის პირობით, შესაძლებელია მუდმივად და უსასყიდლოდ შემდეგ მისამართზე http://ocsp.cra.ge/ocsp, შემდეგი პირობებით:

ა) სერტიფიკატის სტატუსის ავტომატურ რეჟიმში დადასტურების მომსახურებაზე მიმართვა არ მოითხოვს მომხმარებლების ავთენტიფიკაციას;

ბ) ერთი მომხმარებლის მიერ ხუთ წამში ერთზე მეტი მოთხოვნის გამოგზავნის შემთხვევაში, სააგენტო უფლებას იტოვებს, შეზღუდოს ან სხვაგვარად შეაფერხოს მომსახურების მიწოდება.

5. იურიდიული პირებისათვის, ამ მუხლის მე-4 პუნქტისგან განსხვავებული პირობებით, სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღება შესაძლებელია ამ შინაგანაწესის 91-ე მუხლით დადგენილი წესის შესაბამისად.

6. სერტიფიკატის ავტომატური შემოწმების მომსახურების საშუალებით გაუქმებულ სერტიფიკატებზე ინფორმაციის მიღება შესაძლებელია სერტიფიკატის გამცემი ორგანოს მიერ სერტიფიკატის გაუქმებიდან არაუმეტეს 10 წუთის შემდეგ.

7. სერტიფიკატის ავტომატური შემოწმების მომსახურება არ ითვალისწინებს სერტიფიკატების შესახებ ინფორმაციის გაცემას სერტიფიკატების ვადის გასვლის შემდეგ, გარდა ამავე მუხლის მე-8 პუნქტით განსაზღვრული ორგანოების მიერ გაცემული სერტიფიკატებისა. სერტიფიკატის ვადის გასვლის შემდგომ მისი სტატუსის შესახებ ინფორმაციის მიღება შესაძლებელია მხოლოდ სააგენტოსთვის წერილობით მიმართვის გზით. ასეთ შემთხვევაში, ინფორმაცია გაიცემა სერტიფიკატის სასიცოცხლო ციკლის ოპერაციების აღრიცხვის ჩანაწერებზე დაყრდნობით.

8. სერტიფიკატის ავტომატური შემოწმების მომსახურება ითვალისწინებს 88-ე მუხლის მე-3 პუნქტის „ბ“, „ე“ და „ვ“ ქვეპუნქტებში განსაზღვრული სერტიფიკატის გამცემი ორგანოების მიერ გაცემული სერტიფიკატების სტატუსის შესახებ ინფორმაციის გაცემას ამავე ორგანოების მიერ გაცემული სერტიფიკატების ვადის გასვლის შემდგომ.

9. თუ ის მიმწოდებლი აუქმებს კვალიფიციური ელექტრონული ხელმოწერისა ან კვალიფიციური ელექტრონული შტამპის შესაბამისი სერტიფიკატების გამცემ ორგანოს, ამავე ორგანოების მიერ გაცემული სერტიფიკატების სტატუსის შემოწმება შესაძლებელია მხოლოდ გაუქმებუილი სერტიფიკატების სიის მეშვეობით.

10. სანდო მომსახურების მიმწოდებელი არ არის პასუხისმგებელი:

ა) იმ პროგრამული ან/და აპარატურული სისტემების გაუმართავი მუშაობით მიყენებულ ზიანზე, რომლებსაც მომხმარებლები ან/და კონტრაჰენტები გამოიყენებენ სერტიფიკატის სტატუსის ავტომატურ რეჟიმში შესამოწმებლად;

ბ) სერტიფიკატის სტატუსის შესახებ ინფორმაციის გაცემაზე იმ შემთხვევაში, თუ მოთხოვნა შემოსულია წინამდებარე დოკუმენტის მიერ დადგენილი ტექნიკური სტანდარტის დარღვევით;

გ) ზიანზე, რომელიც მიადგა მხარეს იმ შემთხვევაში, თუ მან მიღებულ ინფორმაციაზე დაყრდნობამდე არ გადაამოწმა ხელმოწერის ვალიდურობა.

11. სერტიფიკატის ავტომატური შემოწმების მომსახურება ხელმისაწვდომია შემდეგი პირობების დაცვით:

ა) კალენდარული თვის განმავლობაში უზრუნველყოფილია მომსახურების უწყვეტობა არანაკლებ 99%-ით;

ბ) კალენდარული თვის განმავლობაში მომსახურების შეფერხების მაქსიმალური დასაშვები რაოდენობა შეადგენს შვიდს;

გ) ამ პუნქტის „ბ“ ქვეპუნქტით გათვალისწინებული შეფერხების მაქსიმალური ხანგრძლივობაა 90 წუთი. **(ცვლილება 2021.06.07.N245/ს)**

მუხლი 90. ღია გასაღების ინფრასტრუქტურაში მონაწილე მხარეთა ვალდებულებები და პასუხისმგებლობები

1. წინამდებარე თავის მიზნებისათვის, სერტიფიცირების ცენტრი პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების გამართულ და უსაფრთხო მუშაობაზე, რაც მოიცავს:

ა) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების უსაფრთხოების უზრუნველყოფას, მათ შორის, შესაბამისი დახურული გასაღებისა და აქტივაციის მონაცემების დაცვას კომპრომეტირებისგან;

ბ) წინამდებარე დოკუმენტით განსაზღვრული, გაუქმებული სერტიფიკატების სიის წარმოებას და ხელმისაწვდომობას მომხმარებლისა და კონტრაჰენტებისათვის, ამ დოკუმენტით განსაზღვრულ ფარგლებში;

გ) წინამდებარე დოკუმენტით განსაზღვრული, სერტიფიკატის ავტომატური შემოწმების მომსახურების ხელმისაწვდომობას მომხმარებლისა და კონტრაჰენტებისათვის, ამ დოკუმენტით განსაზღვრულ ფარგლებში;

დ) სერტიფიკატის სტატუსის წარმოებას.

2. წინამდებარე თავის მიზნებისათვის, მარეგისტრირებელი ორგანო ვალდებულია:

ა) განიხილოს განცხადება მომხმარებლისთვის ამ შინაგანაწესის 89-ე მუხლის მე-5 პუნქტით გათვალისწინებული გარანტირებული წარმადობით სერტიფიკატის ავტომატური შემოწმების მომსახურების მიწოდებასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;

ბ) განიხილოს განცხადება მომხმარებლისთვის სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით შეწყვეტასთან ან მომსახურების პირობების ცვლილებასთან დაკავშირებით და უზრუნველყოს განმცხადებლის იდენტიფიკაცია და ავთენტიფიკაცია;

გ) შეამოწმოს განმცხადებლის უფლებამოსილება;

დ) მიიღოს გადაწყვეტილება მომხმარებლისთვის სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიწოდებასთან, მომსახურების პირობების შეცვლასთან ან შეწყვეტასთან დაკავშირებით;

ე) მიაწოდოს სერტიფიკაციის ცენტრს მომხმარებლისთვის სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიწოდებისა და შეწყვეტისათვის საჭირო სრულყოფილი და უტყუარი ინფორმაცია.

3. მომხმარებელი ვალდებულია, წინამდებარე შინაგანაწესის 91-ე მუხლის შესაბამისად სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების მიზნით, წარმოადგინოს შესაბამისი პოლიტიკით ან/და შინაგანაწესით მოთხოვნილი სწორი და სრულყოფილი ინფორმაცია და დროულად განაახლოს აღნიშნული ინფორმაცია მისი ცვლილების შემთხვევაში.

4. წინამდებარე თავის მიზნებისათვის, მომხმარებელს უფლება აქვს, სერტიფიკატის ავტომატური შემოწმების მომსახურების მისაღებად გამოიყენოს ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც თავსებადია წინამდებარე დოკუმენტით განსაზღვრულ ტექნიკურ სტანდარტებთან.

5. წინამდებარე თავის მიზნებისათვის, კონტრაჰენტი ვალდებულია, შეამოწმოს სერტიფიკატის ავტომატური შემოწმების მომსახურებით მიღებული პასუხის ხელმოწერის ვალიდურობა, რომლის საშუალებითაც ჩატარებულია შესაბამისი ოპერაცია, და გაეცნოს შესაბამისი სერტიფიკატის მოქმედი კანონმდებლობითა და ამ შინაგანაწესით დადგენილ გამოყენების პირობებს.

6. წინამდებარე თავის მიზნებისათვის, კონტრაჰენტი უფლებამოსილია:

ა) სერტიფიკატის ავტომატური შემოწმების მომსახურებით მიღებული პასუხის სისწორის ავტომატურ რეჟიმში დადასტურების მიზნით, გამოიყენოს ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც თავსებადია წინამდებარე დოკუმენტით განსაზღვრულ ტექნიკურ სტანდარტებთან;

ბ) თუ სერტიფიკატის ავტომატური შემოწმების მომსახურებით მიღებულ პასუხზე ელექტრონული ხელმოწერის სერტიფიკატის ვადის გასვლის და/ან კომპრომეტირების გამო, ვერ ხერხდება სერტიფიკატის ავტომატური შემოწმების მომსახურებით მიღებული პასუხის სისწორის დადასტურება ავტომატურ რეჟიმში, კონტრაჰენტს უფლება აქვს, აღნიშნული მომსახურების მისაღებად მიმართოს სააგენტოს.

მუხლი 91. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების პირობები

1. გარანტირებული წარმადობით სერტიფიკატის ავტომატური შემოწმების მომსახურება განკუთვნილია მომხმარებლისთვის და მისი გამოყენება შესაძლებელია ნებისმიერი მიზნით, მომხმარებლის შეხედულებისამებრ.

2. სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიწოდება ხდება შემდეგი პირობებით:

ა) მისამართი - http://ocsp.cra.ge/ocsp;

ბ) ერთ წამში მინიმალური გარანტირებული წარმადობაა 1 მოთხოვნა;

გ) კალენდარული დღის განმავლობაში სხვადასხვა გარანტირებული წარმადობა შესაძლებელია შეირჩეს დღის არაუმეტეს 3 მონაკვეთში, რომელთა ჯამიც უნდა შეადგენდეს 24 საათს;

დ) მომსახურების პერიოდში, მომხმარებლის მიერ კალენდარული კვირის განმავლობაში, ორშაბათიდან პარასკევის ჩათვლით, შერჩეული თითოეული დღის გარანტირებული წარმადობის კონფიგურაცია უნდა იყოს იდენტური, ხოლო შაბათსა და კვირას შესაძლებელია განსხვავებული კონფიგურაციით დღეების წარმადობების შერჩევა;

ე) ამ პუნქტის „დ“ ქვეპუნქტში შერჩეული კალენდარული კვირის გარანტირებული წარმადობის კონფიგურაცია უცვლელი უნდა რჩებოდეს მომსახურების მთელი პერიოდის განმავლობაში;

ვ) მომსახურების ერთჯერადად მიღების მინიმალურ პერიოდს წარმოადგენს 30 კალენდარული დღე;

ზ) დღის შერჩეული მონაკვეთის გარანტირებული წარმადობის მინიმალური პერიოდი შეადგენს 1 საათს;

თ) სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების 1 წამში მაქსიმალური გარანტირებული წარმადობაა 100 მოთხოვნა;

ი) მომსახურება შესაძლებელია ამ შინაგანაწესის 92-ე მუხლის მე-10 პუნქტით განსაზღვრულ გადაწყვეტილებაში მითითებული მომხმარებლის IP მისამართიდან;

კ) მომსახურების პერიოდი განისაზღვრება გადახდილი თანხის ოდენობის შესაბამისად.

მუხლი 92. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების წესი

1. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების მიზნით, მომხმარებელი განცხადებით მიმართავს სააგენტოს მიმწოდებელს. წარმოდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:
   ა) სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების შესახებ მოთხოვნას;
   ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;
   გ) ხელმოწერის თარიღს.

2. განცხადებას უნდა დაერთოს:
   ა) ამ შინაგანაწესის N11 დანართით დამტკიცებული განცხადების დანართი;
   ბ) განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

3. მომხმარებელმა უნდა წარმოადგინოს საფასურის გადახდის დამადასტურებელი დოკუმენტი არაუგვიანეს განცხადების შეტანის დღისა.

4. ამ მუხლის მესამე პუნქტით განსაზღვრული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ მომხმარებელმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სადო მომსახურების მიმწოდებელი უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

5. ამ მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტით განსაზღვრული დანართი მომხმარებლის მიერ ივსება სააგენტოს ვებგვერდზე (www.sda.gov.ge) და მას შექმნისთანავე ენიჭება უნიკალური იდენტიფიკატორი. დანართის შექმნის შემდეგ მისი შინაარსის შეცვლა დაუშვებელია. აღნიშნული დანართის სააგენტოში წარდგენა შესაძლებელია მისი შექმნიდან ერთი თვის განმავლობაში.

6. განცხადების მიღების შემდეგ არაუმეტეს 15 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესითა და საქართველოს კანონმდებლობით დადგენილ მოთხოვნებთან.

7. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო ახორციელებს სუბიექტის (მისი წარმომადგენლის) იდენტიფიკაციას და უფლებამოსილების შემოწმებას საქართველოს კანონმდებლობით დადგენილი წესით. მარეგისტრირებელი ორგანო უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს და დაამუშაოს შემდეგი ინფორმაცია:

   ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;
   ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

8. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

   ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ მუხლის პირველი, მე-2 და მე-3 პუნქტებით დადგენილ მოთხოვნებს;
   ბ) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესითა და საქართველოს მოქმედი კანონმდებლობით დადგენილ მოთხოვნებს;
   გ) ამ მუხლის მე-7 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

9. ამ მუხლის მე-8 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. მარეგისტრირებელი ორგანოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

10. მომხმარებლის განცხადების შესაბამისობის დადგენის შემდგომ მარეგისტრირებელი ორგანო იღებს გადაწყვეტილებას სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით ხელმისაწვდომობის შესახებ, რომელიც უნდა შეიცავდეს, სულ მცირე:

   ა) მომხმარებლის მიერ გადახდილი თანხის ოდენობას;
   ბ) მომსახურების წარმადობის კონფიგურაციას;
   გ) მომხმარებლის IP მისამართს, რომლიდანაც ხელმისაწვდომია მომსახურება;
   დ) სააგენტოს ინტერნეტმისამართს, რომელზეც ხელმისაწვდომია მომსახურება;
   ე) მომსახურების დაწყების თარიღს;
   ვ) მომსახურების დასრულების თარიღს.

11. ინფორმაციული ტექნოლოგიების მხარდაჭერის სამსახური, მარეგისტრირებელი ორგანოდან მიღებული მოთხოვნის საფუძველზე, უზრუნველყოფს მომხმარებლის განცხადების შესაბამისად გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების მომხმარებლისთვის ხელმისაწვდომობას და დროის აღნიშვნის მომსახურებაზე მომხმარებლის წვდომისათვის საჭირო ინფორმაციის მარეგისტრირებელი ორგანოსთვის მიწოდებას (საჭიროების შემთხვევაში).

12. სააგენტო სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით ხელმისაწვდომობას უზრუნველყოფს ამ მუხლის მე-10 პუნქტით გათვალისწინებული გადაწყვეტილების გამოცემიდან 10 სამუშაო დღის ვადაში, მომხმარებლის მიერ გადახდილი მომსახურების საფასურის ოდენობის შესაბამისი პერიოდით.

13. მომხმარებელს შეიძლება უარი ეთქვას სერტიფიკატის სტატუსის ავტომატური შემოწმების გარანტირებული წარმადობით მომსახურებაზე, თუ განცხადების დანართი წარდგენილია ამ მუხლის მე-5 პუნქტით დადგენილი მოთხოვნების დარღვევით.

14. ამ შინაგანაწესის N11 დანართით განსაზღვრული სუბიექტის წარმომადგენლობა სააგენტოში გულისხმობს მომსახურების მიღება-ჩაბარების აქტზე ხელმოწერის განხორციელებაზე უფლებამოსილების მინიჭებას.

მუხლი 93. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების ინფორმაციის შენახვა

სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების ჩანაწერები ინახება სააგენტოში დამტკიცებული "ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის" მიხედვით. ჩანაწერები ინახება დაცულ გარემოში და ექვემდებარება პერიოდულ არქივირებას. აღნიშნული ჩანაწერები წარმოადგენს კონფიდენციალურ ინფორმაციას და მოიცავს შემდეგ მონაცემებს:

ა) სერტიფიკატის სტატუსის ავტომატური შემოწმების მოთხოვნებსა და დაბრუნებულ პასუხს;
ბ) სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურებასთან დაკავშირებულ ხდომილებებს.

მუხლი 94. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეჩერებისა და შეწყვეტის საფუძვლები

1. ამ შინაგანაწესის 89-ე მუხლის მე-4 პუნქტით გათვალისწინებული მომსახურება შეიძლება დროებით შეჩერდეს ან შეიზღუდოს:

ა) თუ მომსახურებაზე განხორციელდა კიბერშეტევა;

ბ) სააგენტოს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურაში არსებული ტექნიკური გაუმართაობისას, რომელიც შეუძლებელს ხდის მომსახურებას.

2. ამ შინაგანაწესის 89-ე მუხლის მე-5 პუნქტით გათვალისწინებული მომსახურება შეიძლება დროებით შეჩერდეს, თუ მომსახურებაზე განხორციელდა კიბერშეტევა.

3. ამ შინაგანაწესის 89-ე მუხლის მე-5 პუნქტით გათვალისწინებული მომსახურება წყდება:

ა) უფლებამოსილი პირის განცხადების საფუძველზე;

ბ) მომსახურების ვადის ამოწურვის შემთხვევაში;

გ) საქართველოს კანონმდებლობით დადგენილ სხვა შემთხვევებში.

4. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურება წყდება სააგენტოსმიერ მომსახურების შეწყვეტის ან სააგენტოს ლიკვიდაციის შემთხვევაში. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის შედეგები და ვალდებულებები დარეგულირდება საქართველოს კანონმდებლობის შესაბამისად.

5. მომხმარებლის მოთხვნით გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეჩერება დაუშვებელია.

მუხლი 95. განცხადება გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტაზე

1. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის მოთხოვნა შეუძლია მომხმარებლის უფლებამოსილ წარმომადგენელს ან საქართველოს კანონმდებლობით დადგენილ შესაბამის უფლებამოსილ პირს.

3. შესაბამისი უფლებამოსილი პირი, გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის მოთხოვნით განცხადებით მიმართავს სააგენტოს.

4. სააგენტოში წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

5. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

6. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის მატერიალურად შედგენილი განცხადება, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, მომხმარებლის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

მუხლი 96. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტა

1. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესის მოთხოვნებთან.

2. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო უფლებამოსილია, განახორციელოს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაცია. მარეგისტრირებელი ორგანო, ასევე, უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

3. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ შინაგანაწესის 95-ე მუხლის მე-4 და მე-5 პუნქტებით დადგენილ მოთხოვნებს, გარდა 95-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნტისა;

ბ) ამ მუხლის მე-2 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

4. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

5. განმცხადებელს შეიძლება უარი ეთქვას გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტაზე, თუ:

ა) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ შინაგანაწესის 95-ე მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმომდგენი პირის მონაცემები სხვადასხვაა;

ბ) სააგენტო არ აწვდის განმცხადებელს შესაბამის მომსახურებას;.

6. მომხმარებელს გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურება უწყდება მარეგისტრირებელი ორგანოს მიერ შესაბამის გადაწყვეტილებაში მითითებული თარიღიდან, რომელიც არ უნდა აღემატებოდეს გადაწყვეტილების მიღებიდან 2 სამუშაო დღეს.

7. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შეწყვეტის შემთხვევაში განმცხადებელი უფლებამოსილია, სააგენტოს განცხადებით მიმართოს შესაბამისი მომსახურების მიღების მოთხოვნით.

მუხლი 97. სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით პირობების ცვლილება

1. დასაშვებია, შეიცვალოს გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების შემდეგი პირობები:

ა) მომსახურების წარმადობის კონფიგურაცია;

ბ) მომხმარებლის IP მისამართი, რომლიდანაც ხელმისაწვდომია მომსახურება;

გ) მომსახურების ვადის გაგრძელება.

2. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების პირობების ცვლილების მოთხოვნა შეუძლია იმ მომხმარებლის უფლებამოსილ წარმომადგენელს, რომელსაც სააგენტო უწევს შესაბამის მომსახურებას.

3. შესაბამისი უფლებამოსილი პირი, გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების პირობების ცვლილების მოთხოვნის განცხადებით მიმართავს სააგენტოს.

4. სააგენტოში წარდგენილი განცხადება უნდა შეიცავდეს შემდეგ ინფორმაციას:

ა) გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების პირობების ცვლილების შესახებ მოთხოვნას;

ბ) ორგანიზაციის დასახელებას, ხელმომწერი პირის სახელსა და გვარს, თანამდებობასა და ხელმოწერას;

გ) ხელმოწერის თარიღს;

დ) განცხადების მატერიალური ფორმით წარმოდგენის შემთხვევაში, განცხადების წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტებს (სახელი, გვარი, პირადი ნომერი).

5. განცხადებას უნდა დაერთოს განმცხადებლის უფლებამოსილების დამადასტურებელი დოკუმენტი.

6. ამ მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული პირობის ცვლილების შემთხვევაში, განმცხადებელმა უნდა წარმოადგინოს საფასურის გადახდის დამადასტურებელი დოკუმენტი არაუგვიანეს განცხადების შეტანის დღისა. აღნიშნული დოკუმენტის წარმოდგენა არ მოითხოვება, თუ განმცხადებელმა თანხა გადაიხადა სპეციალური ავტომატიზებული საგადახდო სისტემის საშუალებით, რომელიც უზრუნველყოფს სააგენტოსთვის გადახდილი თანხების შესახებ ინფორმაციის ხელმისაწვდომობას. სააგენტო უფლებამოსილია, საჭიროების შემთხვევაში, მოითხოვოს გადახდის დამადასტურებელი დოკუმენტი.

7. გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების პირობების ცვლილების მატერიალური ფორმით მოთხოვნა, რომელიც არ არის შედგენილი რთული წერილობითი ფორმით, მომხმარებლის წარმომადგენლის ნების დადასტურების მიზნით, სააგენტოს წარედგინება უფლებამოსილი პირის მიერ, სააგენტოში ფიზიკურად გამოცხადების გზით.

8. განცხადების მიღების შემდეგ არაუმეტეს 10 სამუშაო დღის ვადაში მარეგისტრირებელი ორგანო ამოწმებს წარმოდგენილი დოკუმენტების შესაბამისობას ამ შინაგანაწესის მოთხოვნებთან.

9. განცხადების განხილვის ფარგლებში, მარეგისტრირებელი ორგანო უფლებამოსილია, განახორციელოს განმცხადებლის (მისი წარმომადგენლის) იდენტიფიკაცია. მარეგისტრირებელი ორგანო, ასევე, უფლებამოსილია, შესაბამისი უწყებების მონაცემთა ელექტრონული ბაზიდან გამოითხოვოს შემდეგი ინფორმაცია:

ა) იურიდიული პირის სარეგისტრაციო მონაცემები სსიპ - საჯარო რეესტრის ეროვნული სააგენტოდან;

ბ) იურიდიული პირის საგადასახადო რეგისტრაციის შესახებ მონაცემები სსიპ - შემოსავლების სამსახურიდან.

10. მარეგისტრირებელი ორგანო შეაჩერებს განცხადების განხილვას და დაადგენს ხარვეზის გამოსწორებისათვის ვადას იმ შემთხვევაში, თუ:

ა) განცხადება და წარმოდგენილი დოკუმენტაცია არ შეესაბამება ამ მუხლის მე-4 და მე-5 პუნქტებით დადგენილ მოთხოვნებს, გარდა ამ მუხლის მე-4 პუნქტის „დ“ ქვეპუნტისა;

ბ) ამ მუხლის მე-9 პუნქტით გათვალისწინებული ინფორმაციის გადამოწმების დროს ვერ ხორციელდება პირის იდენტიფიკაცია ან საჭირო ინფორმაციის მოძიება.

11. ამ მუხლის მე-3 პუნქტში მითითებული ხარვეზის გამოსწორებისათვის დადგენილი ვადა არ უნდა აღემატებოდეს 10 სამუშაო დღეს. სააგენტოს მიერ დადგენილ ვადაში ხარვეზის გამოუსწორებლობის შემთხვევაში, განცხადება რჩება განუხილველი.

12. განმცხადებელს შეიძლება უარი ეთქვას გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების პირობების ცვლილებაზე, თუ:

ა) სააგენტო არ აწვდის განმცხადებელს შესაბამის მომსახურებას;

ბ) ამავე მუხლის პირველი პუნქტის „გ“ ქვეპუნქტით გათვალისწინებული პირობის ცვლილების შემთხვევაში, განმცხადებელმა არ გადაიხადა მომსახურების საფასური;

გ) განცხადებაში არ არის მითითებული განცხადების მატერიალურად წარმოდგენაზე უფლებამოსილი პირის რეკვიზიტები, ამ მუხლის მე-4 პუნქტის „დ“ ქვეპუნქტის მოთხოვნების შესაბამისად, ან განცხადებაში მითითებული პირისა და სააგენტოში განცხადების უშუალოდ წარმომდგენი პირის მონაცემები სხვადასხვაა.

13. მომხმარებლისთვის გარანტირებული წარმადობით სერტიფიკატის სტატუსის ავტომატური შემოწმების შეცვლილი პირობებით მომსახურების მიწოდება ხორციელდება მარეგისტრირებელი ორგანოს მიერ შესაბამის გადაწყვეტილებაში მითითებული თარიღიდან, რომელიც არ უნდა აღემატებოდეს გადაწყვეტილების მიღებიდან 2 სამუშაო დღეს.

თავი X

სერტიფიკატის გამცემი ძირითადი ორგანოს (GEO Root CA) მიერ სერტიფიკატების გაცემა, მართვა და გამოყენება

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

1. სერტიფიკატის გამცემი ძირითადი ორგანო - GEO Root CA - გამოიყენება საწყის ნდობის წერტილად ზოგადი გამოყენების სანდო მომსახურებებისთვის. იგი მოქმედებს თვითხელმოწერილი სერტიფიკატებით.

