ღია ფინანსების სისტემაში იდენტიფიკაციის, ავთენტიფიკაციისა და ავტორიზაციის განხორციელების სახელმძღვანელო

ვერსია 0.8.RC1

1 სარჩევი

2 დოკუმენტის შესახებ

ეს დოკუმენტი წარმოადგენს ღია ფინანსების სისტემაში იდენტიფიკაციის, ავთენტიფიკაციისა და ავტორიზაციის განხორციელების სახელმძღვანელოს, საქართველოს კანონმდებლობასთან თავსებადი ღია ბანკინგის დანერგვის მიზნით. დოკუმენტი სრულად თავსებადია შესაბამის ჩარჩოსთან (1) და (2)_თან, აზუსტებს მათ მოთხოვნებს, საქართველოს კანონმდებლობისა და ადგილობრივი კონტექსტის გათვალისწინებით.

დოკუმენტის მიზანია, მოახდინოს საქართველოში ღია ბანკინგის სერვისების მაქსიმალური ჰარმონიზაცია და ამ მიზნით, ის აწესებს ბევრ ისეთ შეზღუდვას, რომელთან დაკავშირებითაც NextGenPSD2 XS2A ჩარჩო მეტი თავისუფალი ინტერპრეტაციის საშუალებას იძლევა. კერძოდ, მიუხედავად იმისა, რომ (1) და (2) იძლევა მომხმარებლის ძლიერი ავთენტიფიკაციის მეთოდების არჩევანის საშუალებას, წინამდებარე დოკუმენტი მოითხოვს მხოლოდ მათ გარკვეულ ქვესიმრავლეს.

ასევე დოკუმენტით დარეგულირდა გარკვეული საკითხები, რომლებიც ჩაითვალა (2)-ით არასაკმარისად დარეგულირებულად (ან რეგულირების მიღმა დატოვებულად). ცალკეულ

შემთხვევებში, როდესაც ამ დოკუმენტით გარკვეული საკითხები NextGenPSD2 XS2A ჩარჩოსადმი შეუსაბამო მოთხოვნებს აწესებს, საკითხი მონიშნულია ტექსტით „// გადახვევაXS2A ჩარჩოდან“.

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 RFC21191 -თან.

დოკუმენტს გააჩნია იერარქიული სტრუქტურა. იმ შემთხვევაში, როდესაც დოკუმენტის გარკვეული თავით აღწერილი საკითხი (მაგ. საბარათე ანგარიშების ინფორმაციის სერვისები) მონიშნულია როგორც „**არააუცილებელი**“, აღნიშნულ თავში (და ასევე მის ქვეთავებში) მითითებული აუცილებელი მოთხოვნები ითვლება აუცილებლად მხოლოდ იმ პირობით, როდესაც ხდება შესაბამისი საკითხის რეალიზება.

საკითხებს, რომლებიც მონიშნულია როგორც „**უმჯობესია**“ „**რეკომენდებულია**“ და „**არარეკომენდებულია**“ ასევე მოჰყვება დამაზუსტებელი მითითება იმის თაობაზე, თუ რატომაა რეკომენდებული (ან არარეკომენდებული) აღნიშნული საკითხის გადაწყვეტა ამ დოკუმენტის დანაწესის მიხედვით.

3 დოკუმენტის ისტორია

ვერსია	თარიღი	ცვლილება
0.7	11.04.2021	საწყისი ვერსია, გადმოვიდა შესაბამისი თავები NextGenPSD2 XS2A ჩარჩოს განხორციელების სახელმძღვანელოს 0.6 ვერსიიდან და გადაჯგუფდა უკეთ აღქმისათვის. მაგალითაბისათვის დაემატა მე-8 თავი
0.8.RC1		

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, 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)
სიგმპ	საბარათე ინსტრუმენტის გაცემის მომსახურების პროვაიდერი (Payment Instrument Issuing Service Provider, PIISP)
გსს	გაუქმებული სერტიფიკატების სია (Certificate Revocation List, CRL)
სოსპ	სერტიფიკატების ონლაინ სტატუსის პროტოკოლი (Online Certificate Status Protocol, OCSP)
სმმ	საგადახდო მომსახურების მომხმარებელი (Payment Service User, PSU)

ცხრილი 2: გამოყენებული აბრევიატურები.

