ღია ფინანსების სისტემაში მომხმარებლის ელექტრონული იდენტიფიკაციისა და ავთენტიფიკაციის მომსახურების სტანდარტი

ვერსია 0.3.RC1

1 დოკუმენტის შესახებ

მომხმარებლის იდენტიფიკაცია და ავთენტიფიკაცია ფინანსური და სხვა მომსახურების ერთ-ერთი უმნიშვნელოვანესი რგოლია და წარმოადგენს „იცნობდე შენს მომხმარებელს“ (Know Your Customer) პირველ, ძალიან საპასუხისმგებლო ნაბიჯს. ფინანსური (ან სხვა) მომსახურების მიმწოდებელმა, მაგალითად კომერციულმა ბანკმა, მომხმარებლის იდენტიფიკაცია და ავთენტიფიკაცია შესაძლოა საკუთარი ძალებით აწარმოოს, თუმცა ელექტრონული სისტემების განვითარებასთან ერთად, უკვე არსებობს საშუალება ამგვარმა მიმწოდებლებმა საკუთარი მომხმარებლების იდენტიფიკაციისა და ავთენტიფიკაციის პროცედურა სხვა მხარეებს, ე.წ. იდენტობის პროვაიდერებს მიანდონ.

წინამდებარე დოკუმენტის მიზანია მოხდეს მომხმარებლების იდენტიფიკაციისა და ავთენტიფიკაციის სტანდარტის შემუშავება იმ შემთხვევაში, როდესაც აღნიშნული პროცესი მესამე პირზე (იდენტობის პროვაიდერზე) არის მინდობილი.

დოკუმენტის დანიშნულება არ არის ჩაანაცვლოს NextGenPSD2 XS2A ჩარჩოს მიხედვით მომხმარებლის იდენტიფიკაციისა და ავთენტიფიკაციის სისტემა, რომლებიც განსაზღვრულია (1) და (2)-ით.

იმ გასაღები სიტყვების ქართული თარგმანების ინტერპრეტაცია, რომელიც მოცემულია ცხრილი 1-ში ("MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", და "OPTIONAL") უნდა მოხდეს (3) შესაბამისად. ტერმინებს ეს მნიშვნელობა აქვთ მხოლოდ იმ შემთხვევაში, როცა ისინი **მსხვილი მხედრული** ან/და ᲛᲗᲐᲕᲠᲣᲚᲘ (მთავრული) შრიფტით არიან გამოყენებული.

English	**ქართული**
MUST	უნდა
MUST NOT	არ უნდა
REQUIRED	სავალდებულოა
SHALL	აუცილებელია
SHALL NOT	არავითარ შემთხვევაში
SHOULD	უმჯობესია
SHOULD NOT	არარეკომენდებულია
RECOMMENDED	რეკომენდებულია
MAY	შესაძლოა
OPTIONAL	არააუცილებელია

ცხრილი 1: ტერმინოლოგიური შესაბამისობა RFC2119 -თან.

2 სარჩევი

3 დოკუმენტის ისტორია

ვერსია	თარიღი	ცვლილება
0.1		საწყისი ვერსია.
0.2		მიგრაცია OpenID Connect for Identity Assurance 1.0.12 სტანდარტზე
0.3		მიგრაცია OpenID Connect for Identity Assurance 1.0 Implementer's Draft 4 სტანდარტზე. მარტივი ავთენტიფიკაცია, დამატებითი ინფორმაციის მოთხოვნა

შენიშვნა: შესაძლოა დოკუმენტს ჰქონდეს მე-3 დონის ვერსიები (მაგ. 0.8.RC1), რაც მითითებული იქნება სათაურის ქვემოთ. აღნიშნული მიდგომა გამოიყენება იმ შემთხვევაში, როდესაც ვერსია ჯერ კიდევ არაა საბოლოო და მასში შეიძება შევიდეს სარედაქციო ან/და სხვა ნაკლებად მნიშვნელოვანი შესწორებები. როდესაც ვერსიაზე მუშაობა დასრულდება, მე-3 დონის ვერსია მოიხსნება (ანუ, 0.8.RC1, 0.8.RC2, …0.8.RCn საბოლოოდ გადაიქცევა 0.8 ვერსიად).

4 ტერმინები და აბრევიატურები

ამ დოკუმენტში გამოყენებულ ყველა ტერმინს, რომელიც განსაზღვრულია „საგადახდო სისტემისა და საგადახდო მომსახურების შესახებ“ საქართველოს კანონში, აქვს ამავე კანონით განსაზღვრული მნიშვნელობა, გარდა იმ შემთხვევებისა როცა ამ თავში ტერმინი სხვაგვარად არის განსაზღვრული.

დოკუმენტში დამატებით გამოყენებულია შემდეგი ტერმინები:

ელექტრონული იდენტიფიკაცია	ფიზიკური პირის, იურიდიული პირის ან იურიდიული პირის წარმომადგენელი ფიზიკური პირის უნიკალურად აღმწერი

	ელექტრონული ფორმის საიდენტიფიკაციო მონაცემების გამოყენების პროცესი
ავთენტიფიკაცია	ელექტრონული პროცესი, რომელიც საშუალებას იძლევა, დამოწმდეს ფიზიკური ან იურიდიული პირის ელექტრონული იდენტიფიკაცია
იდენტობის პროვაიდერი	(Identity Provider) პირი, რომელსაც სერვერი აქვს მომხმარებლის ავთენტიფიკაციისა და მომხმარებლის შესახებ ინფორმაციის გარე პირებისთვის მიწოდების საშუალება
მტკიცება	(Claim) ინფორმაციის ნაწილი ამა თუ იმ ერთეულის (მაგ. პირის) შესახებ
დაყრდნობილი მხარე	(Relying Party) პირი, რომელიც იდენტობის პროვაიდერისგან ითხოვს მომხმარებლის ავთენტიფიკაციას და მტკიცებებს მომხმარებლის შესახებ

დოკუმენტში, შემოკლების მიზნით შესაძლოა გამოყენებული იყოს შემდეგი აბრევიატურები:

ამსმპ	ანგარიშის მომსახურე საგადახდო მომსახურების პროვაიდერი (Account Servicing Payment Service Provider, ASPSP)
მმპ	მესამე მხარის პროვაიდერი (Third Party Provider, TPP) - საგადახდო მომსახურების პროვაიდერი, გარდა ამსმპ-ისა
გიმპ	გადახდის ინიცირების მომსახურების პროვაიდერი (Payment Initiation Service Provider, PISP)
აიწპ	ანგარიშის ინფორმაციაზე წვდომის პროვაიდერი (Account Information Service Provider, AISP)
სმმ	საგადახდო მომსახურების მომხმარებელი (Payment Service User, PSU)

ცხრილი 2: გამოყენებული აბრევიატურები.

5 ძირითადი პრინციპები

იმისათვის, რათა დაყრდნობილმა მხარემ (მაგ. კომერციულმა ბანკმა) იმოქმედოს როგორც დაყრდნობილმა მხარემ და მიანდოს მომხმარებლის ავთენტიფიკაციის პროცესი, ამ მომხმარებლის შესახებ მტკიცებების მიღების ჩათვლით, სხვა მხარეს (მაგ. სხვა კომერციულ ბანკს), პირველ რიგში შეიძლება საჭირო იყოს რომ მათ შორის დამყარდეს გარკვეული სამართლებრივი ურთიერთობა (მაგ. დაიდოს მომსახურების ხელშეკრულება). წინამდებარე დოკუმენტი არ აკეთებს რაიმე დაშვებას ან დათქმას ამგვარი ურთიერთობის შინაარსზე ან მისი დამყარების აუცილებლობაზე.

აუცილებელია, დაყრდნობილ მხარესა და იდენტობის პროვაიდერს შორის ინფორმაციის ელექტრონული მიმოცვლის განწესი სრულ შესაბამისობაში იყოს OpenID Connect -თან, რომელიც აღწერილია (4)-ით.

აუცილებელია ასევე სრულად დაკმაყოფილებული იყოს Financial Grade API-ს საბაზისო მოთხოვნები (5) და გაძლიერებული მოთხოვნები (6).

ეს დოკუმენტი განსაზღვრავს დაყრდნობილი მხარისთვის ინფორმაციის მიწოდების 3 დონეს:

დონე	აღწერა	მითითება
საბაზისო	შემოწმებული მტკიცებების მიწოდება, ნდობის ჩარჩოს ჩათვლით	6.1
გაფართოებული	ყველაფერი, რაც შედის „საბაზისო“ დონეში, პლუს მტკიცებულებები და მათი შემოწმების მეთოდები	6.5
სრული	ყველაფერი, რაც შედის „გაფართოებულ“ დონეში, პლუს მომხმარებლის ანკეტის მხარდაჭერა	

6 მტკიცებები და შემოწმებული მტკიცებები

6.1 შემოწმებული მტკიცებების მხარდაჭერა

იმისათვის, რათა დაყრდნობილ მხარეს ჰქონდეს გარანტია, რომ მტკიცებები, რომლებსაც იდენტობის პროვაიდერი დააბრუნებს, სარწმუნო წყაროდანაა მიღებული, **აუცილებელია** იდენტობის პროვაიდერს ჰქონდეს „შემოწმებული მტკიცებების“ (verified claims) მხარდაჭერა (7)-ის მიხედვით და, ამ მიზნით, აუცილებელია მეტაინფორმაციაში რომელიც ფორმირებულია (8)-ის შესაბამისად, მითითებული ჰქონდეს "verified_claims_supported":true.