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

3. სერტიფიკატის გამცემი ძირითადი ორგანო - GEO Root CA - 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 ორგანოს 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.

მუხლი 99. სერტიფიკატის გამცემი ორგანოების განმასხვავებელი სახელები და მათი ინტერპრეტირების წესი

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; **(ცვლილება 2021.06.07.N245/ს)**

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); **(ცვლილება 2021.06.07.N245/ს)**

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); **(ცვლილება 2021.06.07.N245/ს)**

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); **(ცვლილება 2021.06.07.N245/ს)**

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

„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). **(ცვლილება 2021.06.07.N245/ს)**

2. განმასხვავებელ სახელებს განსაზღვრავს სერტიფიცირების ცენტრი. განმასხვავებელი სახელი მიუთითებს სერტიფიკატის დანიშნულებას.

მუხლი 100. სერტიფიკატის გამცემი ორგანოს სერტიფიკატის გაცემის ინიცირება

1. თუ სააგენტო გეგმავს ისეთი სახის ახალი მომსახურების შეთავაზებას მომხმარებლებისათვის, რომელიც საჭიროებს სერტიფიკატის გამცემი ახალი ორგანოს შექმნას, მაშინ შესაბამისი ბიზნესპროცესის მფლობელი სტრუქტურული ერთეულის ხელმძღვანელი ან პროექტის მენეჯერი სააგენტოს დოკუმენტბრუნვის ელექტრონული სისტემის საშუალებით დასაბუთებულ მიმართვას უგზავნის სააგენტოს ინფორმაციული ტექნოლოგიების მმართველი კომიტეტის თავმჯდომარეს, რომელიც ვალდებულია, საკითხი განსახილველად გაიტანოს უახლოეს მმართველ კომიტეტზე.

2. თუ საჭიროა სერტიფიკატის სტატუსის ავტომატური შემოწმების მომსახურების სერტიფიკატის გაცემა ახალი სერვერის ინსტალაციის გამო, შესაბამისი საკითხის ინფორმაციული ტექნოლოგიების მმართველ კომიტეტზე ინიცირებას ახდენს სააგენტოს სტრუქტურული ერთეულის, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის მართვისა და განვითარების სამსახურის უფროსი.

3. არსებული სერტიფიკატის გამცემი ორგანოს ახალი სერტიფიკატის შესაქმნელად შესაბამისი საკითხის ინფორმაციული ტექნოლოგიების მმართველ კომიტეტზე ინიციირებას ახდენს სააგენტოს სტრუქტურული ერთეულის, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის მართვისა და განვითარების სამსახურის უფროსი.

მუხლი 101. სერტიფიკატის გამცემი ორგანოს სერტიფიკატის გაცემაზე განცხადების დამუშავება და გადაწყვეტილების მიღება

ინფორმაციული ტექნოლოგიების მმართველი კომიტეტის მიერ სერტიფიკატის გაცემაზე დადებითი გადაწყვეტილების მიღების შემთხვევაში, საკითხი შესასრულებლად გადაეცემა სერტიფიცირების ცენტრს. სერტიფიცირების ცენტრი განსაზღვრავს შესასრულებელი სამუშაოების ზუსტ მოცულობას, მიმდევრობას, დროსა და სამუშაოს თითოეულ კომპონენტზე პასუხისმგებელ პირს. აღნიშნულთან დაკავშირებით იწერება ცვლილების შესახებ განცხადება, რომელსაც ხელს აწერს სანდო მომსახურების მიმწოდებლის ხელმძღვანელი და ყველა პასუხისმგებელი პირი.

მუხლი 102. სერტიფიკატის გაცემა, ინსტალაცია და განახლება

1. სერტიფიკატი გაიცემა ცვლილებების შესახებ განცხადების შესაბამისად. გაცემის პროცესი გულისხმობს გასაღების წყვილის გენერაციას, ახალი სერტიფიკატის შექმნასა და მის ჩატვირთვას სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემაში (სერტიფიკატის სპეციფიკიდან გამომდინარე). გასაღების წყვილი უნდა შეიქმნას წინამდებარე შინაგანაწესის თავი XII

ტექნიკური უსაფრთხოების კონტროლი) მოთხოვნების შესაბამისად. სერტიფიკატის გაცემის შემდეგ დგება ოქმი ჩატარებული სამუშაოების შესახებ.

2. ჩატარებული სამუშაოების შესაბამისობა ცვლილების პროექტის დოკუმენტთან კონტროლდება ზედამხედველობაზე პასუხისმგებელი პირის მიერ, პროცედურის შესრულების პროცესში - სააგენტოში დადგენილი წესის შესაბამისად.

3. სერტიფიკატი არ გაიცემა გასაღების წყვილზე, რომელზეც სერტიფიკატი ადრე იყო გაცემული. სერტიფიკატის გაცემა ყოველთვის გულისხმობს გასაღების წყვილის ხელახლა შექმნას.

4. სერტიფიკატის განმეორებით გაცემა შესაძლებელია მხოლოდ ორი, სათანადო უფლებამოსილების მქონე პირის მონაწილეობით.

მუხლი 103. სერტიფიკატის განმეორებით გაცემა

1. დაუშვებელია, სერტიფიკატის გამცემმა ორგანომ გასცეს ისეთი სერტიფიკატი, რომლის მოქმედების ვადა აჭარბებს თავად სერტიფიკატის გამცემი ორგანოს სერტიფიკატის მოქმედების ვადას.

2. სერტიფიკატის გამცემი ორგანოს ახალი სერტიფიკატი უნდა შეიქმნას ძველი სერტიფიკატის მოქმედების ვადის ამოწურვამდე 6 თვით ადრე. დასაბუთებული საჭიროების (სერტიფიკატში ინფორმაციის ცვლილების ან სხვა საჭიროების) არსებობის შემთხვევაში, დასაშვებია ახალი სერტიფიკატის შექმნა ამ ვადაზე ადრე. სერტიფიკატის შექმნის მოთხოვნით განცხადება უნდა დაიწეროს წინამდებარე შინაგანაწესის მე-100 მუხლის შესაბამისად. სერტიფიკატი უნდა გაიცეს ამ შინაგანაწესის 102-ე მუხლის შესაბამისად.

3. დასაშვებია, სერტიფიკატის გამცემი ორგანოს ახალმა სერტიფიკატმა არ ჩაანაცვლოს წინა სერტიფიკატი მისი მოქმედების ვადის ამოწურვამდე შესაბამისი მომსახურების მიწოდებისას. აღნიშნულის საჭიროება მითითებული უნდა იყოს მე-2 პუნქტით განსაზღვრულ განცხადებაში და მასზე უნდა არსებობდეს შესაბამისი თანხმობა. წინააღმდეგ შემთხვევაში, მომსახურება სერტიფიკატის გამცემი ორგანოს ახალ სერტიფიკატზე გადაერთვება გაცემისთანავე.

4. წინა სერტიფიკატის შესაბამისი დახურული გასაღები და სარეზერვო ასლი უნდა განადგურდეს შესაბამისი მომსახურების ახალ სერტიფიკატზე გადართვისთანავე.

მუხლი 104. სერტიფიკატში ინფორმაციის ცვლილება

სერტიფიკატის გამცემი ორგანოს სერტიფიკატში ინფორმაციის ცვლილება აუცილებლად გულისხმობს სერტიფიკატის განმეორებით გაცემას, წინამდებარე შინაგანაწესით დადგენილი წესით.

მუხლი 105. სერტიფიკატის გაუქმება და შეჩერება

1. სერტიფიკატის გაუქმების საჭიროების შემთხვევაში, გარდა „ბიზნეს უწყვეტობის გეგმით“ გათვალისწინებული ფორსმაჟორული სიტუაციებისა, სააგენტოს სტრუქტურული ერთეულის, ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის მართვისა და განვითარების სამსახურის უფროსი ადგენს მოტივირებულ მიმართვას სანდო მომსახურების მიმწოდებლის ხელმძღვანელის სახელზე, რის შემდეგაც სანდო მომსახურების მიმწოდებლის ხელმძღვანელის დავალებით დგება ამ დოკუმენტის მე-100 მუხლის მე-3 პუნქტით დადგენილი ცვლილების პროექტის ამსახველი დოკუმენტი, რომლის აღსრულება ხდება წინამდებარე დოკუმენტის 102-ე მუხლით დადგენილი წესით. სერტიფიკატის გაუქმება გულისხმობს სუბიექტის მოწყობილობაში დახურული გასაღებისა და სარეზერვო ასლის განადგურებას.

2. სანდო მომსახურების მიმწოდებლის მიერ სერტიფიკატის მოქმედების შეჩერება არ დაიშვება.

თავი XI

ინფრასტრუქტურა, მართვა, ოპერაციული და ფიზიკური კონტროლი

მუხლი 106. ინფორმაციული უსაფრთხოება, რისკებისა და აქტივების მართვა

1. სააგენტო წარმოადგენს კრიტიკული ინფორმაციული სისტემის სუბიექტს საქართველოს კანონმდებლობის შესაბამისად. სააგენტოში დამტკიცებულია „ინფორმაციული უსაფრთხოების პოლიტიკა“. წინამდებარე შინაგანაწესით განსაზღვრული სანდო და კვალიფიციური სანდო მომსახურების მიწოდების, კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნის, გაცემისა და მასთან დაკავშირებული მომსახურებების გაწევის საკითხები, მათ შორის, რისკების მართვისა და აქტივების მართვის საკითხები აღნიშნული პოლიტიკის ფარგლებში რეგულირდება.

2. სანდო მომსახურების უსაფრთხო სისტემების კონფიგურაცია პერიოდულად გადაიხედება, ინფორმაციული უსაფრთხოების პოლიტიკის მიმართ შეუსაბამობების აღმოჩენისა და აღმოფხვრის მიზნით. ორ გადახედვას შორის ინტერვალი 1 წელს არ აღემატება.

მუხლი 107. დაშვების ზონების კლასიფიკაცია

1. სააგენტოს ტერიტორია „საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – სახელმწიფო სერვისების განვითარების სააგენტოს ფიზიკური უსაფრთხოების და გარემოს

კონტროლის პოლიტიკის“ მიხედვით დაყოფილია სხვადასხვა ზონად, მათში დაცული ინფორმაციის ან/და ინფრასტრუქტურის და დაშვების წესების მიხედვით. წინამდებარე შინაგანაწესის მიზნებისათვის ეს ზონებია:

ა) კრიტიკული ზონა - სააგენტოს მონაცემთა დამუშავების ძირითადი და სარეზერვო ცენტრები;

ბ) მკაცრად აკრძალული ზონა - სააგენტოს სტრუქტურული ერთეულის, ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრის (სამსახური) განთავსების ადგილები;

გ) აკრძალული ზონა - მატერიალური და ინფორმაციული აქტივების შენახვისათვის სპეციალურად გამოყოფილი საცავი (არქივები და საწყობები);

დ) დაცული საოფისე ზონა - სააგენტოს თანამშრომელთათვის განკუთვნილი ზონა.

2. აღნიშნულ ზონებში დაშვება რეგულირდება სააგენტოში დამტკიცებული პროცედურების შესაბამისად.

მუხლი 108. კრიტიკული და მკაცრად აკრძალული ზონების ადგილმდებარეობა და დანიშნულება

1. სანდო მომსახურების მიწოდებასთან დაკავშირებული ყველა კრიტიკული მონაცემი ინახება და მუშავდება მონაცემთა დამუშავების ორ - ძირითად და სარეზერვო ცენტრში, რომლებიც რისკების გათვალისწინებით, განთავსებულია საქართველოს ტერიტორიაზე, გეოგრაფიულად დაშორებულ ადგილებზე.

2. თუ ამ შინაგანაწესის შესაბამისი თავებით სხვა რამ არ არის განსაზღვრული, სუბიექტის მოწყობილობების პერსონალიზაცია ხდება ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრში (სამსახური), რომელიც განლაგებულია საქართველოს ტერიტორიაზე - ქალაქ თბილისის მუნიციპალიტეტში, ქალაქ ქუთაისის მუნიციპალიტეტში და ქალაქ ბათუმის მუნიციპლიტეტშიი.

3. სააგენტოს მონაცემთა დამუშავების ორივე ცენტრი, ასევე ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრი (სამსახური) მდებარეობს მხოლოდ ამ მიზნისთვის გამოყოფილ სპეციალიზებულ ოთახებში.

4. სააგენტოს მონაცემთა დამუშავების ორივე ცენტრში სანდო მომსახურების მიწოდებასთან დაკავშირებული აპარატურული უზრუნველყოფა განთავსებულია იზოლირებულ სასერვერო კარადებში, რომლებიც მუდმივად ჩაკეტილია და გახსნისათვის აუცილებელია, სულ მცირე, ორი პასუხისმგებელი პირის ერთდროული მონაწილეობა.

მუხლი 109. ფიზიკური დაშვება სააგენტოს მონაცემთა დამუშავების ცენტრებში

1. სააგენტოს მონაცემთა დამუშავების თითოეული ცენტრის თითოეული შესასვლელი აღჭურვილია რკინის კარით. შესასვლელთან მოხვედრა შესაძლებელია მხოლოდ შესაბამისი შენობის შიდა პერიმეტრიდან.