ამ დოკუმენტის არც ერთ თავში ტერმინი „კლიენტი“ არ აღნიშნავს პირს, რომელსაც სარგებლობს რაიმე სახის ფინანსური მომსახურებით. დოკუმენტის ამ ვერსიის მიზნებისათვის ტერმინი „კლიენტი“ შემთხვევათა უმრავლესობაში აღნიშნავს მმპ-ს.

5 მმპ, ამსმპ და მათი ავთენტიფიკაცია ერთმანეთის მიმართ

აუცილებელია, მმპ და ამსმპ ერთმანეთს უკავშირდებოდნენ დაცული არხით, რომელიც ამავდროულად უზრუნველყოფს ორივე მხარის საიმედო ავთენტიფიკაციას ერთმანეთის მიმართ. **სავალდებულოა**, აღნიშნული განხორციელდეს (2)-ის მიხედვით როგორც საკომუნიკაციო არხის, ისე გამოყენებითი პროგრამული უზრუნველყოფის დონეზე.

5.1 უნიკალური იდენტიფიკატორის გამოყენება

აუცილებელია, მმპ და ამსმპ ურთიერთკავშირისას ერთმანეთის საიდენტიფიკაციოდ იყენებდნენ უნიკალურ ნომრებს, რომლებიც შედგენილია შემდეგი პრინციპით:

სადაც „სუფიქსი“ განისაზღვრება შემდეგნაირად:

1. თუ საგადახდო მომსახურების პროვაიდერი (ამსმპ, მმპ) საგადახდო მომსახურების დაწყების მომენტისათვის ჩართულია საქართველოს ეროვნული ბანკის დროის რეალურ რეჟიმში ანგარიშსწორების (RTGS) სისტემაში, მაშინ მის იდენტიფიკატორში სუფიქსი ავტომატურად (საქართველოს ეროვნულ ბანკთან შეთანხმების საჭიროების გარეშე) იქნება RTGS სისტემაში მონაწილის იდენტიფიკატორი (ამრიგად, სუფიქსები იქნება PSDGE-NBG-BAGAGE22, PSDGE-NBG-CBASGE22, PSDGE-NBG-DISNGE22 და ა.შ.).
   1.1. თუ საგადახდო მომსახურების პროვაიდერი მოგვიანებით დაკარგავს RTGS სისტემის მონაწილის სტატუსს, მას უფლება ექნება გამოიყენოს აღნიშნული იდენტიფიკატორი სტატუსის დაკარგვიდან 2 წლის განმავლობაში.
   1.2. თუ საგადახდო მომსახურების პროვაიდერი შეიცვლის RTGS სისტემაში მონაწილის იდენტიფიკატორს, მას უფლება ექნება გამოიყენოს ძველი იდენტიფიკატორი ცვლილებიდან 2 წლის განმავლობაში.
2. სხვა შემთხვევაში სუფიქსი არის საგადახდო მომსახურების პროვაიდერისათვის საქართველოს ეროვნული ბანკის მიერ მინიჭებული უნიკალური იდენტიფიკატორი. წინამდებარე დოკუმენტი არ არეგულირებს ეროვნული ბანკის მიერ აღნიშნული იდენტიფიკატორების მინიჭების წესს. თუ ასეთი საგადახდო მომსახურების პროვაიდერი, რომელსაც უკვე მინიჭებული აქვს იდენტიფიკატორი მე-2 პუნქტის შესაბამისად, მოგვიანებით ჩაერთვება RTGS სისტემაშიც, მას უფლება ექნება გამოიყენოს თავდაპირველი იდენტიფიკატორი RTGS სისტემაში ჩართვიდან 2 წლის განმავლობაში
3. თუ საგადახდო მომსახურების პროვაიდე რი იცვლის იდენტიფიკატორს წინა პუნქტებით განსაზღვრულ რომელიმე შემთხვევაში, მან **არავითარ შემთხვევაში** აღარ უნდა გამოიყენოს ძველი იდენტიფიკატორი, მიუხედავად იმისა, დარჩენილი აქვს თუ არა მას ზემოთაღნიშნული პუნქტებით განსაზღვრული 2-წლიანი ვადა