აუცილებელია, იდენტობის პროვაიდერმა მხარი დაუჭიროს მტკიცებების გამოთხოვას, სულ მცირე, ქართულ ენაზე (**უმჯობესია** ასევე ინგლისურ ენაზეც) აღნიშნული ასახოს საკუთარ მეტაინფორმაციაში (8)-ის შესაბამისად, ველში claims_locales.

აუცილებელია, მხარდაჭერილი იყოს, სულ მცირე, შემდეგი შემოწმებული მტკიცებები:

- given_name - სახელი
- family_name - გვარი
- personal_number - პირადი ნომერი
- birthdate - დაბადების თარიღი
- nationalities - მოქალაქეობა

უმჯობესია, მხარდაჭერილი იყოს შემდეგი შემოწმებული მტკიცებები:

- place_of_birth
- msisdn
- email

აუცილებელია მტკიცება msisdn, თუ იგი მხარდაჭერილია, დაფორმირდეს MSISDN ფორმატის შესაბამისად (მაგ. +995322054142).

შესაძლოა იდენტობის პროვაიდერი მხარს უჭერდეს სხვა შემოწმებულ მტკიცებებსაც.

აუცილებელია, მტკიცება personal_number დაფორმირდეს შემდეგნაირად:

- PNO
- ქვეყნის 2-სიმბოლოიანი კოდი (მაგ. GE)

- ტირე („-„)
- პირადი ნომერი

<u>მაგალითად:</u> PNOGE-12345678901

აუცილებელია, ყველა მხარდაჭერილი შემოწმებული მტკიცების სია მითითებული იყოს იდენტობის პროვაიდერის მეტაინფორმაციაში, (8)-ის მიხედვით (ველი claims_in_verified_claims_supported).

დაყრდნობილმა მხარემ **არავითარ შემთხვევაში** არ უნდა ჩათვალოს მტკიცება შემოწმებულად, თუ იგი არ არის მოცემული არ არის verified_claims ელემენტის შიგნით.

იდენტობის პროვაიდერმა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს მტკიცება შემოწმებული მტკიცებების (verified_claims) სიაში, თუ მას თან არ მოაყოლებს სულ მცირე ერთ მტკიცებულებას (Evidence) რომელითაც აღნიშნული მტკიცების „შემოწმებულად“ ჩასათვლელად იხელმძღვანელა.

6.2 შემოწმებული მტკიცებების გამოთხოვა userinfo-ს საშუალებით

აუცილებელია, იდენტობის პროვაიდერი მხარს უჭერდეს შემოწმებული მტკიცებების გაცემას userinfo ბოლოწერტილის მეშვეობით, როგორც ეს (7)-ით არის განსაზღვრული.

აუცილებელია, userinfo ბოლოწერტილი იყოს მხარდაჭერილი და მისი მისამართი მითითებული იყოს იდენტობის პროვაიდერის მეტაინფორმაციაში, (8)-ის მიხედვით (ველი userinfo_endpoint).

აუცილებელია, userinfo ბოლოწერტილის მიერ დაბრუნებული პასუხი იყოს ხელმოწერილი და შესაბამისი ალგორითმი მითითებული იყოს მეტაინფორმაციაში (8)-ის მიხედვით (ელემენტი userinfo_signing_alg_values_supported). **აუცილებელია** userinfo ბოლოწერტილის მიერ დაბრუნებულ JWT ტოკენის ფორმატის პასუხის სათაურში მითითებული იყოს:

1) ერთ-ერთი შემდეგი ალგორითმი: RS256, RS512, ES256, ES512, PS256, PS512.
2) kid ატრიბუტი რომლითაც მოხდება იდენტობის პროვაიდერის მეტაინფორმაციაში მითითებული გასაღებების სიმრავლეში (ელემენტი jwks_uri) ხელმოწერის გასაღების იდენტიფიცირება. **უმჯობესია** ხელმოწერისთვის გამოიყენებოდეს დახურული გასაღები, რომლის შესაბამის ღია გასაღებზეც გაცემულია ელექტრონული შტამპის სერტიფიკატი (10) და (11) დოკუმენტებთან თავსებადობის მიზნებისათვის

Commented [MK1]: შემდეგ ვერსიაში ვფიქრობთ დავწეროთ "აუცილებელია"

იდენტობის პროვაიდერმა **არავითარ შემთხვევაში** არ უნდა გახადოს სავალდებულო წესად userinfo ბოლოწერტილის მიერ დაბრუნებული პასუხის დაშიფრვა: **აუცილებელია**, იდენტობის პროვაიდერი მხარს უჭერდეს მის დაბრუნებას დაუშიფრავი სახით, **შესაძლოა** იგი მხარს უჭერდეს შიფრაციას როგორც ინფორმაციის დაცვის არააუცილებელ, დამატებით ზომას (მაგ. დაყრდნობილ მხარესთან შეთანხმებით და მარეგულირებელი კანონმდებლობის დაცვით, განსაკუთრებული კატეგორიის პერსონალური მონაცემების დაბრუნების შემთხვევაში, რომლებიც ამ დოკუმენტით არ რეგულირდება).

6.3 შემოწმებული მტკიცებების გამოთხოვა ID Token - საშუალებით

შესაძლოა იდენტობის პროვაიდერმა მხარი დაუჭიროს შემოწმებული მტკიცებების გამოთხოვას ID Token-ის საშუალებით, როგორც ეს აღწერილია (7)-ით.

შემოწმებული მტკიცებების გაცემის მხარდაჭერა ID Token-ის საშუალებით **არარეკომენდებულია**. თუ იდენტობის პროვაიდერს სურს აღნიშნულის მხარდაჭერა, **უმჯობესია** მან შემოწმებული მტკიცებები დაამატოს ID Token-ს, თუ დაკმაყოფილებულია ერთი პირობა მაინც:

1. ტოკენის გასაცემად გამოყენებულია „ავტორიზაციის კოდის“ თანმიმდევრობა 10.1 მიხედვით, კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაციის თანმიმდევრობა 10.2 მიხედვით ან ხელსაწყოს კოდის თანმივდევრობა 10.3
2. ID Token დაშიფრულია

6.4 ნდობის ჩარჩო

აუცილებელია, იდენტობის პროვაიდერი მხარს უჭერდეს ნდობის ჩარჩოს დასახელებით ge_aml, რომელიც გულისხმობს იმას, რომ მტკიცებების შემოწმება განხორციელდა საქართველოს იმ კანონმდებლობის შესაბამისად, რომელიც უკანონო შემოსავლების ლეგალიზაციისა და ფულის გათეთრების წინააღმდეგ ბრძოლის მიზნით მოქმედებს ქვეყანაში.[1] **აუცილებელია**, აღნიშნული ჩანაწერი მითითებული იყოს იდენტობის პროვაიდერის მეტაინფორმაციაში, (8)-ის მიხედვით (ველი trust_frameworks_supported).

თუ იდენტობის პროვაიდერი მხარს არ უჭერს ge_aml ნდობის ჩარჩოს, დაყრდნობილმა მხარემ აღნიშნული პროვაიდერის მიერ მოწოდებული ინფორმაცია **არავითარ შემთხვევაში** არ უნდა გამოიყენოს ღია ფინანსების სისტემაში მომხმარებლის იდენტიფიკაციისა და ავთენტიფიკაციის მიზნებისათვის.

მაგალითად :

```
verified_claims_supported:true,
trust_frameworks_supported:[
     "ge_aml"
]
```

6.4.1 ge_aml ნდობის ჩარჩოს დამატებითი ატრიბუტები

როდესაც ნდობის ჩარჩო არის ge_aml, verification ელემენტის დანარჩენი ველები განისაზღვრება ამ თავის მიხედვით:

- assurance_level - **არააუცილებელია**. დაბრუნების შემთხვევაში, დოკუმენტის ამ ვერსიასთან თავსებადობის მიზნებისათვის **აუცილებელია** მისი მნიშვნელობა იყოს ერთ-ერთი მნიშვნელობა რაც განსაზღვრულია ცხრილი 3-ში

[1] ge_aml კოდი ამჟამად არ არის რეგისტრირებული და იგეგმება მისი რეგისტრაცია სტანდარტის შესაბამისად.

- time - **აუცილებელია** და მიუთითებს უახლეს თარიღს და დროს, რომლის მდგომარეობითაც იდენტობის პროვაიდერმა მიაღწია assurance_level -ით მითითებულ რწმუნების დონეს.

რწმუნების დონე	განმარტება
basic	1. პირის ვინაობა არის დადასტურებული შესაბამისი მტკიცებულებებით, რომლის დაბრუნებაც იდენტობის პროვაიდერს შეუძლია evidence ელემენტში, მოთხოვნის შემთხვევაში 2. პირი არ ირიცხება საერთაშორისო და ლოკალურ მონაცემთა ბაზებში რომლებიც შეიცავენ ცნობას ტერორისტებზე, ძებნილებზე 3. პირის არსებობა გადამოწმდა პოლიტიკურად აქტიურ პირთა რეესტრში

ცხრილი 3: რწმუნების დონეები

შენიშვნა: ელემენტში verification მითითებული დრო **შესაძლოა** არ ემთხვეოდეს მტკიცებულებების (evidence) ელემენტში კონკრეტული მტკიცებულების გადამოწმების დროს. მაგალითად AML შემოწმება არის პერიოდული პროცესი და ის შეიძლება განხორციელდეს რამდენჯერმე, მაშინაც კი როდესაც მომხმარებლის საიდენტიფიკაციო დოკუმენტი მოქმედია. ამდენად, verification/time ელემენტის მნიშვნელობა იქნება უფრო ახალი, ვიდრე evidence-ში კონკრეტული დოკუმენტის დრო.