2. სააგენტოს მონაცემთა დამუშავების ცენტრში დაშვება შესაძლებელია უსაფრთხოების მრავალდონიანი დაცული სისტემის გავლით, რომელიც რეგულირდება სააგენტოში დამტკიცებული პროცედურების მიხედვით და მოიცავს:

ა) გარე პერიმეტრს:

ა.ა) შესვლა მონაცემთა დამუშავების ორივე ცენტრში შესაძლებელია მხოლოდ შესაბამისი გარე პერიმეტრის გავლით;

ა.ბ) შესვლა გარე პერიმეტრში კონტროლდება შესაბამისი კონტრაქტორი ორაგანიზაციის მიერ (დაცვის სამსახურის) მიერ;

ა.გ) აღნიშნულ სამსახურთან თანხმდება სააგენტოს და მომსახურე კომპანიების პასუხისმგებელი თანამშრომლების სია;

ა.დ) შესვლა გარე პერიმეტრში შესაძლებელია პიროვნების იდენტიფიკაციის შემდეგ პირადობის დამადასტურებელი დოკუმენტის საშუალებით.

ბ) შიდა პერიმეტრს:

ბ.ა) შიდა პერიმეტრში მოხვედრა შესაძლებელია მხოლოდ გარე პერიმეტრის გავლის შემდეგ;

ბ.ბ) შიდა პერიმეტრში განთავსებულია:

ბ.ბ.ა) მონაცემთა დამუშავების ცენტრი;

ბ.ბ.ბ) დიზელის გენერატორები;

ბ.ბ.გ) გაგრილების სისტემის კომპონენტები.

ბ.გ) დიზელგენერატორებისა და გაგრილების სისტემის კომპონენტების განთავსების ადგილი კონტროლდება ვიდეოსათვალთვალო სისტემის საშუალებით;

ბ.დ) მონაცემთა დამუშავების ორივე ცენტრის მიმდებარე ტერიტორია კონტროლდება ვიდეოსათვალთვალო სისტემის საშუალებით;

ბ.ე) შესვლა მონაცემთა დამუშავების ცენტრის ოთახებში შესაძლებელია მხოლოდ ელექტრონული პირადობის მოწმობით, მხოლოდ ავტორიზებული პირებისათვის.

მუხლი 110. ფიზიკური დაშვება ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრში (სამსახური)

1. ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრში (სამსახური) მოხვედრა შესაძლებელია მხოლოდ შენობის შიდა პერიმეტრიდან.

2. ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრებში (სამსახური) დაშვება, ასევე, ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრის (სამსახური) შიდა პერიმეტრი და ყველა კრიტიკული დანადგარი კონტროლდება ტერიტორიაზე დაშვების ელექტრონული და ვიდეოსათვალთვალო სისტემის მეშვეობით, სააგენტოში დამტკიცებული პროცედურების შესაბამისად.

3. ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრში (სამსახური) შესვლა რეგულირდება სააგენტოში დამტკიცებული პროცედურების შესაბამისად და დასაშვებია მხოლოდ ავტორიზებული პირებისათვის.

მუხლი 111. ელექტროკვების და გაგრილების სისტემები, წყლისგან და ხანძრისგან დაცვა

1. სააგენტოს მონაცემთა დამუშავების ცენტრებში და ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრში (სამსახური) გამოყენებული აპარატურა უწყვეტად მარაგდება ელექტროენერგიით, ორი სხვადასხვა წყაროდან. მონაცემების დამუშავების ძირითადი და სარეზერვო ცენტრები აღჭურვილია გაგრილებისა და კლიმატის კონტროლის ცენტრალიზებული სისტემით. უზრუნველყოფილია მუდმივი ელექტრო მომარაგებისა და მონიტორინგის სისტემა.

2. სააგენტოს მონაცემთა დამუშავების ცენტრები, ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრი (სამსახური) და არქივი წყალმოვარდნისაგან დასაცავად განთავსებულია მიწის ზედაპირიდან ამაღლებულ სართულზე. მეტი იზოლაციისათვის, ელექტრონული აპარატურა განთავსებულია იატაკის ზედაპირიდან ამაღლებულ საყრდენზე. სასერვერო კარადები არის ჰერმეტულად დაცული.

3. სააგენტოს მონაცემთა დამუშავების ცენტრები აღჭურვილია ხანძრის აღმოჩენის სისტემით. დამატებით, ხანძრის ჩამქრობი მოწყობილობები ხელმისაწვდომია მთელ შენობაში. სერტიფიცირების ცენტრის და ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრის (სამსახური) პერსონალს გავლილი აქვს მათი გამოყენების ტრენინგები. სასერვერო კარადები, სადაც განთავსებულია სანდო მომსახურების მიწოდებასთან დაკავშირებული აპარატურა, აღჭურვილია ხანძრის აღმოჩენის და ავტომატიზებული ქრობის ცენტრალიზებულად მართვადი სისტემით, რომლის ამოქმედება, მოთხოვნის შემთხვევაში, შესაძლებელია ხელით.

მუხლი 112. მონაცემთა სანახების დაცვა და სარეზერვო ასლების შენახვა

1. საწარმოო გარემოში გამოყენებული პროგრამული უზრუნველყოფა და მონაცემები, ასევე, ყველა მოწყობილობა, რომლებზეც შენახულია აუდიტის მონაცემები, არქივი ან სარეზერვო ასლის მონაცემები - მოთავსებული და დაცულია სააგენტოს კრიტიკულ, მკაცრად აკრძალულ ან აკრძალულ ზონებში, მონაცემთა მგრძნობიარობის გათვალისწინებით, მათზე წვდომა შეუძლიათ მხოლოდ ავტორიზებულ პირებს, მხოლოდ შიდა პერიმეტრიდან. მოწყობილობები დაცულია შესაძლო ინციდენტებისა და დაზიანებებისგან.

2. მონაცემთა დაზიანების/დაკარგვის თავიდან აცილების მიზნით, სააგენტო ცენტრალიზებული და ავტომატიზებული სისტემის მეშვეობით იღებს უსაფრთხოებისა და/ან ყველა მუშა პროცესის უწყვეტობის თვალსაზრისით მგრძნობიარე ინფორმაციის სარეზერვო ასლებს. სარეზერვო ასლის აღება ხდება სააგენტოში მოქმედი „მონაცემთა ბაზების და პროგრამული უზრუნველყოფის სარეზერვო ასლების შექმნის პროცედურის“ შესაბამისად მონაცემთა დამუშავების ორივე (ძირითად და სარეზერვო) ცენტრში.

მუხლი 113. ნარჩენების კონტროლი

ელექტრონული მონაცემები და სანახები, რომლებიც შეიცავენ უსაფრთხოების თვალსაზრისით კრიტიკულ ინფორმაციას (ისეთ ინფორმაციას, რომლის გამჟღავნებამ შეიძლება საფრთხე შეუქმნას სანდო მომსახურების მიმწოდებელს და/ან ღია გასაღების ინფრასტრუქტურის სხვა მონაწილე მხარეებს) ნადგურდება შემდეგი წესით:

ა) მატერიალური დოკუმენტები ნადგურდება ქაღალდების გამანადგურებლის საშუალებით;

ბ) ელექტრონული ინფორმაცია ნადგურდება სააგენტოში დამტკიცებული ,,ღია გასაღების ინფრასტრუქტურის მედიის (ინფორმაციის მატარებლის) მართვის პროცედურისა“ და ,,ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“ შესაბამისად.

მუხლი 114. ნდობით აღჭურვილი პოზიციები/უფლებრივი როლები

1. სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემებს და მათთან დაკავშირებულ ინფორმაციულ აქტივებს მართავს და აკონტროლებს ნდობით აღჭურვილი პერსონალი, რომელსაც აქვს დაშვება და კონტროლის უფლებამოსილება.

2. ნდობით აღჭურვილი პერსონალი დანიშვნამდე გადის კონტროლს წინამდებარე დოკუმენტის 35-ე მუხლით დადგენილი წესის შესაბამისად.

3. სააგენტოს ნდობით აღჭურვილი პერსონალი:

ა) ინფორმაციული უსაფრთხოების მენეჯერი - პირი, რომელიც პასუხისმგებელია სანდო მომსახურების მიმწოდებელში:

ა.ა) გასაღებების გენერაციის პროცესისა და სხვა კონფიდენციალური მონაცემების მართვის ზედამხედველობაზე;

ა.ბ) აუდიტის ოქმების მიღებაზე, შენახვასა და მათზე პასუხის მომზადებაზე.

ბ) შიდა აუდიტის სამსახურის პასუხისმგებელი თანამშრომელი - პირი, რომელიც პასუხისმგებელია სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების ხდომილებების ჟურნალების ანალიზსა და შიდა აუდიტის ჩატარებაზე.

გ) სისტემური ადმინისტრატორი - პირი, რომელიც პასუხისმგებელია სანდო მომსახურების მიმწოდებლის:

გ.ა) პროგრამული სისტემების (გარდა სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემებისა) ინსტალაციაზე, კონფიგურაციასა და გამართულ ფუნქციონირებაზე;

გ.ბ) ხდომილებების აღრიცხვის, მომსახურების მონიტორინგის სისტემების ინსტალაციაზე, კონფიგურაციასა და გამართულ მუშაობაზე;

გ.გ) სისტემისა და მონაცემების ავტომატიზებული რეზერვირების გამართულ ფუნქციონირებაზე.

დ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემის მონაცემთა ბაზების ადმინისტრატორი - პირი, რომელიც პასუხისმგებელია მონაცემთა ბაზის სისტემის ინსტალაციაზე, კონფიგურაციასა და გამართული ფუნქციონირების უზრუნველყოფაზე.

ე) ქსელის უფროსი ადმინისტრატორი - პირი, რომელიც პასუხისმგებელია სერტიფიცირების ცენტრის საკომუნიკაციო ინფრასტრუქტურის ინსტალაციაზე, კონფიგურაციასა და გამართული მუშაობის უზრუნველყოფაზე.

ვ) პროგრამული უზრუნველყოფის ადმინისტრატორი - პირი, რომელიც პასუხისმგებელია ღია გასაღების ინფრასტრუქტურის კომპონენტებზე, რაც მოიცავს:

ვ.ა) სერტიფიკატის გაცემასა და მომსახურებასთან დაკავშირებული სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების ინსტალაციის, კონფიგურაციისა და გამართული მუშაობის უზრუნველყოფას;

ვ.ბ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების საშუალებით ადმინისტრირებას და მართვას;

ვ.გ) დროის აღმნიშვნელ ორგანოებთან დაკავშირებული სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების ინსტალაციის, კონფიგურაციისა და გამართული მუშაობის უზრუნველყოფას;

ვ.დ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემების საშუალებით ადმინისტრირებას და მართვას.

4. ამ მუხლის მე-3 პუნქტით განსაზღვრული ნდობით აღჭურვილი პოზიციების/უფლებრივი როლების გარდა, დამატებით ნდობით აღჭურვილი პოზიციები/უფლებრივი როლები და პერსონალი განისაზღვრება სააგენტოს თავმჯდომარის სამართლებრივი აქტით. **(ცვლილება 2021.06.07.N245/ს)**

მუხლი 115. ამოცანების შესასრულებლად საჭირო პერსონალის რაოდენობა

1. უსაფრთხოების თვალსაზრისით კრიტიკულ ოპერაციებზე სანდო მომსახურების მიმწოდებელში განსაზღვრულია 2 (ორი) ან მეტი პირის ერთდროული მონაწილეობა. აღნიშნული მოიცავს, სულ მცირე, შემდეგ მოქმედებებს:

ა) უსაფრთხოების აპარატურული მოდულის ინიციალიზაციას;

ბ) წინამდებარე შინაგანაწესით განსაზღვრული გასაღებების წყვილის მექანიკურად შექმნას ან/და სერტიფიკატის მექანიკურ გაცემას;

გ) სერტიფიკატის გამცემი ორგანოს გასაღების წყვილის სარეზერვო ასლის შექმნასა და რეზერვიდან აღდგენას.

2. წინამდებარე მუხლის პირველი პუნქტის „ა“ და „ბ“ ქვეპუნქტები დეტალურად რეგულირდება „გასაღების წყვილის შექმნისა და სერტიფიკატის მექანიკურ რეჟიმში გაცემის პროცედურით“.

მუხლი 116. იდენტიფიკაცია და ავთენტიფიკაცია თითოეული პოზიციისთვის/უფლებრივი როლისთვის

1. სანდო მომსახურების მიმწოდებლის ფუნქციონირებაში მონაწილე პოზიციების უფლებამოსილებებია:

ა) ინფორმაციული უსაფრთხოების მენეჯერს გააჩნია ფიზიკური დაშვება მომაცემთა დამუშავების ცენტრებში.

ბ) სისტემის აუდიტორს:

ბ.ა) გააჩნია ფიზიკური დაშვება მონაცემთა დამუშავების ცენტრებში;

ბ.ბ) გააჩნია პროგრამული წვდომა მხოლოდ დათვალიერების უფლებით ხდომილებების აღრიცხვის, მონიტორინგის, მონაცემების რეზერვირებისა და არქივირების სისტემებზე;

ბ.გ) სისტემებში იდენტიფიცირდება უნიკალური სახელითა და პაროლით.