6.5 მტკიცებულებების და მათი შემოწმების მეთოდების მხარდაჭერა

6.5.1 მტკიცებულების ტიპები

6.5.1.1 საიდენტიფიკაციო დოკუმენტები

აუცილებელია იდენტობის პროვაიდერი მხარს უჭერდეს მტკიცებულების ტიპს „ საიდენტიფიკაციო დოკუმენტი“ (document, ან მოძველებული ფორმით id_document). აუცილებელია, ტიპები. ამ დოკუმენტით მხარდაჭერილი ტიპების სია მოცემულია 13.1 თავში.

აუცილებელია, გარდა სტანდარტული ველებისა (type, issuer, number…) საიდენტიფიკაციო დოკუმენტებს ასევე ჰქონდეთ ველი personal_number რომელშიც ჩაიწერება პირის პირადი ნომერი, თუ იგი მითითებულია საიდენტიფიკაციო დოკუმენტზე. **აუცილებელია**, პირადი ნომერი ამ ველში ბრუნდებოდეს ისევე, როგორც დოკუმენტზე წერია (რაიმე პრეფიქსის ან სუფიქსის გარეშე).

თუ საიდენტიფიკაციო დოკუმენტს ნომრის გარდა გააჩნია ე.წ. „სერია“ (მაგ. 2011 წლამდე გამოშვებულ საქართველოს მოქალაქის პირადობის მოწმობებს“, **აუცილებელია** სერიაც გახდეს დოკუმენტის ნომრის ნაწილი და მიეწეროს ნომერს მარცხნიდან, რაიმე გამყოფის გარეშე.

6.5.1.2 ელექტრონული ჩანაწერები

თუ იდენტობის პროვაიდერი მხარს უჭერს ისეთ საიდენტიფიკაციო დოკუმენტებს, რომელთა გადამოწმებასაც მარეგულირებელი კანონმდებლობა მას სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ერთიან ელექტრონულ ბაზაში ავალდებულებს, **აუცილებელია** იდენტობის პროვაიდერი მხარს ასევე უჭერდეს ელექტრონული ჩანაწერის (electronic_record) ტიპის მტკიცებულებებს.

შენიშვნა: მაგალითად, შეიძლება ზოგიერთი პროვაიდერი მხარს უჭერდეს მომხმარებლის მიერ დასახელებული პირადი ნომრის საშუალებით ინფორმაციის პირდაპირ სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ერთიან ელექტრონულ ბაზაში.

6.5.2 შემოწმების და დამტკიცების მეთოდები

თითოეულ მტკიცებულებას განესაზღვრება შემოწმების (verification) და დამტკიცების (validation) მეთოდები, რომლებიც გამოყენებული იქნა ამ კონკრეტული მტკიცებულებისათვის.

- შემოწმების მეთოდი (verification_method) მიუთითებს, რა სახით გადამოწმდა ამ მტკიცებულების ავთენტიკურობა (მაგ. პასპორტის ავთეტიკურობა შეიძლება დამტკიცებულიყო მისი ფიზიკურად წარმოდგენით და უფლებამოსილი პირის მიერ შემოწმებით)

- დამტკიცების მეთოდი (validation_method) მიუთითებს, რა სახით დამტკიცდა რომ კონკრეტული პირი შეესაბამება ამ მტკიცებულებას (მაგ. უფლებამოსილი პირი ამოწმებს ოფისში ფიზიკურად გამოცხადებული მომხმარებლის სახის შესაბამისობას დოკუმენტზე დატანილ სახესთან, თუ მტკიცებულების ტიპია document, ან ელექტრონულ ჩანაწერში არსებულ სურათთან, თუ მტკიცებულების ტიპია electronic_record)

6.5.2.1 დამტკიცების მეთოდები

ამ თავით განისაზღვრება მეთოდების სრული სია, რომლების მხარდაჭერილია ამ დოკუმენტებთან თავსებადობის მიზნით და იმ შემთხვევების აღწერა, როდის უნდა დააბრუნოს იდენტობის პროვაიდერმა კონკრეტული მეთოდი. **შესაძლოა**, იდენტობის პროვაიდერი მხარს არ უჭერდეს ერთ ან რამდენიმე მეთოდს, საკუთარი ბიზნეს-პროცესებიდან გამომდინარე.

იდენტიფიკატორი	გამოყენება
pvp	პირადად გამოცხადებული პირი ფიზიკურად გადაამოწმა უფლებამოსილმა პირმა. პირის ფიზიკური მახასიათებლები (მაგ. სახე) შედარდა ცნობილ ინფორმაციას (სახეს ან მის შაბლონს)
pvr	უფლებამოსილმა პირმა გადაამოწმა დისტანციაზე მყოფი პირი (მაგ. ვიდეოზარით). პირის ფიზიკური მახასიათებლები (მაგ. სახე) შედარდა ცნობილ ინფორმაციას (სახეს ან მის შაბლონს)
bvp	პირადად გამოცხადებული პირი ავტომატურ რეჟიმში გადაამოწმა ბიომეტრიული შედარების სისტემამ. პირის ფიზიკური მახასიათებლები

	(მაგ. სახე, თითის ანაბეჭდი) შედარდა ცნობილ ინფორმაციას (სახეს ან მის შაბლონს)
bvr	ბიომეტრიული შედარების სისტემამ გადაამოწმა დისტანციაზე მყოფი პირი. პირის ფიზიკური მახასიათებლები (მაგ. სახე) შედარდა ცნობილ ინფორმაციას (სახეს ან მის შაბლონს)

6.5.2.2 შემოწმების მეთოდები

ამ თავით განისაზღვრება მეთოდების სრული სია, რომლების მხარდაჭერილია ამ დოკუმენტებთან თავსებადობის მიზნით და იმ შემთხვევების აღწერა, როდის უნდა დააბრუნოს იდენტობის პროვაიდერმა კონკრეტული მეთოდი. **შესაძლოა**, იდენტობის პროვაიდერი მხარს არ უჭერდეს ერთ ან რამდენიმე მეთოდს, საკუთარი ბიზნეს-პროცესებიდან გამომდინარე.

იდენტიფიკატორი	გამოყენება
vpip	ფიზიკურად წარმოდგენილი, ფიზიკური ფორმის მტკიცებულების შემოწმება მოხდა ფიზიკურად (მაგ. ოპერატორმა გამოართვა პირს პირადობის მოწმობა და დარწმუნდა მის ავთენტიკურობაში)
vpiruv	მსგავსია vpip, ოღონდ ფიზიკურად წარმოდგენილი, ფიზიკური ფორმის მტკიცებულების შემოწმება ასევე მოხდა ფიზიკურად, მათ შორის უხილავი (ინფრაწითელი ან/და ულტრაიისფერი) სინათლის ქვეშ
vri	ფიზიკური ფორმის მტკიცებულების შემოწმება მოხდა დისტანციურად, ხილული სინათლის ქვეშ (მაგ. პირმა გადაიღო ვიდეო რომელშიც ხელში უჭირავს მართვის მოწმობა)
vdig	ციფრული/ელექტრონული მტკიცებულების შემოწმება მოხდა მისი ელექტრონული შიგთავსის შემოწმების გზით
vcrypt	მტკიცებულების კრიპტოგრაფიული დამცავი მექანიზმები ურღვევი და სწორია (მაგ. ბიომეტრიული პასპორტის შემოწმება მოხდა ჩიპზე დატანილი ინფორმაციის ელექტრონული ხელმოწერის ან/და ჩიპის ავთენტიფიკაციის განწესის მეშვეობით)
data	ნაპოვნია ელექტრონული ჩანაწერი რომელიც შეესაბამება მომხმარებლის მიერ განცხადებულ მტკიცებებს
auth	ის, რომ მომხმარებელი ფლობს განცხადებულ მტკიცებებს, დადასტურდა ელექტრონული ავთენტიფიკაციის პროცედურით რომელიც ამ მტკიცებების მფლობელთანაა დაკავშირებული
token	ის, რომ მომხმარებელი ფლობს განცხადებულ მტკიცებებს, დადასტურდა ფიზიკური ავთენტიფიკაციის მოწყობილობით მომხდარი ელექტრონული ავთენტიფიკაციის პროცედურით რომელიც ამ მტკიცებების მფლობელთანაა დაკავშირებული (მაგ. პირადობის ელექტრონული მოწმობით განხორციელებული ელექტრონული ავთენტიფიკაცია ან კვალიფიციური ელექტრონული ხელმოწერა)
kbv	ის, რომ მომხმარებელი ფლობს განცხადებულ მტკიცებებს, დადასტურდა კითხვა-პასუხით, როცა სწორი პასუხები მხოლოდ მტკიცების მფლობელს შეეძლო სცოდნოდა

6.5.2.3 შემოწმება-დამტკიცების ერთობლივი მხარდაჭერა

უმჯობესია, იდენტობის პროვაიდერი მხარს უჭერდეს შემოწმების და დამტკიცების მეთოდების ცალ-ცალკე დაბრუნებას და არ გამოიყენოს method ველი. თუ იდენტობის პროვაიდერი იყენებს method ველს, **აუცილებელია** მნიშვნელობა განისაზღვროს შემდეგი წესით:

1. pipp - მომხმარებელი პირადად გამოცხადდა იდენტობის პროვაიდერის ოფისში და წარადგინა საიდენტიფიკაციო დოკუმენტი
2. eid - მოხდა მტკიცებულების ონლაინ შემოწმება (მაგ. სსიპ „სახელმწიფო სერვისების განვითარების სააგენტოს“ ელექტრონულ ბაზაში)

შესაძლოა იდენტობის პროვაიდერი ასევე მხარს უჭერდეს საიდენტიფიკაციო დოკუმენტების გადამოწმების შემდეგ მეთოდებს:

1. sripp - გადამოწმება ვიდეოკომუნიკაციის საშუალებით, როდესაც იდენტობის პროვაიდერის მხრიდან გადამოწმებას ადამიანი ახორციელებს
2. uripp - გადამოწმება ვიდეოკომუნიკაციის საშუალებით, როდესაც იდენტობის პროვაიდერის მხრიდან გადამოწმებაში ადამიანი ჩართული არ არის (ავტოპორტრეტის ვიდეოს, სიცოცხლის შემოწმების და საიდენტიფიკაციო დოკუმენტის ვიდეოგადაღების გზით)
3. onsite - გადამოწმება ჩიპის, PIN კოდისა და ავთენტიფიკაციის სერტიფიკატის გამოყენებით (არა კვალიფიციური ელექტრონული ხელმოწერის)

6.6 ინფორმაციის გამოთხოვის პროცესის მართვა დაყრდნობლი მხარის მიერ

აუცილებელია, იდენტობის პროვაიდერმა ყურადღება მიაქციოს და გაითვალისწინოს დაყრდნობილი მხარის მოთხოვნა, რომელიც მას წარედგინება (7)-ის მე-5 თავით განსაზღვრული წესით (ანუ ავტორიზაციის მოთხოვნაში გადაეცემა claims პარამეტრი რომელიც მიუთითებს, შემოწმებული მტკიცებები დაბრუნდეს userinfo ბოლოწერტილით ID Token-ით მოთხოვნისას (თუ მხარდაჭერილია) თუ ორივეთი). კერძოდ:

1. **აუცილებელია** მტკიცების გამოთხოვისას ენის ცხადად მითითების შემთხვევაში (მაგ. family_name#ka) მტკიცება დაბრუნდეს შესაბამის ენაზე, თუ აღნიშნული ენა მხარდაჭერილია იდენტობის პროვაიდერის მიერ.
2. თუ მტკიცების გამოთხოვისას ენა ცხადად არ არის მითითებული, მაგრამ გადმოცემულია claims_locales პარამეტრი, **აუცილებელია** იდენტობის პროვაიდერმა მტკიცებები დააბრუნოს შესაბამის ენაზე
3. თუ მტკიცების გამოთხოვისას არც ენაა ცალსახად მითითებული და არც claims_locales პარამეტრია მითითებული, **აუცილებელია** იდენტობის პროვაიდერმა იგულისხმოს რომ მოთხოვნილია ქართული ენა (claims_locales=ka)
4. **აუცილებელია** მხარდაჭერილი იყოს essential (აუცილებლობა) პარამეტრი მტკიცებების გამოთხოვისას და იდენტობის პროვაიდერმა იმოქმედოს შესაბამისად.

აუცილებელია მხარდაჭერილი იყოს გადამოწმების მონაცემების კონკრეტული ტიპების (მაგ. მხოლოდ document), მეთოდების (მაგ. მხოლოდ pipp) და ნდობის ჩარჩოს (მაგ. მხოლოდ ge_aml) მიხედვით შეზღუდვა.

Commented [MK2]: ენასთან დაკავშირებით რამე ღია საკითხი თუ გვაქვს დარჩენილი, გავიაროთ.

თუ მოითხოვება საიდენტიფიკაციო დოკუმენტი, **აუცილებელია** მხარდაჭერილი იყოს გამცემი ქვეყნის მიხედვით შეზღუდვა. მაგალითად:

```
{
  "userinfo": {
    "verified_claims": {
      "verification": {
        "trust_framework": null,
        "time": null,
        "evidence": [
          {
            "type": {
              "value": "document"
            },
            "method": null,
            "document_details": {
              "type": null,
              "issuer":  {
                "country": "GE",
                "name": null
              },
              "number": null,
              "date_of_issuance": null,
              "personal_number": null
            }
          }
        ]
      },
      "claims": {
        "given_name": null,
        "family_name": null,
        "birthdate": null,
        "personal_number": null
      }
    }
  }
```

იდენტობის პროვაიდერმა claims პარამეტრი **არავითარ შემთხვევაში** არ უნდა გამოაცხადოს სავალდებულო პარამეტრად და თუ დაყრდნობილ მხარეს სჭირდება სერვისის გამოყენება მასთან ხელმეორედ მისული მომხმარებლის ავთენტიფიკაციის მიზნებისათვის, შემოწმებული მტკიცებების გამოთხოვის მოთხოვნის გარეშე, **აუცილებელია** მას მიეცეს ამის საშუალება. **აუცილებელია** იდენტობის პროვაიდერმა უზრუნველყოს რომ მომხმარებლის იდენტიფიკატორი (მტკიცება sub) იყოს ერთიდაიგივე და უცვლელი დაყრდნობილი მხარისათვის.

რეკომენდებულია, subject_types_supported პარამეტრის მნიშვნელოვა მეტაინფორმაციაში (8) მითითებული იყოს როგორც pairwise.

აუცილებელია მხარდაჭერილი იყოს ინფორმაციის გამოთხოვა მტკიცებულებების (evidence) გარეშე. და ასეთ შემთხვევაში იდენტობის პროვაიდერმა არავითარ შემთხვევაში არ უნდა დაბრუნოს evidence ტიპის ჩანაწერები:

```
{
  "userinfo": {
    "verified_claims": {
      "verification": {
        "trust_framework": null,
```

```
        "time": null
      },
      "claims": {
        "given_name": null,
        "family_name": null,
        "birthdate": null,
        "personal_number": null
      }
    }
  }
}
```

შესაძლოა იდენტობის პროვაიდერმა განახორციელოს ერთფაქტორიანი ავთენტიფიკაცია, თუ დაყრდნობილი მხარე ინფორმაციის გამოთხოვას მტკიცებულებების გარეშე ითხოვს.

7 მომხმარებლის ანკეტის გამოთხოვა

მომხმარებლის ანკეტა არის დოკუმენტი, რომელსაც იდენტობის პროვაიდერი ადგენს ამ მომხმარებლის შესახებ. ფინანსურ ინსტიტუტებში მომხმარებლის ანკეტა დგება საქართველოს კანონმდებლობის შესაბამისად, უკანონო შემოსავლების ლეგალიზაციის, ფულის გათეთრების და სხვა ფინანსური დანაშაულის წინააღმდეგ ბრძოლის მიზნით.

მომხმარებლის ანკეტის გამოთხოვაზე უფლების მოპოვება შეიძლება მოხდეს:

1) უშუალოდ პირველადი ავთენტიფიკაციის მოთხოვნასთან ერთად
2) მოგვიანებით, დამატებითი ავტორიზაციის გზით

როგორც ერთ, ისე მეორე შემთხვევაში, დაყრდნობილი მხარე თავის სურვილს მიიღოს მომხმარებლის ანკეტა გამოხატავს scopes პარამეტრში შემდეგი მნიშვნელობის მითითებით: https://openfinance.ge/ns/scope/kyc. ასეთ შემთხვევაში **აუცილებელია** იდენტობის პროვაიდერმა განახორციელოს მომხმარებლის ძლიერი ავთენტიფიკაცია, საქართველოს კანონმდებლობის შესაბამისად.

იმ შემთხვევაში როდესაც დაყრდნობილ მხარეს თავიდანვე არ მოუთხოვია ანკეტის გამოთხოვა, მას შეუძლია ხელახლა წამოიწყოს ავთენტიფიკაციის პროცესი და scopes პარამეტრში მიუთითოს https://openfinance.ge/ns/scope/kyc ავთენტიფიკაციის სრული პროცესის თავიდან აცილების მიზნით უმჯობესია მან ასევე მომხმარებლის id_token გადაცეს id_token_hint პარამეტრად.

8 დაყრდნობილი მხარის რეგისტრაცია და ავთენტიფიკაცია

8.1 დაყრდნობილი მხარის ავთენტიფიკაცია

ამ დოკუმენტის ამ ვერსიასთან თავსებადობისათვის აუცილებელია, დაყრდნობილი მხარე მოქმედებდეს როგორც „კონფიდენციალური კლიენტი“ (6)-ის მიხედვით.

აუცილებელია, იმ დაყრდნობილი მხარეების ავთენტიფიკაცია რომლებიც ფლობენ ელექტრონულ სერტიფიკატებს (10) და (11) დოკუმენტებთან თავსებადობის მიზნებისათვის, განხორციელდეს აღნიშნული სერტიფიკატებით, (9)-ის მიხედვით. ამგვარი სერტიფიკატების არ

ფლობის შემთხვევაში **აუცილებელია** ავთენტიფიკაცია განხორციელდეს ერთ-ერთი შემდეგი წესით:

1. თუ დაყრდნობილი მხარე უკვე ფლობს საქართველოს ან ევროპის კავშირის კანონმდებლობის შესაბამისად გაცემულ კვალიფიციურ სერტიფიკატს ვებსაიტის ავთენტიფიკაციისათვის, მათ შორის ისეთ შემთხვევაშიც კი როდესაც აღნიშნული სერტიფიკატები არ არის გაცემული (10) და (11) დოკუმენტებთან თავსებადობის მიზნებისათვის, იდენტობის პროვაიდერს უფლება აქვს გამოიყენოს აღნიშნული სერტიფიკატი დაყრდნობილი მხარის ავთენტიფიკაციისათვის. **უმჯობესია** იდენტობის პროვაიდერმა ისარგებლოს ამ მეთოდით
2. ავთენტიფიკაცია განხორციელდეს (6)-ით დადგენილი რომელიმე სხვა წესით. ამ შემთხვევაში **აუცილებელია** იდენტობის პროვაიდერს დანერგილი ჰქონდეს პროცესი რომელიც გაითვალისწინებს კომპრომეტირებული საიდენტიფიკაციო მონაცემების გაუქმებას დაუსაბუთებელი შეფერხების გარეშე, დაყრდნობილი მხარის ან საქართველოს კანონმდებლობით განსაზღვრული სხვა უფლებამოსილი პირის (ასეთის არსებობის შემთხვევაში) მიმართვის საფუძველზე.

იდენტობის პროვაიდერების მხრიდან დაყრდნობილი მხარეების ავტომატური დაშვების უზრუნველყოფა **არააუცილებელია** (ვინაიდან აღნიშნულ დაშვებას შესაძლოა ესაჭიროებოდეს რეგისტრაცია, სახელშეკრულებო ურთიერთობაში შესვლა და სხვა, რაც ამ დოკუმენტის ამ ვერსიის მიზნებს სცდება).

9 ავთენტიფიკაციის სიძლიერის მოთხოვნა

აუცილებელია, იდენტობის პროვაიდერმა მხარი დაუჭიროს acr_values პარამეტრს (4)-ის მიხედვით. ასევე აუცილებელია, მხარდაჭერილი ავთენტიფიკაციის კონტექსტის კლასები ჩამოთვლილი იყოს იდენტობის პროვაიდერის მეტაინფორმაციაში (8)-ის მიხედვით (acr_values_supported).

აუცილებელია, მხარდაჭერილი იყოს, სულ მცირე, შემდეგი კლასები:

1. https://openfinance.ge/ns/assurance/basic - საბაზისო ავთენტიფიკაცია
2. https://openfinance.ge/ns/assurance/sca - მომხმარებლის ძლიერი ავთენტიფიკაცია

თუ გადმოცემულია acr_values პარამეტრი ავთენტიფიკაციისას, **აუცილებელია**, იდენტობის პროვაიდერმა მომხმარებელს ავთენტიფიკაცია გაატაროს გადმოცემული კლასის (ან უფრო ძლიერი კლასის) შესაბამისად. თუ გადამოცემულია რამდენიმე კლასი და ერთ-ერთი კლასი უფრო ძლიერ (უსაფრთხო) ავთენტიფიკაციას ითვალისწინებს, **აუცილებელია** იდენტობის პროვაიდერმა აირჩიოს ყველაზე უფრო უსაფრთხო კონფიგურაცია. **აუცილებელია** იდენტობის პროვაიდერმა id_token-ში, acr ველში დააბრუნოს ის კლასი რომელიც შეესაბამება ფაქტობრივად განხორციელებულ ავთენტიფკაციის დონეს.

თუ ავთენტიფიკაციის კლასი ცალსახად არ არის მოთხოვნილი დაყრდნობილი მხარეს, მაგრამ დაყრდნობილი მხარე ავთენტიფიკაციას გადის სერტიფიკატით რომელიც გაცემულია (10) და (11)-ის მიმართ თავსებადობის მიზნით, **აუცილებელია** იდენტობის პროვაიდერმა id_token-ში acr ველში დააბრუნოს https://openfinance.ge/ns/assurance/basic ან

https://openfinance.ge/ns/assurance/sca იმის მიხედვით თუ რომელი შეესაბამება ფაქტობრივად განხორციელებული იდენტიფიკაციის დონეს.

10 ავთენტიფიკაციის და ავტორიზაციის მეთოდების მხარდაჭერა

10.1 ავთენტიფიკაცია „ავტორიზაციის კოდის მიმდევრობის“ მეშვეობით

აუცილებელია იდენტობის პროვაიდერი მხარს უჭერდეს ავთენტიფიკაციას „ავტორიზაციის კოდის მიმდევრობის“ (Authorization Code Flow) მეშვეობით. **აუცილებელია** აღნიშნულის შესახებ მითითებული იყოს პროვაიდერის მეტაინფორმაციაში (response_types_supported და grant_types_supported მნიშვნელობებში)

10.2 კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაცია

აუცილებელია იდენტობის პროვაიდერი მხარს უჭერდეს კლიენტის ინიციირებულ შემოვლით ავთენტიფიკაცის (Client Initiated Backchannel Authentication, CIBA) რომელიც განსაზღვრულია (12)-ის მიხედვით.

შენიშვნა: CIBA-ში იგულისხმება რომ მომხმარებელი მუშაობს ერთ მოწყობილობაზე (მაგ. კომპიუტერზე ან თვითმომსახურების ტერმინალზე), ხოლო ავთენტიფიკაციას გადის სხვა მოწყობილობაზე (მაგ. სმარტფონზე). თუმცა ამ დოკუმენტის მიზნებისათვის ეს ვალდებულება მკაცრი არაა.

შემოვლითი ტოკენის მიწოდების მეთოდების მხარდაჭერის ვალდებულება, ამ დოკუმენტთან თავსებადობის მიზნით, შემდეგია:

1) **აუცილებელია** მხარდაჭერილი იყოს poll
2) **შესაძლოა** მხარდაჭერილი იყოს ping
3) **არავითარ შემთხვევაში** არ უნდა იყოს მხარდაჭერილი push

აუცილებელია იდენტობის პროვაიდერი ავთენტიფიკაციის მოთხოვნაში მხარს უჭერდეს login_hint პარამეტრს.

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია** მხარდაჭერილი იყოს login_hint პარამეტრად შემდეგი სახის დოკუმენტების გადაცემა:

1) პირადი ნომერი: { "personal_number":"PNOGE-987654321098" }
2) ტელეფონის ნომერი: { "msisdn": "+995543123321" }

შესაძლოა იდენტობის პროვაიდერი მხარს უჭერდეს სხვა ტიპის ჩანაწერებსაც login_hint -ში. **აუცილებელია**, (4)-ის შესაბამისად, სხვა პარამეტრების მსგავსად ეს პარამეტრიც „application/x-www-form-urlencoded" ფორმატში იყოს სერიალიზებული.

იდენტობის პროვაიდერის სურვილისამებრ, ავთენტიფიკაცია შეიძლება მოხდეს რომელიმე შემდეგი მეთოდით:

1) ტელეფონზე SMS ერთჯერადი კოდით (იხ. 10.2.1)
2) სმარტფონზე SMS მეშვეობით ერთჯერადი URL-ის გაგზავნით (იხ. 10.2.2)

3) ელფოსტის მისამართზე ერთჯერადი URL-ის გაგზავნით. პროცესი ანალოგიურია SMS-ის მეშვეობით ერთჯერადი URL-ის გაგზავნისა
4) მობილურ აპლიკაციაში (მაგ. მობილბანკი)
5) კომპიუტერზე დაინსტალირებულ დესკტოპ აპლიკაციაში
6) რაიმე სხვა მეთოდით

აუცილებელია მხარდაჭერილი იყოს სულ მცირე ტელეფონზე SMS კოდით (იხ. 10.2.1) ავთენტიფიკაცია.

10.2.1 კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაცია SMS კოდით

SMS კოდით ავთენტიფიკაცია ხდება 2 ეტაპად:

1. დაყრდნობილი მხარე იწყებს „კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაციის“ პროცესს. **აუცილებელია**, მტკიცებების მოთხოვნა (მათ შორის შემოწმებული მტკიცებების მოთხოვნა) ამ ეტაპზევე იქნას გადაცემული. დაყრდნობილი მხარე გადადის მოლოდინის რეჟიმში (12)-ის შესაბამისად
2. მომხმარებელს ტელეფონზე მისდის SMS კოდი
3. SMS-ის წარმატებით გაგზავნისთანავე იდენტობის პროვაიდერი ავთენტიფიკაციის ამ ფაზას ასცხადებს დასრულებულად და დაყრდნობილ მხარეს უგზავნის id_token-სა და access_token-ს (ე.წ. „შუალედურ ტოკენებს“). იდენტობის პროვაიდერმა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს refresh_token.
4. დაყრდნობილი მხარე ამოწმებს მიღებული id_token არის შუალედური თუ საბოლოო, 10.2.3-ის მიხედვით. თუ ტოკენი საბოლოოა, **აუცილებელია** ავთენტიფიკაციის პროცესი ამ ბიჯზე დასრულდეს.
5. მას შემდეგ რაც მომხმარებელი დაყრდნობილ მხარეს მიაწვდის SMS კოდის მნიშვნელობას, დაყრდნობილი მხარე კვლავ დაიწყებს „კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაციის“ პროცესს, სადაც:
   5.1. პარამეტრში id_token_hint გადაეცემა წინა ბიჯზე მიღებული id_token
   5.2. პარამეტრში user_code გადაეცემა მომხმარებლის მიერ მითითებული ერთჯერადი SMS კოდი
6. შემოვლითი ავთენტიფიკაციის წარმატებით დასრულების შემდეგ დაყრდნობილი მხარე იღებს ახალ access_token და id_token-ს. **შესაძლოა** დაყრდნობილმა მხარემ ასევე მიიღოს refresh_token.