გ) სისტემურ ადმინისტრატორს:

გ.ა) გააჩნია ფიზიკური დაშვება მონაცემთა დამუშავების ცენტრებში;

გ.ბ) გააჩნია წვდომა ადმინისტრირების უფლებებით ოპერაციულ სისტემაზე, ხდომილებების აღრიცხვის, მონიტორინგისა და რეზერვირების ავტომატიზებულ სისტემებზე;

გ.გ) სისტემებში იდენტიფიცირდება უნიკალური სახელითა და პაროლით.

დ) სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემის მონაცემთა ბაზების ადმინისტრატორს:

დ.ა) გააჩნია ფიზიკური დაშვება მონაცემთა დამუშავების ცენტრებში;

დ.ბ) გააჩნია წვდომა ადმინისტრირების უფლებებით მონაცემთა ბაზის სისტემებზე;

დ.გ) სისტემებში იდენტიფიცირდება უნიკალური სახელისა და პაროლის საშუალებით.

ე) ქსელის უფროსი ადმინისტრატორი:

ე.ა) გააჩნია ფიზიკური დაშვება მონაცემთა დამუშავების ცენტრებში;

ე.ბ) გააჩნია წვდომა სერტიფიცირების ცენტრის საკომუნიკაციო აპარატურაზე;

ე.გ) სისტემაში იდენტიფიცირდება უნიკალური სახელითა და პაროლით.

ვ) პროგრამული უზრუნველყოფის ადმინისტრატორს:

ვ.ა) გააჩნია ფიზიკური დაშვება მონაცემთა დამუშავების ცენტრებში;

ვ.ბ) გააჩნია წვდომა ადმინისტრირების უფლებებით ღია გასაღების ინფრასტრუქტურაზე, სადაც იდენტიფიცირდება მრავალფაქტორიანი ავთენტიფიკაციის მექანიზმებით;

ვ.გ) გააჩნია წვდომა შეზღუდული უფლებებით შესაბამისი სერვერების ოპერაციულ სისტემებზე, სადაც იდენტიფიცირდება უნიკალური სახელითა და პაროლით;

ვ.დ) შესაბამის უფლებამოსილ პირთან ერთად გააჩნია ადმინისტრატორის წვდომა უსაფრთხოების აპარატურულ მოდულზე;

ვ.ე) შეუძლია სისტემაში იდენტიფიცირება უნიკალური სახელითა და პაროლით.

ზ) მარეგისტრირებელი ორგანოს თანამშრომელს გააჩნია წვდომა სერტიფიკატების მართვის სისტემაზე შემდეგი შესაძლო უფლებებით: სერტიფიკატების გენერაციასა და გაუქმებაზე განცხადების მიღება და სერტიფიკატის გაუქმება. მარეგისტრირებელი ორგანოს თანამშრომელი სისტემაში იდენტიფიცირდება უნიკალური სახელითა და პაროლით.

2. განსაკუთრებული უფლებების მქონე მომხმარებლების ანგარიშების გამოყენება მიმდინარეობს ,,განსაკუთრებული უფლებების მქონე მომხმარებლების წვდომის მართვის პროცედურის“ შესაბამისად.

მუხლი 117. პროფესიულ ცოდნასთან, კვალიფიკაციასა და გამოცდილებასთან დაკავშირებული პირობები და განსაკუთრებული შემოწმების აუცილებლობა

სერტიფიცირების ცენტრს, ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრსა (სამსახური) და კონტრაქტორებს სააგენტო უწესებს მაღალ საკონკურსო სტანდარტებს. აღნიშნული მოიცავს, მაგრამ არ შემოიფარგლება, განათლებით, სამუშაო გამოცდილებითა და რეკომენდაციებით.

მუხლი 118. თანამშრომელთა ტრენინგი

1. დაკისრებული მოვალეობის შესრულებამდე სააგენტოს თანამშრომლებსა და კონტრაქტორების იმ ჯგუფებს , რომლებიც პასუხისმგებელი არიან წინამდებარე შინაგანაწესით განსაზღვრული ამოცანების შესრულებაზე, უტარდებათ ტრენინგები სამართლებრივ, უსაფრთხოებისა და ტექნიკურ საკითხებზე.

2. სააგენტოს ტრენინგის მასალების მონიტორინგი მიმდინარეობს უწყვეტ რეჟიმში და, საჭიროების შემთხვევაში, განიცდის ცვლილებებს.

3. სააგენტოში პროცედურული, გამოყენებული პროგრამული უზურნველყოფის ან ინფრასტრუქტურული ცვლილებების დროს ტარდება რიგგარეშე ტრენინგები.

4. სისტემის უსაფრთხოებისა და მომსახურების ხარისხის გაუმჯობესების მიზნით, წელიწადში ერთხელ სერტიფიცირების ცენტრის თანამშრომელთათვის ტარდება დამატებითი ტრენინგები.

5. ტრენინგის აღრიცხვის ფურცლები აუცილებლად უნდა შეიცავდეს ტრენინგის სათაურს, ჩატარების თარიღს (ან ინტერვალს) და მოკლე აღწერას; თითოეული თანამშრომლის სახელს, გვარს, სტრუქტურულ ერთეულს. ფურცელი დადასტურებული უნდა იყოს თითოეული თანამშრომლის ხელმოწერით.

6. ტრენინგის აღრიცხვის დოკუმენტაცია ინახება სააგენტოში დამტკიცებული წესის მიხედვით.

მუხლი 119. თანამშრომლებისთვის დოკუმენტების გაცნობა

სააგენტო ვალდებულია, წინამდებარე შინაგანაწესი და სააგენტოში დამტკიცებული ყველა დოკუმენტი, რომელიც დაკავშირებულია შინაგანაწესით განსაზღვრულ სამუშაოებთან, გააცნოს თანამშრომლებს.

მუხლი 120. სერტიფიკატის სასიცოცხლო ციკლის ოპერაციების აღრიცხვა

1. სასიცოცხლო ციკლის ოპერაციები აღირიცხება ელექტრონული ჩანაწერების საშუალებით და/ან ბეჭდური სახით. აღირიცხება, სულ მცირე, მოვლენის განმარტება, ხდომილების თარიღი და ინფორმაცია მოვლენაში ჩართული პირების შესახებ. სასიცოცხლო ციკლის ოპერაციებია:

ა) გასაღების წყვილის შექმნა, სარეზერვო ასლის აღება, შენახვა, აღდგენა, დაარქივება და განადგურება;

ბ) უსაფრთხოების აპარატურული მოდულის პერიოდული მართვის ღონისძიებები;

გ) სერტიფიკატზე განცხადების წარდგენა, გასაღების წყვილის განახლება და სერტიფიკატის გაუქმება;

დ) სერტიფიკატებისა და გაუქმებული სერტიფიკატების სიის შექმნა და გამოქვეყნება;

ე) სისტემაზე წვდომის წარმატებული და წარუმატებელი მცდელობები;

ვ) სისტემური და აპარატურული შეცდომები და სხვა ანომალიები;

ზ) ქსელთაშორისი ეკრანისა და მარშრუტიზატორის აქტივობები;

თ) სააგენტოს კრიტიკულ, მკაცრად აკრძალულ, აკრძალულ და დაცულ საოფისე ზონაში შესვლა და გასვლა.

2. დროის აღმნიშვნელი ორგანოების მართვასთან დაკავშირებული ხდომილებებისა და ოპერაციების შესახებ ინფორმაცია აღირიცხება 15 წლის ვადით, ხოლო სხვა ინფორმაცია - 10 წლის ვადით.

მუხლი 121. შესრულებული მოქმედებების ჩანაწერების დამუშავების სიხშირე

შესრულებული მოქმედებების ჩანაწერები ავტომატურად გადადის სპეციალიზებულ სისტემაში, რომელიც საეჭვო აქტივობების აღმოჩენის შემთხვევაში შეტყობინებას უგზავნის შესაბამის პასუხისმგებელ პირებს.

მუხლი 122. აუდიტის ჩანაწერის შენახვა და დაცვა

1. ავტომატურ რეჟიმში შექმნილი აუდიტის ჩანაწერები ინახება შესაბამის სერვერებზე. ისინი ავტომატურად არქივდება.

2. ფიზიკური და ლოგიკური წვდომის კონტროლი გამოიყენება შესრულებული მოქმედებების ჩანაწერების (როგორც ელექტრონული, ასევე ბეჭდური) მიმართ მათი არაავტორიზებული ნახვის, შეცვლის, წაშლის ან მათზე სხვაგვარი წვდომის თავიდან ასაცილებლად. აუდიტის ჩანაწერები დაცულია არასანქცირებული წვდომისაგან, უზრუნველყოფილია მათი მთლიანობა და უცვლელობა.

მუხლი 123. შესრულებული მოქმედებების ჩანაწერების სარეზერვო ასლების აღების პროცედურა

აუდიტორული აღრიცხვის ჩანაწერების სარეზერვო ასლის აღება ხდება სააგენტოში დამტკიცებული ,,მონაცემთა ბაზების და პროგრამული უზრუნველყოფის სარეზერვო ასლების შექმნის პროცედურის“ შესაბამისად.

მუხლი 124. შესრულებული მოქმედებების მონაცემების შეგროვების სისტემა

1. პროგრამული უზრუნველყოფის ფუნქციონირების განმავლობაში შესრულებული მოქმედებების ჩანაწერებს რეალურ რეჟიმში აგროვებს და აანალიზებს ავტომატიზებული და ცენტრალიზებული სისტემა.

2. შესრულებული მოქმედებები, რომლებიც დაკავშირებულია მექანიკურ ოპერაციებთან, აღირიცხება სააგენტოს თანამშრომლების მიერ.

3. უსაფრთხოების ხარვეზები ფასდება სააგენტოს „ინფორმაციული უსაფრთხოების პოლიტიკის“ შესაბამისად.

მუხლი 125. ჩანაწერების არქივირება

სააგენტო ავტომატურად აარქივებს მონაცემებს „ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“ მიხედვით. არქივირებას ექვემდებარება წინამდებარე დოკუმენტში განსაზღვრული ჩანაწერები.

მუხლი 126. ელექტრონული არქივის უსაფრთხოება

1. ელექტრონული ჩანაწერების არქივი ინახება მონაცემთა დამუშავების ძირითად ცენტრში არსებულ ელექტრონულ სანახში.

2. არქივი დაცულია ნებისმიერი სახის ცვლილებისგან. დაცვის რეჟიმი განისაზღვრება ,,ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“ მიხედვით.

მუხლი 127. არქივის სარეზერვო ასლების აღების პროცედურა

1. არქივის სარეზერვო ასლების აღება ხორციელდება მონაცემების რეზერვირების ცენტრალიზებული და ავტომატიზებული სისტემის საშუალებით, არქივი გადაიტანება მონაცემთა დამუშავების სარეზერვო ცენტრში.

2. სარეზერვო ასლის აღება ხორციელდება სააგენტოში დამტკიცებული „მონაცემთა ბაზების და პროგრამული უზრუნველყოფის სარეზერვო ასლების შექმნის პროცედურის“ შესაბამისად. სარეზერვო ასლის აღების შესახებ ინფორმაცია აღირიცხება და პროცესის სტატუსის შესახებ ინფორმაცია მიეწოდება სისტემის ადმინისტრატორს.

3. სარეზერვო ასლის აღების პროცესის დასრულების შემდეგ სარეზერვო ასლს ავტომატურად ენიჭება დროის აღნიშვნა.

მუხლი 128. კომპრომეტირება და ავარიული აღდგენა

1. სანდო მომსახურების მიმწოდებლის უსაფრთხო სისტემის კომპრომეტირების, ასევე ინფორმაციის დაზიანების ან მისი ხელმიუწვდომლობის შემთხვევაში, ავარიული აღდგენა ხდება: „ღია გასაღების ინფრასტრუქტურის კომპონენტების ხდომილებების მართვის პროცედურის“, ,,მონაცემთა ბაზების და პროგრამული უზრუნველყოფის სარეზერვო ასლების შექმნის პროცედურის“, “ბიზნესის უწყვეტობის გეგმისა“ და „სახელმწიფო სერვისების განვითარების სააგენტოს ინფორმაციული ტექნოლოგიების ინციდენტების მართვის პროცედურის“ შესაბამისად.

2. დროის აღნიშვნის მომსახურების, გაუქმებული სერტიფიკატების სიისა და სერტიფიკატის შემოწმების ავტომატური მომსახურების მიწოდება ხდება პარალელურად მონაცემთა დამუშავების ძირითადი და სარეზერვო ცენტრებიდან. ერთ-ერთი ცენტრის გამორთვის შემთხვევაში მომსახურება არ შეწყდება.

მუხლი 129. სააგენტოს მიერ სანდო მომსახურების შეწყვეტა

1. სააგენტო შექმნილია ,,სახელმწიფო სერვისების განვითარების სააგენტოს შესახებ“ საქართველოს კანონის საფუძველზე და მის ერთ-ერთ ძირითად ფუნქციას წარმოადგენს, საქართველოს იუსტიციის მინისტრის ბრძანებით დადგენილი წესით „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონით გათვალისწინებული კვალიფიციური სანდო მომსახურებისა და სანდო მომსახურების მიწოდება და კრიპტოგრაფიული გასაღებების სერტიფიკატის შექმნა, გაცემა და მასთან დაკავშირებული მომსახურებების გაწევა. სააგენტოსთვის აღნიშნული ფუნქციების ჩამორთმევა შესაძლებელია, მხოლოდ საქართველოს პარლამენტის მიერ კანონმდებლობით დადგენილი წესით

აღნიშნულ კანონში ცვლილების შეტანით, რაც ასევე გულისხმობს „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონით დადგენილი წესით ამ ცვლილების გამოქვეყნებასაც.

2. სააგენტოს მიერ ერთი ან რამდენიმე სანდო და კვალიფიციური სანდო მომსახურების შეწყვეტის გეგმა მტკიცდება სააგენტოს თავმჯდომარის ინდივიდუალური ადმინისტრაციულ - სამართლებრივი აქტით. (ცვლილება 2021.06.07.N245/ს)

3. ამოღებულია (2021.06.07.N245/ს)

თავი XII

ტექნიკური უსაფრთხოების კონტროლი

მუხლი 130. სერტიფიკატების გამცემი ორგანოების გასაღების წყვილის შექმნა, ინსტალაცია და შენახვა

1. სერტიფიკატების გამცემი ორგანოების დახურული გასაღები იქმნება და ინახება უსაფრთხოების აპარატურულ მოდულში, რომელიც სერტიფიცირებულია FIPS 140-2 Level 3-ის მიხედვით. უსაფრთხოების აპარატურული მოდული მოთავსებულია სააგენტოს მონაცემთა დამუშავების ძირითად ცენტრში.

2. სერტიფიკატის გამცემი ძირითადი ორგანოს (GEO Root CA) 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.

3. გასაღების გენერაციის პროცედურა იმართება მონაცემთა დამუშავების ძირითად ცენტრში სერტიფიცირების ცენტრის პასუხისმგებელი თანამშრომლების მიერ.

4. გასაღებების წყვილის გენერაციისა და ინსტალაციის პროცედურები განსაზღვრულია „გასაღების წყვილის შექმნისა და სერტიფიკატის მექანიკურ რეჟიმში გაცემის პროცედურით“.

5. სერტიფიკატების გამცემი ორგანოების გასაღების წყვილის გენერაციისას გამოიყენება შემდეგი პარამეტრები: კრიპტოგრაფიული ალგორითმი RSA, გასაღების სიგრძე 4096 ბიტი.

მუხლი 131. სერტიფიკატის გამცემი ორგანოების გასაღებების ცვლილება

1. სერტიფიკატების გამცემი ორგანოების გასაღების ცვლილებისას ხდება გასაღების ახალი წყვილის გენერაცია და ღია გასაღებზე გაიცემა ახალი სერტიფიკატი სერტიფიკატის გამცემი ძირითადი ორგანოს მიერ.

2. სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების ცვლილების შემთხვევაში, იქმნება ორი სერტიფიკატი ახალ ღია გასაღებზე. პირველი (ე.წ. ბმული სერტიფიკატი) გაიცემა სერტიფიკატის გამცემი ძირითადი ორგანოს ძველი გასაღებით, ხოლო მეორე (თვითხელმოწერილი სერტიფიკატი) გაიცემა ახლად გენერირებული გასაღებით.

3. თუ სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღები იცვლება ძველი გასაღების კომპრომეტაციის გამო, სანდო მომსახურების მიმწოდებელს უფლება აქვს, არ გასცეს ბმული სერტიფიკატი. ამ შემთხვევაში, სერტიფიკატების გამცემი ძირითადი ორგანოს ახალი სერტიფიკატის გავრცელების წესი განისაზღვრება ბიზნესუწყვეტობის გეგმის მიხედვით.

4. გასაღების ცვლილების შემდეგ სერტიფიკატების გამცემი ორგანოს ძველი გასაღები გამოიყენება მხოლოდ იმ ვადის განმავლობაში, რომელიც აუცილებელია ძველი გასაღებით გაუქმებული სერტიფიკატების სიაზე ხელის მოსაწერად. მისი გამოყენებით სერტიფიკატები (გარდა ბმული სერტიფიკატისა) აღარ გაიცემა.

5. სერტიფიკატის გამცემი ორგანოს ძველი გასაღები მოქმედია მხოლოდ იმ ვადით, რა ვადითაც მოქმედებსმისი გამოყენებით გაცემული სერტიფიკატები. უკანასკნელი ასეთი სერტიფიკატის ვადის გასვლის შემდეგ, არაუმეტეს 1 თვის განმავლობაში, წყდება გაუქმებული სერტიფიკატების სიის წარმოება და გასაღები ნადგურდება.

6. გასაღების ცვლილების პროცედურა ტარდება შესაბამისი სერტიფიკატის ვადის გასვლამდე არანაკლებ 3 თვით ადრე, წინამდებარე დოკუმენტით განსაზღვრული წესით. საერთაშორისოდ აღიარებული სტანდარტებისა და რეკომენდაციების (მაგ., ETSI TS 119 312) შესაბამისად, გასაღების ცვლილების პროცედურა შეიძლება ჩატარდეს უფრო ადრეც, რათა გამოირიცხოს კომპრომეტაციის რისკი. შესაბამისი შინაგანაწესით შეიძლება დადგინდეს, ასევე, გასაღების ცვლილების უფრო მცირე ვადა.

7. ახალი სერტიფიკატი ვრცელდება წინამდებარე დოკუმენტის შესაბამისად.

მუხლი 132. გასაღების მართვის ოპერაციებში მონაწილე პერსონალის აუცილებელი რაოდენობა

სერტიფიკატების გამცემი ორგანოს გასაღების მართვის ნებისმიერ ოპერაციაში (შექმნა, სარეზერვო ასლის აღება, აღდგენა, აქტივაცია შემდგომი გამოყენებისთვის, განადგურება და სხვა) აუცილებელია სანდო მომსახურების მიმწოდებლის მინიმუმ ორი, ხოლო ზოგიერთ შემთხვევაში, სამი ან მეტი თანამშრომლის მონაწილეობა.

მუხლი 133. დახურული გასაღების სარეზერვო ასლი

1. სერტიფიკატების გამცემი ორგანოს გასაღების შექმნისთანავე, სააგენტოს მონაცემთა დამუშავების სარეზერვო ცენტრში დაცული ქსელური შეერთების გამოყენებით ავტომატურ რეჟიმში იქმნება მისი სარეზერვო ასლი უსაფრთხოების აპარატურულ მოდულში ან მის მოსახსნელ სეგმენტში. იმის მიხედვით, თუ როგორ ინახება ორიგინალი. აღნიშნული რეგულირდება „ღია გასაღების ინფრასტრუქტურის უსაფრთხოების აპარატურული მოდულის მართვის პროცედურით“.

2. სუბიექტის დახურული გასაღების სარეზერვო ასლის აღება დაუშვებელია, გარდა იმ შემთხვევისა, როდესაც აღნიშნული საკითხი ცხადად განისაზღვრება წინამდებარე შინაგანაწესით.

3. დაუშვებელია დროის კვალიფიციური აღნიშვნის, სერტიფიკატის ავტომატური შემოწმების მომსახურების დახურული გასაღებების სარეზერვო ასლის შექმნა.

4. დაუშვებელია სერტიფიკატის გამცემი ორგანოების, დროის კვალიფიციური აღნიშვნის, სერტიფიკატის ავტომატური შემოწმების მომსახურების დახურული გასაღებების მესამე პირისთვის მიბარება.

მუხლი 134. გასაღების წყვილის აქტივაციის მონაცემები და განადგურება

1. სერტიფიკატების გამცემი ორგანოების, დროის კვალიფიციური აღმნიშვნელი ერთეულების, სერტიფიკატის ავტომატური შემოწმების მომსახურების გასაღების წყვილის აქტივაციის მონაცემების ტიპები განისაზღვრება უსაფრთხოების კრიპტოგრაფიული მოდულების მწარმოებლის მიერ. აღნიშნული მონაცემების მართვის წესი განისაზღვრება „ღია გასაღების ინფრასტრუქტურის უსაფრთხოების აპარატურული მოდულის მართვის პროცედურით“.

2. უსაფრთხოების აპრატურული მოდულის ფუნქციონირების პერიოდის ამოწურვისას, მასში არსებული ყველა გასაღები, როგორც ძირითადი, ასევე სარეზერვო ასლი ნადგურდება საამისოდ უფლებამოსილი პირების მიერ მწარმოებლის ინსტრუქციების მიხედვით.

3. სუბიექტის მონაცემების აქტივაციის მონაცემების ადმინისტრირების საკითხი რეგულირდება წინამდებარე შინაგანაწესით.

მუხლი 135. კომპიუტერული უსაფრთხოების კონტროლი

სანდო მომსახურების მიმწოდებლის კომპიუტერული უსაფრთხოების კონტროლი უზრუნველყოფილია შემდეგი კომპონენტებით:

ა) შესაბამის აპარატურაზე ან მოწყობილობაზე პასუხისმგებელი თანამშრომლების წვდომა და მათი უფლებები განსაზღვრულია და კონტროლდება;

ბ) აღირიცხება წვდომის შემთხვევები;

გ) არაავტორიზებული წვდომა შეუძლებელია;

დ) მგრძნობიარე კრიპტოგრაფიული ინფორმაცია (მაგ., დახურული გასაღები) ინახება უსაფრთხო წესით. სერტიფიკატის გამცემი ორგანოების გასაღებები მოთავსებულია უსაფრთხოების აპარატურულ მოდულებში, რომლებიც სერტიფიცირდება წინამდებარე შინაგანაწესით განსაზღვრული მოთხოვნების შესაბამისად.

მუხლი 136. სასიცოცხლო ციკლის უსაფრთხოების კონტროლი

1. თითოეული პროგრამული კომპონენტი, რომელიც შემუშავებულია სააგენტოს ძალებით, განთავსებულია საწყისი კოდის და ვერსიების მართვისათვის განკუთვნილ სპეციალურ სანახებში და ხელმისაწვდომია ავტორიზებული პირებისათვის. განსაკუთრებით მნიშვნელოვანი სისტემების შექმნისას ტარდება ურთიერთგადამოწმების პროცედურები. შემუშავებული სისტემები საწარმოო გარემოში გაშვებამდე გადიან ტესტირებას.

2. ნებისმიერი სახის ცვლილება ხორციელდება სააგენტოს ცვლილებების მართვის პროცესის შესაბამისად.

მუხლი 137. ქსელის უსაფრთხოების კონტროლი

სანდო მომსახურების მიწოდებასთან დაკავშირებული, აპარატურისთვის საჭირო ქსელური ინფრასტრუქტურა განთავსებულია სააგენტოს მონაცემთა დამუშავების ძირითად და სარეზერვო ცენტრებში. სააგენტოს საქსელო არქიტექტურა დაფუძნებულია საუკეთესო გამოცდილებაზე. აგებულია მრავალდონიანი დაცვის სისტემა. ქსელის შიდა და გარე პერიმეტრი, შიდა ქსელის სხვადასხვა ლოგიკური სეგმენტის შორის შეერთებების ჩათვლით, კონტროლდება ქსელური ეკრანების (Firewall) სისტემით. მომსახურების მიწოდების მდგრადობისთვის გამოყენებულია დატვირთვის გამანაწილებელი ტექნოლოგია. ყველა ქსელური შეერთება კონტროლდება და აღირიცხება.

მუხლი 138. დროის აღნიშვნა

დროის აღნიშვნა სხვადასხვა მონაცემში დაფუძნებულია UTC-სთან გასწორებულ დროის სანდო წყაროზე. გარდა დროის აღმნიშვნელი ერთეულებისა, საათი სწორდება სტანდარტული საშუალებებით. დროის აღმნიშვნელ ერთეულებზე საათის გასწორებისა და დროის კონტროლის საკითხი რეგულირდება ამ დოკუმენტით.

თავი XIII

შესაბამისობის აუდიტი

მუხლი 139. აუდიტის და შეფასების სიხშირე

1. აუდიტორული შემოწმება ტარდება ორ წელიწადში ერთხელ დამოუკიდებელი აუდიტორის მიერ, სააგენტოს ხარჯით.

1[1]. სააგენტო ვალდებულია, საჯარო სამართლის იურიდიულ პირს - ციფრული მმართველობის სააგენტოს წარუდგინოს აუდიტის დასკვნა მისი მიღებიდან 3 დღის ვადაში.

2. შიდა აუდიტორული შემოწმებები ტარდება შიდა აუდიტის სამსახურის მიერ შემუშავებული აუდიტის გეგმის მიხედვით და საჭიროებისამებრ.

3. რეგულაციებიდან, სერტიფიცირებიდან ან/და სახელშეკრულებო ვალდებულებებიდან გამომდინარე, აუდიტი ასევე შესაძლებელია განხორციელდეს სახელმწიფო კონტროლის ან/და მარეგულირებელი/მასერტიფიცირებელი ორგანოების მიერ.

4. აუდიტორული შემოწმება განგრძობადი პროცესია, რომელიც შეიძლება შედგებოდეს რამდენიმე შემოწმების შედეგად რეკომენდაციების შემუშავების, მათი შესრულებისა და შესრულების ხარისხის მონიტორინგის მიზნით.

მუხლი 140. აუდიტორის კვალიფიკაცია და მიუკერძოებლობა

1. აუდიტორს უნდა გააჩნდეს სანდო მომსახურების მიმწოდებლების შემოწმებისა და შეფასების შესაბამისი კვალიფიკაცია და გამოცდილება.