უსაფრთხოების რისკების თავიდან ასაცილებლად **აუცილებელია**, იდენტობის პროვაიდერმა მკაცრად გააკონტროლოს რომ „შუალედური“ access_token და id_token გამოიყენება მკაცრად SMS ავთენტიფიკაციის პროცესში.

10.2.2 კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაცია SMS-ზე ბმულის გაგზავნით

SMS კოდით ავთენტიფიკაცია ხდება შემდეგი წესით:

1. დაყრდნობილი მხარე იწყებს „კლიენტის ინიციირებული შემოვლითი ავთენტიფიკაციის“ პროცესს. **აუცილებელია**, მტკიცებების მოთხოვნა (მათ შორის შემოწმებული მტკიცებების მოთხოვნა) ამ ეტაპზევე იქნას გადაცემული. დაყრდნობილი მხარე გადადის მოლოდინის რეჟიმში (12)-ის შესაბამისად
2. მომხმარებელს ტელეფონზე მისდის SMS რომელიც მოიცავს ერთჯერად URL-ს. URL მიუთითებს იდენტობის პროვაიდერის კონტროლქვეშ არსებულ რაიმე ბმულზე. **რეკომენდებულია** SMS ტექსტში იმის მითითება რომ ბმულის დაჭერის შემთხვევაში გამოსულ ეკრანზე მომხმარებელმა არ უნდა შეიყვანოს რაიმე მონაცემი და უბრალოდ უნდა დახუროს.
3. მომხმარებლის მიერ SMS-ში მითითებული URL-ზე დაჭერის შემდეგ მის სმარტფონზე იხსნება ვებგვერდი, რომელიც ამცნობს რომ ავთენტიფიკაცია წარმატებით დასრულდა. იდენტობის პროვაიდერი ავთენტიფიკაციას ჩათვლის წარმატებულად. იმის მიხედვით (12)-ში განსაზღვრული რომელი მეთოდი (poll თუ ping) არის ავთენტიფიკაციის პროცესში, დაყრდნობილ მხარეს ან გაეგზავნება შეტყობინება რომ ავთენტიფიკაცია წარმატებით დასრულდა (ping) ან ტოკენები შემდეგი მოკითხვისას დაუბრუნდება
4. შემოვლითი ავთენტიფიკაციის წარმატებით დასრულების შემდეგ დაყრდნობილი მხარე იღებს ახალ access_token და id_token-ს. **შესაძლოა** დაყრდნობილმა მხარემ ასევე მიიღოს refresh_token.

10.2.3 შუალედური და საბოლოო id_token-ის ერთმანეთისაგან გარჩევის წესი

აუცილებელია, შუალედურ id_token -ს acr მნიშვნელობაში მნიშვნელობად მინიჭებული ჰქონდეს https://openfinance.ge/ns/assurance/tmp/otp-challenge.

შუალედური id_token **არავითარ შემთხვევაში** არ უნდა შეიცავდეს მომხმარებლის რაიმე მაიდენტიფიცირებელ ინფორმაციას. გამონაკლისს შეიძლება შეადგენდეს მხოლოდ ის ინფორმაცია რომელიც ამ ტოკენის მოსაპოვებლად დაყრდნობილმა მხარემ login_hint-ში გადასცა. თუმცა ამ ინფორმაციის მითითებაც არარეკომენდებულია.

10.3 მოწყობილობის კოდის თანმიმდევრობა

აღნიშნული მეთოდის მხარდაჭერა **არააუცილებელია**, თუმცა **რეკომენდებულია** მისი მხარდაჭერა რათა ინფორმაციის შეყვანის შეზღუდული შესაძლებლობის შემთხვევაშიც (მაგ. ბანკომატის შემთხვევაში) შესაძლებელი გახდეს მომხმარებლის ავთენტიფიკაცია. მხარდაჭერის შემთხვევაში **აუცილებელია** ავთენტიფიკაცია განხორციელდეს (13)-ის მიხედვით.

აუცილებელია ავთენტიფიკაციის პროცესში მხარდაჭერილი იყოს verification_uri_complete პარამეტრი. **აუცილებელია** დაყრდნობილმა მხარემ მომხმარებელს ეს მისამართი გამოუჩინოს QR კოდის ფორმით და ასევე მცირე უჩვენოს ტექსტური ფორმით მისი საწყისი კომპონენტები:

1) პროტოკოლი

2) ჰოსტი
3) პორტი (პორტის არსებობის შემთხვევაში)

11 სესიის ცხადი დასრულება

უმჯობესია იდენტობის პროვაიდერი მხარს უჭერდეს სესიის დასრულებას (14)-ის მიხედვით.

12 მომხმარებლის თანხმობა ინფორმაციის გაზიარებაზე

აუცილებელია, დაყრდნობილი მხარისთვის გაზიარებამდე იდენტობის პროვაიდერმა სრულად უჩვენოს მომხმარებელს ეკრანზე, რა ინფორმაციის გაზიარებას აპირებს და მიიღოს თანხმობა.

თუ რომელიმე მტკიცება მონიშნულია როგორც აუცილებელი (essential), იდენტობის პროვაიდერმა მომხმარებელს **არავითარ შემთხვევაში** არ უნდა მისცეს საშუალება, არ გააზიაროს ეს ინფორმაცია ან მისი შესაბამისი მტკიცებულება. თუ მომხმარებელს არ სურს ამგვარი მტკიცების გაზიარება, მან უარი უნდა თქვას ავთენტიფიკაციაზე.

13 მტკიცებულების ტიპების სტანდარტიზაცია

ამ თავის მიზანია, განსაზღვროს სტანდარტული მნიშვნელობები სხვადასხვა მტკიცებულებებისთვის

13.1 დოკუმენტის ტიპის მტკიცებულებები

ამ თავში განსაზღვრულია იდენტობის პროვაიდერის მონაცემთა ბაზაში დაცული დოკუმენტის შესაძლო ტიპების გადაყვანის წესი სტანდარტულ ტიპებში.

დოკუმენტის ტიპი	**სტანდარტული ტიპი**
პირადობის მოწმობა	idcard
მუდმივი ბინადრობის მოწმობა	ge_residence_permanent
დროებითი ბინადრობის მოწმობა	ge_residence_temporary
დროებითი ბინადრობის მოწმობა ლტოლვილებისათვის	ge_residence_temporary
პასპორტი 32 გვერდიანი	passport
პასპორტი 48 გვერდიანი	passport
პასპორტი მოქალაქეობის არმქონე პირებისათვის	passport
პასპორტი დიპლომატიური	passport
პასპორტი სამსახურეობრივი	passport
დევნილის დროებითი საბუთი	ge_idcard_temporary
სამგზავრო დოკუმენტი	passport
დროებითი პირადობის მოწმობა	ge_idcard_temporary
პასპორტი (ბიომეტრიული)	passport
სამგზავრო პასპორტი (ბიომეტრიული)	passport
პასპორტი დიპლომატიური (ბიომეტრიული)	passport

Commented [MK3]: შეგვიძლია ვიმსჯელოთ კომიტეტზე, უფრო მეტად დაკონკრეტება ხომ არ გვინდა. მაგალითად, 32 და 48 გვერდიან პასპორტს ჩვენთან passport ჰქვია. შეგვიძლია რამე დამატებითი "ქვეტიპის" დამატებაზე ვიფიქროთ, თუ გვჭირდება.

Commented [MK4]: ლამინირებული პირადობის მაგვარი ქაღალდი იყო 2008 წლის ომისთვის., აღარ გაიცემა

Commented [MK5]: საარჩევნოდ იყო 2010-ში, დროებითი ქაღალდი

პასპორტი სამსახურეობრივი (ბიომეტრიული)	passport
სამგზავრო დოკუმენტი (ბიომეტრიული)	passport
პირადობის ელექტრონული მოწმობა	idcard
მუდმივი ბინადრობის ელექტრონული მოწმობა	ge_residence_permanent
დროებითი ბინადრობის ელექტრონული მოწმობა	ge_residence_temporary
დროებითი ბინადრობის ელექტრონული მოწმობა ლტოლვილებისთვის	ge_residence_temporary
პირადობის ნეიტრალური მოწმობა	ge_idcard_neutral
ნეიტრალური სამგზავრო დოკუმენტი	ge_passport_neutral
თანამემამულის მოწმობა	ge_compatriot_id
დროებითი ბინადრობის ელექტრონული მოწმობა ჰუმანიტარებისთვის	ge_residence_temporary
დროებითი საიდენტიფიკაციო მოწმობა(გასაძევებელი)	ge_idcard_temporary
დროებითი საიდენტიფიკაციო მოწმობა(თავშესაფრის მაძიებელი)	ge_idcard_temporary
დროებითი საიდენტიფიკაციო მოწმობა(მოქალაქეობის არმქონე პირის სტატუსის მაძიებელი)	ge_idcard_temporary
დროებითი საიდენტიფიკაციო მოწმობა (მიუსაფარი ბავშვი)	ge_idcard_temporary
დროებითი საიდენტიფიკაციო მოწმობა (ძალადობის მსხვერპლი ბავშვი)	ge_idcard_temporary
სამგზავრო პასპორტი ჰუმანიტარებისთვის (ბიომეტრიული)	passport
დროებითი ბინადრობის ელექტრონული მოწმობა დროებითი დაცვის ქვეშ მყოფი პირებისათვის	ge_residence_temporary
მართვის მოწმობა	driving_permit

Commented [MK6]: ბუკლეტია, არაბიომეტრიული

Commented [MK7]: ვიზუალურად ბუკლეტია (პასპორტს ჰგავს) თუმცა იდეურად პირადობის მოწმობაა. ანუ სამგზავრო დოკუმენტი არაა.