2. აუდიტორი უნდა იყოს სააგენტოსგან დამოუკიდებელი, უნდა მოქმედებდეს ობიექტურად და მიუკერძოებლად და არ უნდა გააჩნდეს ინტერესთა კონფლიქტი შესრულებულ/შესასრულებელ სამუშაოსთან.

მუხლი 141. აუდიტორული შემოწმების შეფასების მასშტაბი და შეფასების საკითხები

1. აუდიტორული შემოწმების დანიშნულებაა სანდო მომსახურების მიმწოდებლის ყოველდღიური ფუნქციონირების შესაბამისობის შემოწმება შინაგანაწესის მოთხოვნებთან, სააგენტოში დამტკიცებულ პოლიტიკებთან/ინსტრუქციებთან და საქართველოს კანონმდებლობასთან.

2. აუდიტორული შემოწმებების შედეგები და შესაბამისი რეკომენდაციები აისახება აუდიტორის ანგარიშში, რომელსაც აუდიტორი წარუდგენს სააგენტოს.

მუხლი 142. შეუსაბამობის აღმოსაფხვრელად გასატარებელი ღონისძიებები

1. აუდიტორული შემოწმების შედეგად შეუსაბამობის აღმოჩენის შემთხვევაში, აუდიტორთან შეთანხმებით განისაზღვრება:

ა) შეუსაბამობის აღმოსაფხვრელად საჭირო სამუშაოების გეგმა;

ბ) მომდევნო შემოწმების თარიღი.

2. თუ აუდიტორული შემოწმების შედეგად აღმოჩენილი შეუსაბამობების აღმოფხვრა დაკავშირებულია მნიშვნელოვან დანახარჯებთან, გადაწყვეტილებას შემდგომი მოქმედებების თაობაზე იღებს სააგენტოს თავმჯდომარე.

3. აუდიტორული შემოწმებების შესახებ ანგარიშები და საბოლოო დასკვნა წარედგინება სააგენტოს ხელმძღვანელობას. ინფორმაცია საბოლოო დასკვნის შესახებ შესაძლებელია ხელმისაწვდომი გახდეს ნებისმიერი დაინტერესებული პირისათვის.

მუხლი 143. ტესტირების ხელშეწყობა

1. სანდო მომსახურებათა ინტეგრაციისა და ტესტირების მიზნით, სააგენტოს გააჩნია სატესტო ინფრასტრუქტურა, რომელიც იყენებს სპეციალურად ამ მიზნისთვის არსებულ უსაფრთხოების აპარატურულ მოდულებს ან/და მათ ლოგიკურ სეგმენტებს. პროგრამული უზრუნველყოფა ინსტალირებულია ცალკე სერვერებზე, რომლებიც ჩართულია განცალკევებულ კომპიუტერულ ქსელში.

2. სატესტო ინფრასტრუქტურაში მოქმედი სერტიფიკატის გამცემი ორგანოები გამოიყენება მხოლოდ ტესტირების მიზნებისათვის (მაგ., სატესტო სერტიფიკატების გასაცემად). ამგვარი ორგანოების სუბიექტის დასახელება იწყება ტექსტით “Test”.

3. დროის აღმნიშვნელი სატესტო ერთეულების სერტიფიკატები გაიცემა სერტიფიკატის გამცემი სატესტო ორგანოების მიერ.

4. სატესტო ინფრასტრუქტურაში სერტიფიკატის გამცემი სატესტო ორგანოების ან/და დროის აღნიშვნის სატესტო მომსახურების ამოქმედება და შეჩერება, ასევე, შესაბამისი სერტიფიკატებისა და მომსახურების მიწოდება ხდება სანდო მომსახურების მიმწოდებლის ხელმძღვანელის თანხმობის საფუძველზე - სააგენტოში შემოსული ოფიციალური მოთხოვნის ან/და მომხმარებელთან დადებული ხელშეკრულების შესაბამისად.

5. იმ შემთხვევაში, როდესაც სერტიფიკატი გაიცემა სააგენტოს მიერ გაცემულ სუბიექტის მოწყობილობაზე 35-ე და 50-ე მუხლებით განსაზღვრული მომსახურებების ტესტირების მიზნით, შესაძლებელია სერტიფიკატები მომხმარებელზე გაიცეს სააგენტოს ელექტრონულ მატარებელზე დატანილი (ჩაწერილი) ფორმით. ამ შემთხვევაში გასაღების წყვილის ელექტრონულ მატარებელზე გენერაციაზე და სერტიფიკატების დატანაზე პასუხისმგებელია ბიომეტრიული დოკუმენტების პერსონალიზაციის ცენტრი (სამსახური). ყველა სხვა მომსახურების შემთხვევაში სატესტო სერტიფიკატების შექმნას და გაცემას ახორციელებს სერტიფიცირების ცენტრი რა დროსაც გასაღების წყვილის შექმნის საკითხები რეგულირდება ურთიერთშეთანხმებით.

6. თითოეული მომსახურების შესაბამისი სატესტო სერტიფიკატების ტექნიკური პროფილები შეესაბამება ამ შინაგანაწესის N2-დანართით დადგენილ მოთხოვნებს.

დანართი N1(ცვლილება 2021.06.07.N245/ს)

განცხადება

კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების/კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატებთან ერთად პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების განმეორებით გაცემა

წარმოდგენილი დოკუმენტი:

რეგისტრაციის თარიღი:

რეგისტრაციის №

გაცემის თარიღი:

მომსახურებისათვის გადასახდელი თანხა:

1. პირადი №
2. გვარი:
3. სახელი:
4. დაბადების თარიღი:
5. პირადობის/ბინადრობის მოწმობის **№** N
6. ტელ. მობ.:
7. ელფოსტა:
8. მოთხოვნა:

განცხადება მიიღო (გვარი, სახელი):

_____

(ხელმოწერა)

სამახსოვრო ბარათი

კვალიფიციური ელექტრონული ხელმოწერისა და ავთენტიფიკაციის სერტიფიკატების/კვალიფიციური ელექტრონული ხელმოწერის და ავთენტიფიკაციის სერტიფიკატებთან ერთად პერსონალური ავთენტიფიკაციის, კვალიფიციური ელექტრონული ხელმოწერის აქტივაციისა და განბლოკვის კოდების განმეორებით გაცემა

რეგისტრაციის თარიღი:

რეგისტრაციის №

კოდი:

გაცემის თარიღი:

მომსახურეობისთვის გადასახდელი თანხა:

1.პირადი №

2.გვარი:

3.სახელი:

4.პირადობის სერიული №

გაცნობებთ, რომ:

1. პერსონალური მონაცემები დამუშავდება კანონით გათვალისწინებული ფორმით, მოცულობით და მიზნის მისაღწევად;

2. სამახსოვრო ბარათში მითითებული განაცხადის ნომრისა და კოდით, შესაძლებელი იქნება საქმისწარმოების სტატუსის (დამზადდა, დახარვეზდა, მიღებულია უარყოფითი გადაწყვეტილება) შესახებ ინფორმაციის მიღება სატელეფონო კონსულტაციის საშუალებით;

3. 10 დღის განმავლობაში საფასურის გადაუხდელობის შემთხვევაში კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატი არ გააქტიურდება;

4. გადმოგეცემათ კვალიფიციური ელექტრონული ხელმოწერისა და ფიზიკური პირის ავთენტიფიკაციის სერტიფიკატის მომსახურების წესები და პირობები, რომლის ჩაბარებასაც ადასტურებთ სამახსოვრო ბარათზე ხელმოწერით.

5. მოთხოვნა: კოდების გაცემა/

სერტიფიკატების განახლება

სამახსოვრო ბარათი ჩავიბარე:

ხელმოწერა

განცხადება მიიღო:

სახელმწიფო სერვისების განვითარების სააგენტო

იუსტიციის სახლი

ვებ გვერდები: www.sda.gov.ge და www.psh.gov.ge

სატელეფონო სამსახური: 2 405 405

სერტიფიკატის ტექნიკური პროფილები

1. GEO Signing CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის [illegible]	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვლილებადი (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)		+	GEO Signing 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 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=1.3.6.1.4.1.37733.10.3.1.1.0 [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			KeyID=93 00 66 db 95 51 d3 87 90 78 07 92 22 ed 30 6f 60 e5 88 bf	-	+

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/GEORootCA.crt		

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

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)		+	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 სახელი (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, 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 (Critical)	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=1.3.6.1.4.1.37733.10.3.1.1.0 [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/geosigningcag(n).crl	-	+

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/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-semanticsId-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		

3. Biometric Encryption CA

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვლებადი (Changeable)	აღწერილობა (Description)
ვერსია (Version)			+	V3	-	სერტიფიკატის ფორმატის ვერსია
სერიული ნომერი (Serial Number)			+	53E43DC35143EE526A2FCE2B6CDA0940D80FBFF5	-	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)			+	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 დასახელება
	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	+	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 იდენტიფიკატორი (OID)**	**მნიშვნელობა და შეზღუდვები (Values and Limitations)**	**კრიტიკულობა**	**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		

4. Biometric Data Encryption

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი	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 დასახელება
	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, 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	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 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 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 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)		+	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 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=1.3.6.1.4.1.37733.10.4.1.1.0 [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)				-	+
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 იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი	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 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 სახელი (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 (Giventname) (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, 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	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=1.3.6.1.4.1.37733.10.4.1.1.0 [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/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 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/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	-	-

7. GEO ESeal CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი	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)		+	GEO ESeal 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 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=1.3.6.1.4.1.37733.10.7.1.1.0 [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/georootca.crl	-	+
სერტიფიკატის გამცემი ძირითადი ორგანოს გასაღების			KeyID=93 00 66 db 95 51 d3 87 90 78 07 92 22 ed 30 6f 60 e5 88 bf	-	+

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/GEORootCA.crt		

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

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვლადებადი (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 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, 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	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/geoesealcag(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 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		

9. GEO Root 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)			+	5b 6f fb 51 f1 d4 05 d6	-	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)			+	2011 წლის 07 07, 18:02:27	-	სერტიფიკატის ძალაში შესვლის თარიღი
ძალაშია (-მდე) (Valid to)			+	2032 წლის 01 07, 18:02:27	-	სერტიფიკატის მოქმედების შეწყვეტის თარიღი
სუბიექტის უნიკალური დასახელება (Subject Distinguished Name)			+		+	სერტიფიკატების ინფრასტრუქტურაში სუბიექტის 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
	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 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)			93 00 66 db 95 51 d3 87 90 78 07 92 22 ed 30 6f 60 e5 88 bf	-	+

10. GEO OCSP Signer

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვლადები (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)		+		-	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)		+		+	სერტიფიკატის ავტომატური შემოწმების 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)		End Entity		
	გზის სიგრძის შეზღუდვა (Path Length Constraint)		None		
გასაღების გამოყენება (Key Usage)				+	+
			Digital Signature		
CRL-ის გავრცელების წერტილები (CRL Distribution Points)				-	-
გასაღების გაფართოებული გამოყენება (Extended Key Usage)			OCSP Signing	-	+
სერტიფიკატის გამცემი ორგანოს გასაღების იდენტიფიკატორი (Authority Key Identifier)				-	+
სუბიექტის გასაღების იდენტიფიკატორი (Subject Key Identifier)				-	+

სერტიფიკატის გამცემი ორგანოს ინფორმაციის ხელმისაწვდომობა (Authority Information Access)				-	-
სერტიფიკატის ავტომატური შემოწმება (id-pkix-ocsp-nocheck)				-	- (გამოიყენება მხოლოდ OCSP პასუხის სერტიფიკატში)

11. SDA TimeStamping CA

სერტიფიკატის ველები

ველის დასახელება (Field)		ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი	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	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/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		

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 (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	-	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, 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/sdatimestampingca.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/TimeStampingCA.crt		

13. GEO Organizational Authentication CA G(n)

სერტიფიკატის ველები

ველის დასახელება (Field)	ველის ობიექტის იდენტიფიკატორი (OID)	სავალდებულო (Mandatory)	მნიშვნელობა (Value)	ცვალებადი	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)		+	GEO Organizational 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 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=1.3.6.1.4.1.37733.10.8.1.1.0 [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/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)		URI: http://aia.id.ge/pki/GEORootCA.crt		

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

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)		+	GEO Organizational 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 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, 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 (Critical)	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 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		

N3 დანართი

სუბიექტის მიერ წარმოდგენილ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემა სუბიექტის მიერ წარმოდგენილ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების მონაცემები

4.1 მწარმოებელი ქვეყანა: _____

4.2 მწარმოებელი კომპანია: _____

4.3 მოდელი: _____

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

„დოკუმენტი არის ელექტრონული. ორიგინალი ელექტრონული დოკუმენტი ხელმისაწვდომია ვებ გვერდზე http://sda.gov.ge. აღნიშნული ვებ გვერდიდან (http://sda.gov.ge) დოკუმენტის ჩამოტვირთვა შესაძლებელია XXXXXX ნომრით. ელექტრონული დოკუმენტის ამონაბეჭდი წარმოადგენს მის ასლს.“

N4 დანართი

სუბიექტის ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემა სუბიექტის ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების მონაცემები

4.1 მწარმოებელი ქვეყანა: _____

4.2 მწარმოებელი კომპანია: _____

4.3 მოდელი: _____

4.4 ინფრასტრუქტურის ადგილმდებარეობა: _____

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. კვალიფიციური ელექტრონული შტამპის გაცემის პოლიტიკასკვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

„დოკუმენტი არის ელექტრონული. ორიგინალი ელექტრონული დოკუმენტი ხელმისაწვდომია ვებ გვერდზე http://sda.gov.ge. აღნიშნული ვებ გვერდიდან (http://sda.gov.ge) დოკუმენტის ჩამოტვირთვა შესაძლებელია XXXXXX ნომრით. ელექტრონული დოკუმენტის ამონაბეჭდი წარმოადგენს მის ასლს.“

N5 დანართი

სახელმწიფო სერვისების განვითარების სააგენტოს მიერ გაცემულ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: კვალიფიციური ელექტრონული შტამპის სერტიფიკატის სახელმწიფო სერვისების განვითარების სააგენტოს მიერ გაცემულ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე ვიზუალურად დასატანი სუბიექტის დასახელება (მაქს. 38 სიმბოლო თითოეულ ნაწილში)

4.1 ქართ. I ნაწილი _____

4.2 ქართ. II ნაწილი _____

4.3 ინგლ. I ნაწილი _____

4.4 ინგლ. II ნაწილი _____

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას

3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

„დოკუმენტი არის ელექტრონული. ორიგინალი ელექტრონული დოკუმენტი ხელმისაწვდომია ვებ გვერდზე http://sda.gov.ge. აღნიშნული ვებ გვერდიდან (http://sda.gov.ge) დოკუმენტის ჩამოტვირთვა შესაძლებელია XXXXXX ნომრით. ელექტრონული დოკუმენტის ამონაბეჭდი წარმოადგენს მის ასლს.“

N6 დანართი

სახელმწიფო სერვისების განვითარების სააგენტოს ინფრასტრუქტურაში ინტეგრირებული კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემის შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: კვალიფიციური ელექტრონული შტამპის სერტიფიკატის სახელმწიფო სერვისების განვითარების სააგენტოს ინფრასტრუქტურაში ინტეგრირებულ კვალიფიციური ელექტრონული შტამპის შექმნის საშუალებაზე

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. სუბიექტის წარმომადგენელი

4.1 პირადი ნომერი: _____

4.2 სახელი და გვარი: _____

4.3 ტელეფონის ნომერი: _____ 4.4 მობილურის ნომერი:_____

4.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. კვალიფიციური ელექტრონული შტამპისა და ორგანიზაციის ავთენტიფიკაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

„დოკუმენტი არის ელექტრონული. ორიგინალი ელექტრონული დოკუმენტი ხელმისაწვდომია ვებ გვერდზე http://sda.gov.ge. აღნიშნული ვებ გვერდიდან (http://sda.gov.ge) დოკუმენტის ჩამოტვირთვა შესაძლებელია XXXXXX ნომრით. ელექტრონული დოკუმენტის ამონაბეჭდი წარმოადგენს მის ასლს.“

N7 დანართი

ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემის შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატის გაცემა

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. ელექტრონული ხელმოწერის დეშიფრაციის ინსტრუმენტის მოწოდებაზე უფლებამოსილი პირის მონაცემები

4.1 ორგანიზაციის დასახელება: _____

4.2 სახელი და გვარი: _____

4.3 ელ ფოსტის მისამართი: _____

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

„დოკუმენტი არის ელექტრონული. ორიგინალი ელექტრონული დოკუმენტი ხელმისაწვდომია ვებ გვერდზე http://sda.gov.ge. აღნიშნული ვებ გვერდიდან (http://sda.gov.ge) დოკუმენტის ჩამოტვირთვა შესაძლებელია XXXXXX ნომრით. ელექტრონული დოკუმენტის ამონაბეჭდი წარმოადგენს მის ასლს.“

ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის ინსტრუმენტის მახასიათებლები

1. ბიომეტრიული მონაცემების შემგროვებელი სუბიექტის მიერ მოწოდებული დაშიფრული ელექტრონული ხელმოწერის ბიომეტრიული დეშიფრაციის ინსტრუმენტი (შემდგომში - ინსტრუმენტი) უნდა იყოს შექმნილი პროგრამირების ენა Java-ზე (მოწოდების ფორმატი zip არქივი), რომლის საქაღალდეების სტრუქტურა მოცემული უნდა იყოს შემდეგი სახით:

   არქივი „biodecryption“
   ..src
   ....main
   ......java
   ....Java-ფაილები და პაკეტების შესაბამისი ქვესაქაღალდეები
   ......resources
   ....META-INF
   ....services
   ..... ge.gov.sda.signpad.SignPADSignatureDecrypter (ფაილი)
   ..lib

სადაც დასაშვებია, ცარიელი დირექტორიები იყოს გამოტოვებული.

2. ამ მუხლის პირველი პუნქტის შესაბამისად src/main/resources/META-INF/services საქაღალდეში განთავსებული ge.gov.sda.signpad.SignPADSignatureDecrypter ფაილი მოცემული უნდა იყოს ტექსტური ფაილის სახით, რომელშიც დეშიფრაციის ინსტრუმენტის ძირითადი კლასის დასახელება სრულად უნდა იყოს მითითებული (მაგ.: ge.vendorname.signpad.SignatureDecrypterImpl)

3. დეშიფრაციის ინსტრუმენტის ძირითადი კლასის საწყისი კოდი (ისევე როგორც საწყისი კოდი ნებისმიერი სხვა კლასისა, რომელიც მოწოდებულია დეშიფრაციის ინსტრუმენტის ფარგლებში) მოთავსებული უნდა იყოს ამავე მუხლის პირველი პუნქტის შესაბამისად განსაზღვრულ src/main/java დირექტორიაში, რომელიც უნდა ახდენდეს შემდეგი Java ინტერფეისის რეალიზაციას:

```
package ge.gov.sda.signpad;

import java.io.InputStream;

public interface SignPADSignatureDecrypter {

   byte[] decryptSignature(byte[] signatureData, InputStream keyStore, char[]
   ksPassword, String ksType, String keyAlias, char[] keyPassword);

   }
```

4. დეშიფრაციის ინსტრუმენტის ძირითად კლასს აუცილებლად უნდა ეწეროს ანოტაცია ge.gov.sda.signpad.Description, რომელსაც პარამეტრად გადაეცემა კლასის აღწერა. ანოტაციაში, სულ მცირე, მითითებული უნდა იყოს ხელმოწერის მოწყობილობის მწარმოებლის დასახელება. ამასთან, დასაშვებია, სხვა ინფორმაციას. სასურველია, ანოტაციის ტექსტის ზომა არ აღემატებოდეს 30 სიმბოლოს.

5. სააგენტოს მიერ განსაზღვრული ინტერფეისი ge.gov.sda.signpad.SignPADSignatureDecrypter და ანოტაცია ge.gov.sda.signpad.Description მომხმარებელს გადაეცემა კომპილირებულ მდგომარეობაში, jar ფაილის სახით. შესაბამისად, მოწოდებული Java-კლასებიდან არც ერთი არ უნდა მოთავსდეს პაკეტში ge.gov.sda.

6. დამატებითი ფაილების სახით დასაშვებია, მოწოდებული zip არქივის ძირითად საქაღალდეში მოთავსებული იყოს, ასევე, pom.xml ფაილი, რომელიც შექმნილი იქნება Apache Maven 2/3 წესების მიხედვით. ამ შემთხვევაში, არტიფაქტის ჯგუფის იდენტიფიკატორი (groupId) უნდა ემთხვეოდეს მოწოდებულ zip არქივში გამოყენებულ Java-პაკეტს ან წარმოადგენდეს მის პრეფიქსს.

7. სააგენტო იტოვებს უფლებას, არ მიიღოს დაშიფრული ბიომეტრიის დეშიფრაციის ინსტრუმენტი და მოითხოვოს მასში ცვლილებების შეტანა, თუკი მიიჩნევს, რომ მოწოდებული Java-კოდი არ შეესაბამება პროგრამირების ენისთვის - Java-სთვის - დადგენილ, ხარისხიანი პროგრამული კოდის საყოველთაოდ მიღებულ სტანდარტებს ან თუ გაჩნდება ეჭვი, რომ აღნიშნული Java-კოდი საფრთხეს უქმნის შიფრაციის დახურული გასაღების კონფიდენციალობას ან სხვაგვარად აზიანებს სააგენტოს ინფრასტრუქტურაში არსებულ პროგრამულ ან/და აპარატურულ სისტემებს.

8. იმ შემთხვევაში, თუკი გადმოცემული კოდის კომპილაციისა და შემდგომი შესრულებისთვის საჭირო იქნება დამატებითი ბიბლიოთეკების გამოყენება, ისინი უნდა მოთავსდეს lib დირექტორიაში. სააგენტო უფლებას იტოვებს, მოითხოვოს თითოეული ასეთი ფაილის წარმომავლობის დადასტურება. თითოეული გამოყენებული ბიბლიოთეკა უნდა აკმაყოფილებდეს, სულ მცირე, ერთ მოთხოვნას:

   ა) შექმნილი უნდა იყოს მოწყობილობის მწარმოებლის მიერ და სააგენტოსთვის ხელმისაწვდომი მწარმოებლის ვებგვერდიდან;

   ბ) შექმნილი უნდა იყოს მოწყობილობის მწარმოებლის მიერ და ატარებდეს მოწყობილობის მწარმოებლის სწორ ციფრულ ხელმოწერას, დადასტურებულს სერტიფიკატის საერთაშორისოდ აღიარებული გამცემის მიერ გაცემული სერტიფიკატით;

   გ) შექმნილი უნდა იყოს მოწყობილობის მწარმოებლის ან მესამე პირის მიერ და სააგენტოსთვის ხელმისაწვდომი იყოს მისი საწყისი კოდი, ანალიზის და შემდგომი კომპილაციის საშუალებით.

N9 დანართი

ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაციის მომსახურების მიღების შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის დახურული გასაღებისა და შესაბამისი სერტიფიკატის შენახვისა და ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების დეშიფრაცია

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

2.3 დასახელება ინგლისურად: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. სუბიექტის წარმომადგენელი

4.1 პირადი ნომერი: _____

4.2 სახელი და გვარი: _____

4.3 ტელეფონის ნომერი: _____ 4.4 მობილურის ნომერი:_____

4.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. ელექტრონული ხელმოწერის ბიომეტრიული მონაცემების შიფრაციის სერტიფიკატების გაცემისა და მომსახურების პოლიტიკას
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

N10 დანართი

დროის კვალიფიციური აღნიშვნის მომსახურების გარანტირებული წარმადობით მიღების შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: დროის კვალიფიციური აღნიშვნა გარანტირებული წარმადობით

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. მომსახურების კონფიგურაცია

4.1 მომხმარებლის IP მისამართი: _____

4.2 გარანტირებული წარმადობით მომსახურების კონფიგურაცია

კვირის დღეები	დღის მონაკვეთების რაოდენობა	დღის I მონაკვეთი		დღის II მონაკვეთი		დღის III მონაკვეთი	
		მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში	მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში	მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში
ორშაბათი - პარასკევი							
შაბათი							
კვირა							

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებსა და პირობებს
2. დროის კვალიფიციური აღნიშვნის გაწევისა და მომსახურების პოლიტიკა
3. სანდო მომსახურების მიმწოდებლის შინაგანაწესს

N11 დანართი

სერტიფიკატის ავტომატური შემოწმების მომსახურების გარანტირებული წარმადობით მიღების შესახებ განცხადების დანართი

შექმნის თარიღი: _____

ნომერი: _____

კოდი: _____

1. მომსახურება: სერტიფიკატის ავტომატური შემოწმება გარანტირებული წარმადობით

2. სუბიექტის მონაცემები

2.1 საიდენტიფიკაციო კოდი: _____

2.2 დასახელება: _____

3. სუბიექტის საკონტაქტო ინფორმაცია

3.1 იურიდიული მისამართი: _____

3.2 ფაქტობრივი მისამართი: _____

3.3 ტელეფონის ნომერი: _____ 3.4 მობილურის ნომერი: _____

3.5 ელ ფოსტის მისამართი: _____

4. მომსახურების კონფიგურაცია

4.1 მომხმარებლის IP მისამართი: _____

4.2 გარანტირებული წარმადობით მომსახურების კონფიგურაცია

კვირის დღეები	**დღის მონაკვეთების რაოდენობა**	**დღის I მონაკვეთი**		**დღის II მონაკვეთი**		**დღის III მონაკვეთი**	
		მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში	მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში	მონაკვეთის დასაწყისი და დასასრული (24- საათიანი ფორმატი)	წარმადობა წამში
ორშაბათი - პარასკევი							
შაბათი							
კვირა							

5. სუბიექტის წარმომადგენელი

5.1 პირადი ნომერი: _____

5.2 სახელი და გვარი: _____

5.3 ტელეფონის ნომერი: _____ 5.4 მობილურის ნომერი:_____

5.5 ელ ფოსტის მისამართი: _____

დანართის წარდგენით სუბიექტი ეთანხმება:

1. მომსახურების ზოგად წესებს და პირობებს
2. სანდო მომსახურების მიმწოდებლის შინაგანაწესს