Commented [MK8]: პირადობის დამადასტურებელი ქაღალდი

13.2 „ელექტრონული ჩანაწერის“ ტიპის მტკიცებულებები

ამ ქვეთავით განისაზღვრება დოკუმენტის ამ ვერსიის მიზნებისათვის მხარდაჭერილი ელექტრონული ჩანაწერების ტიპები

13.2.1 სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ბაზა

სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს ერთიანი ელექტრონული მონაცემთა ბაზისთვის ტიპი არის population_register

აუცილებელია შემოწმების მეთოდი დაბრუნდეს იმ შემთხვევაში, როდესაც ხდება თვალით ან ბიომეტრიულად მონაცემთა ბაზის სურათის შესაბამისობას შემოწმება პირის სახესთან/ელექტრონულად დაფიქსირებულ გამოსახულებასთან. ასეთ დროს type ველის დაბრუნება **აუცილებელია** და მან უნდა მიიღოს ერთ-ერთი შემდგომი მნიშვნელობა

- pvp - ფიზიკურად გამოცხადებული მომხმარებელი, შემოწმება ოპერატორის მიერ
- pvr - დისტანციური იდენტიფიკაცია, შემოწმებული ოპერატორის მიერ
- bvp - ფიზიკურად გამოცხადებული მომხმარებელი, შემოწმება ბიომეტრიული სისტემის მიერ
- bvr - დისტანციური იდენტიფიკაცია, შემოწმებული ბიომეტრიული სისტემის მიერ

თუ მონაცემთა ბაზის ჩანაწერში არსებული სურათის მიმართ შემოწმება არ განხორციელებულა, შემოწმების მეთოდი **არავითარ შემთხვევაში** არ უნდა დაბრუნდეს.

აუცილებელია დაბრუნდეს დამოწმების მეთოდი და მისი მნიშვნელობა **აუცილებელია** იყოს data

მაგალითად:

```
            {
               "type":"electronic_record",
               "check_details":[
                  {
                     "check_method": "data"
                  },
                  {
                     "check_method": "pvp"
                  }
               ],
               "time":"2014-04-22T11:30Z",
               "record":{
                  "type":"population_register",
                  "source":{
                     "country_code":"GE"
                  },
                  "personal_number":"987654321098"
               }
            }
```

14 იდენტობის პროვაიდერის მიერ დაბრუნებული ინფორმაციის მაგალითები (ინფორმაციული)

14.1 პირადად გამოცხადება, პირადობის მოწმობის წარდგენით

ქვემოთ მოცემული მაგალითი აღწერს შემთხვევას, როდესაც ადამიანი პირადად გამოცხადდა იდენტობის პროვაიდერის ოფისში, წარმოადგინა საქართველოს მოქალაქის პირადობის მოწმობა (რომელიც არ შეიცავს მისამართის რეკვიზიტს).

მოძველებული ფორმატი (თავსებადი დოკუმენტის წინა ვერსიებთან):

```
{
   "verified_claims":{
```

```
      "verification":{
         "trust_framework":"ge_aml",
         "time":"2012-04-23T18:25Z",
         "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
         "evidence":[
            {
               "type":"id_document",
               "method":"pipp",
               "time": "2014-04-22T11:30Z",
               "document":{
                  "type":"idcard",
                  "issuer":{
                     "name":"საქართველოს იუსტიციის სამინისტრო",
                     "country":"GE"
                  },
                  "number":"13IA123456",
                  "personal_number":"987654321098",
                  "date_of_issuance":"2013-03-23",
                  "date_of_expiry":"2023-03-22"
               }
            }
         ]
      },
      "claims":{
         "given_name":"სახელი",
         "family_name":"გვარიაშვილი",
         "personal_number":"PNOGE-987654321098",
         "birthdate":"1956-01-28",
         "place_of_birth":{
            "country":"GE",
            "locality":"ჩხოროწყუ"
         },
         "nationalities":[
            "GE"
         ]
      }
   }
}
```

დოკუმენტის ამ ვერსიასთან თავსებადი ფორმატი:

```
{
   "verified_claims":{
      "verification":{
         "trust_framework":"ge_aml",
         "time":"2012-04-23T18:25Z",
         "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
         "evidence":[
            {
               "type":"document",
               "check_details":[
                  {
                     "check_method": "vpip"
                  },
                  {
```

```
                    "check_method": "pvp"
                }
            ],
            "time":"2014-04-22T11:30Z",
            "document_details":{
               "type":"idcard",
               "issuer":{
                  "name":"საქართველოს იუსტიციის სამინისტრო",
                  "country":"GE"
               },
               "document_number":"13IA123456",
               "personal_number":"987654321098",
               "date_of_issuance":"2013-03-23",
               "date_of_expiry":"2023-03-22"
            }
         }
      ]
   },
   "claims":{
      "given_name":"სახელი",
      "family_name":"გვარიაშვილი",
      "personal_number":"PNOGE-987654321098",
      "birthdate":"1956-01-28",
      "place_of_birth":{
         "country":"GE",
         "locality":"ჩხოროწყუ"
      },
      "nationalities":[
         "GE"
      ],
      "address":{
         "locality":"თბილისი",
         "postal_code":"0162",
         "country":"GE",
         "street_address":"ილია ჭავჭავაძის გამზირი 1"
      }
   }
}
```


14.2 პირადად გამოცხადება, პირადობის მოწმობის წარდგენით და სერვისების განვითარების სააგენტოს ბაზაში გადამოწმებით

ქვემოთ მოცემული მაგალითი აღწერს შემთხვევას, როდესაც ადამიანი პირადად გამოცხადდა იდენტობის პროვაიდერის ოფისში, წარმოადგინა საქართველოს მოქალაქის პირადობის მოწმობა (რომელიც არ შეიცავს მისამართის რეკვიზიტს), ხოლო შემდეგ პროვაიდერმა აღნიშნული მოწმობა დამატებით გადაამოწმა სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ბაზაში და, მათ შორის, ამ გზით დარწმუნდა მისამართის სისწორეში:

```
{
   "verified_claims":{
      "verification":{
         "trust_framework":"ge_aml",
         "time":"2012-04-23T18:25Z",
         "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
         "evidence":[
            {
               "type":"document",
               "check_details":[
                  {
                     "check_method": "vpip"
                  },
                  {
                     "check_method": "pvpr"
                  }
               ],
               "time":"2014-04-22T11:30Z",
               "document_details":{
                  "type":"idcard",
                  "issuer":{
                     "name":"საქართველოს იუსტიციის სამინისტრო",
                     "country":"GE"
                  },
                  "document_number ":"13IA123456",
                  "personal_number":"987654321098",
                  "date_of_issuance":"2013-03-23",
                  "date_of_expiry":"2023-03-22"
               }
            },
            {
               "type":"electronic_record",
               "check_details":[
                  {
                     "check_method": "data"
                  },
                  {
                     "check_method": "pvp"
                  }
               ],
               "time":"2014-04-22T11:30Z",
               "record":{
                  "type":"population_register",
                  "source":{
                     "name":"სახელმწიფო სერვისების განვითარების სააგენტო",
                     "country_code":"GE"
                  },
                  "personal_number":"987654321098"
               }
            }
         ]
      },
      "claims":{
         "given_name":"სახელი",
```

```
          "family_name":"გვარიაშვილი",
          "personal_number":"PNOGE-987654321098",
          "birthdate":"1956-01-28",
          "place_of_birth":{
             "country":"GE",
             "locality":"ჩხოროწყუ"
          },
          "nationalities":[
             "GE"
          ],
          "address":{
             "locality":"თბილისი",
             "postal_code":"0162",
             "country":"GE",
             "street_address":"ილია ჭავჭავაძის გამზირი 1"
          }
       }
    }
}
```

როდესაც ოპერატორი ახორციელებს სსიპ სახელმწიფო სერვისების განვითარების სააგენტოდან დაბრუნებული სურათის ვიზუალურ შემოწმებას **უმჯობესია** დაბრუნდეს შემოწმების მეთოდი და ამ შემთხვევაში **აუცილებელია** მისი მნიშვნელობა იყოს pvp. თუ ოპერატორი ამგვარ შემოწმებას არ ახორციელებს (მაგ. და გამოძახება მხოლოდ დოკუმენტის სტატუსის გადამოწმების მიზნით ხდება), მაშინ შემოწმების მეთოდში pvp **არავითარ შემთხვევაში** არ უნდა დაბრუნდეს.

14.3 პირადად გამოცხადება, მართვის მოწმობის წარდგენით და სერვისების განვითარების სააგენტოს ბაზაში გადამოწმებით

ქვემოთ მოცემული მაგალითი აღწერს შემთხვევას, როდესაც ადამიანი პირადად გამოცხადდა იდენტობის პროვაიდერის ოფისში, წარმოადგინა საქართველოს მოქალაქის პირადობის მოწმობა (რომელიც არ შეიცავს მისამართის რეკვიზიტს), ხოლო შემდეგ პროვაიდერმა აღნიშნული მოწმობა დამატებით გადაამოწმა სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ბაზაში და, მათ შორის, ამ გზით დარწმუნდა მისამართის სისწორეში:

```
{
   "verified_claims":{
      "verification":{
         "trust_framework":"ge_aml",
         "time":"2012-04-23T18:25Z",
         "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
         "evidence":[
            {
               "type":"document",
               "check_details":[
                  {
                     "check_method": "vpip"
```

```
                  },
                  {
                     "check_method": "pvp"
                  }
               ],
               "time":"2014-04-22T11:30Z",
               "document_details":{
                  "type":"driving_permit",
                  "issuer":{
                     "name":"საქართველოს შინაგან საქმეთა სამინისტრო",
                     "country":"GE"
                  },
                  "document_number":"TH654321",
                  "birthdate":"1956-01-28",
                  "personal_number":"987654321098",
                  "date_of_issuance":"2010-03-21",
                  "date_of_expiry":"2030-03-22"
               }
            },
            {
               "type":"electronic_record",
               "check_details":[
                  {
                     "check_method": "data"
                  },
                  {
                     "check_method": "pvp"
                  }
               ],
               "time":"2014-04-22T11:30Z",
               "record":{
                  "type":"population_register",
                  "source":{
                     "name":"სახელმწიფო სერვისების განვითარების სააგენტო",
                     "country_code":"GE"
                  },
                  "personal_number":"987654321098"
               }
            }
         ]
      },
      "claims":{
         "given_name":"სახელი",
         "family_name":"გვარიაშვილი",
         "personal_number":"PNOGE-987654321098",
         "birthdate":"1956-01-28",
         "place_of_birth":{
            "country":"GE",
            "locality":"ჩხოროწყუ"
         },
         "nationalities":[
            "GE"
         ],
         "address":{
            "locality":"თბილისი",
            "postal_code":"0162",
```

```
            "country":"GE",
            "street_address":"ილია ჭავჭავაძის გამზირი 1"
         }
      }
   }
}
```

14.4 ონლაინ ავთენტიფიკაცია იდენტობის პროვაიდერის მიერ, სტანდარტული კამერით, პირადობის დამადასტურებელი დოკუმენტის წარდგენით ვიდეო სესიაში და შემდგომი გადამოწმებით სსგს მონაცემთა ბაზაში

ქვემოთ მოცემული მაგალითი აღწერს შემთხვევას, როდესაც კმაყოფილდება ყველა შემდეგი პირობა

- პირმა იდენტიფიკაცია და ავთენტიფიკაცია გაიარა დისტანციურად, სტანდარტული კამერის (მობილურის ან კომპიუტერის) გამოყენებით და კამერის წარმოადგინა დოკუმენტი
- იდენტობის პროვაიდერის მიერ მართულმა სისტემამ (და არა მესამე პირთან არსებულმა სერვისმა) დოკუმენტის ავთენტიკურობა შეამოწმა გარკვეული წესით (მაგ. დოკუმენტის ვიზუალური შემოწმების ზონასა და ამავე დოკუმენტის მანქანაკითხვად ზონაში არსებული ინფორმაცია ერთმანეთს შეადარა)
- იმავე სისტემამ ერთმანეთს შეადარა მომხმარებლის სახე და საიდენტიფიკაციო დოკუმენტზე დატანილი სახე
- იდენტობის პროვაიდერმა გამოითხოვა მონაცემები სსიპ სახელმწიფო სერვისების განვითარების სააგენტოს მონაცემთა ელექტრონულ ბაზიდან
- იდენტობის პროვაიდერმა შეადარა დისტანციურად გადაღებული სურათი (ან საიდენტიფიკაციო დოკუმენტის სურათი) სსიპ სახელმწიფო სერვისების განვითარების სააგენტოში დაფიქსირებულ სურათს.
- იდენტობის პროვაიდერმა სსგს-დან მონაცემების გამოთხოვისას ასევე მიიღო მომხმარებლის რეგისტრაციის მისამართი

```
{
   "verified_claims":{
      "verification":{
         "trust_framework":"ge_aml",
         "time":"2012-04-23T18:25Z",
         "verification_process":"f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
         "evidence":[
            {
               "type":"document",
               "check_details":[
                  {
                     "check_method": "vri"
                  },
                  {
                     "check_method": "bvr"
                  }
               ],
```

```
            "time":"2014-04-22T11:30Z",
            "document_details":{
               "type":"idcard",
               "issuer":{
                  "name":"საქართველოს იუსტიციის სამინისტრო",
                  "country":"GE"
               },
               "document_number ":"13IA123456",
               "personal_number":"987654321098",
               "date_of_issuance":"2013-03-23",
               "date_of_expiry":"2023-03-22"
            }
         },
         {
            "type":"electronic_record",
            "check_details":[
               {
                  "check_method": "data"
               },
               {
                  "check_method": "bvr"
               }
            ],
            "time":"2014-04-22T11:30Z",
            "record":{
               "type":"population_register",
               "source":{
                  "name":"სახელმწიფო სერვისების განვითარების სააგენტო",
                  "country_code":"GE"
               },
               "personal_number":"987654321098"
            }
         }
      ]
   },
   "claims":{
      "given_name":"სახელი",
      "family_name":"გვარიაშვილი",
      "personal_number":"PNOGE-987654321098",
      "birthdate":"1956-01-28",
      "place_of_birth":{
         "country":"GE",
         "locality":"ჩხოროწყუ"
      },
      "nationalities":[
         "GE"
      ],
      "address":{
         "locality":"თბილისი",
         "postal_code":"0162",
         "country":"GE",
         "street_address":"ილია ჭავჭავაძის გამზირი 1"
      }
   }
}
```

```
}
```

15 წყაროები

1. **The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface.** NexGenPSD2 XS2A Framework, Operational Rules. ვერსია 1.3 2018 წლის 21 დეკემბერი.

2. —. NexGenPSD2 XS2A Framework, Implementation Guidelines. ვერსია 1.3.9 2021 წლის 29 მარტი.

3. **Bradner, Scott.** *RFC 2119 Key words for use in RFCs to Indicate Requirement Levels.* 1997 წლის March.

4. **N. Sakimura, NRI, J. Bradley, Ping Identity, M. Jones, Microsoft, B. de Medeiros, Google, C. Mortimore, Salesforce.** OpenID Connect Core 1.0 incorporating errata set 1. [ინტერნეტი] 2014 წლის 8 November. https://openid.net/specs/openid-connect-core-1_0.html.

5. **N. Sakimura, Nat Consulting, J. Bradley, Yubico, E. Jay, Illumila.** Financial-grade API Security Profile 1.0 - Part 1: Baseline. [ინტერნეტი] 2021 წლის 12 March. https://openid.net/specs/openid-financial-api-part-1-1_0-final.html.

6. —. Financial-grade API Security Profile 1.0 - Part 2: Advanced. [ინტერნეტი] 2021 წლის 12 May. https://openid.net/specs/openid-financial-api-part-2-1_0.html.

7. **T. Lodderstedt, D. Fett, M. Haine, A. Pulido, K. Lehmann, K. Koiwai.** OpenID Connect for Identity Assurance 1.0. [ინტერნეტი] 2021 წლის 6 September. https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html.

8. **N. Sakimura, NRI, J. Bradley, Ping Identity, M. Jones, Microsoft, E. Jay, Illumila.** OpenID Connect Discovery 1.0 incorporating errata set 1. 2014 წლის 8 November.

9. **Campbell, B., Bradley, J., Sakimura, N., and T. Lodderstedt.** RFC 8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens. 2020 წლის February. RFC 8705.

10. **საქართველოს საბანკო ასოციაცია.** *XS2A სტანდარტის განხორციელების სახელმძღვანელო.* ვერსია 0.7.

11. —. *ღია ფინანსების სისტემაში იდენტიფიკაციის, ავთენტიფიკაციისა და ავტორიზაციის განხორციელების სახელმძღვანელო.* ვერსია 0.8.

12. **G. Fernandez, Telefonica, F. Walter, A. Nennker, Deutsche Telekom AG, D. Tonge, Moneyhub, B. Campbell, Ping Identity.** OpenID Connect Client-Initiated Backchannel Authentication Flow - Core 1.0. [ინტერნეტი] 2021 წლის 1 09. https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html.

13. **W. Denniss, J. Bradley, M. Jones, H. Tschofenig.** RFC 8628 OAuth 2.0 Device Authorization Grant. 2019 წლის 08.

14. **Jones, M., de Medeiros, B., Agarwal, N., Sakimura, N., and J. Bradley.** OpenID Connect RP-Initiated Logout 1.0 - draft 01. 2020 წლის 7 August. OpenID.RPInitiated.

15. **Stateless, M. Kelly.** JSON Hypertext Application Language. [ინტერნეტი] https://datatracker.ietf.org/doc/html/draft-kelly-json-hal-08.

16. **Jones, M., Sakimura, N., and J. Bradley.** OAuth 2.0 Authorization Server Metadata. 2018 წლის June. RFC 8414.