აუცილებელია, OAuth2 პროტოკოლის ინიცირებისას გამოყენებული client_ID პარამეტრი მკაცრად (მათ შორის სიმბოლოების რეგისტრების გათვალისწინებით) უდრიდეს ზემოთაღნიშნულ იდენტიფიკატორს.

5.2 დაცული საკომუნიკაციო არხის მოთხოვნები

აუცილებელია, კავშირის არხი დამყარდეს TLS პროტოკოლის მიხედვით, TLS 1.2 ან უფრო მაღალის მიხედვით.

აუცილებელია, კავშირის დამყარებისას ორივე მხარემ ერთმანეთს წარუდგინოს X.509 სერტიფიკატები.

აუცილებელია, თითოეული მხარის X.509 სერტიფიკატი ტექნიკურად სრულად აკმაყოფილებდეს (4)-ის მოთხოვნებს ვებსაიტის ავთენტიფიკაციის კვალიფიციური სერტიფიკატების მიმართ, შეიცავდეს 5.1 თავით განსაზღვრულ იდენტიფიკატორს და გაცემული იყოს სერტიფიკატის ისეთი გამცემის მიერ, რომელიც აკმაყოფილებს საქართველოს კანონმდებლობით და ამ დოკუმენტით ღია ბანკინგისათვის/ღია ფინანსებისთვის საჭირო სერტიფიკატის გამცემისათვის წაყენებულ მოთხოვნებს.

აუცილებელია, OAuth2 პროტოკოლის რეალიზაციისას გამოყენებული იქნას კლიენტის (მმპ-ს) ავთენტიფიკაცია და ტოკენების გაცემა ხორციელდებოდეს (5)-ის მოთხოვნების შესაბამისად და ამ პროცესში გამოიყენებოდეს წინამდებარე თავით განსაზღვრული სერტიფიკატები.

აუცილებელია, ამსმპ-მა და მმპ-მა სერტიფიკატებით დაიცვან ყველა ის ჰიპერბმული, რომელსაც ისინი ერთმანეთს გადასცემენ ამ დოკუმენტით განსაზღვრული კომუნიკაციის პროცესში (მაგ. ამსმპ უბრუნებს ჰიპერბმულს მმპ-ს _links სექციით, როგორც ეს განსაზღვრულია **Error! Reference source not found.** თავის ქვეთავებში).

5.3 OAuth2 კლიენტების დინამიკური რეგისტრაციის დამატებითი მოთხოვნები

შესაძლოა, ამსმპ მხარს უჭერდეს კლიენტების დინამიკურ რეგისტრაციას (6)-ის და ასევე (7)-ის შესაბამისად და დინამიკური რეგისტრაციის მართვას (8)-ის შესაბამისად.

აუცილებელია, დინამიკური რეგისტრაციისას (თუ იგი მხარდაჭერილია) ამსმპ-მა მმპ-ს მიანიჭოს იგივე იდენტიფიკატორი (client_id) რაც მკაცრად ემთხვევა მმპ-ს 5.1 თავით განსაზღვრულ იდენტიფიკატორს.

თუ არ არსებობს წინასწარი შეთანხმება ამსმპ-სა და მმპ-ს შორის, დინამიკური რეგისტრაცია **არავითარ შემთხვევაში** არ უნდა იქნას გამოყენებული იდენტიფიკაციის, ავთენტიფიკაციის ან/და ხელმოწერის მონაცემების გასაცვლელად.

5.4 მოთხოვნები გამოყენებითი პროგრამული უზრუნველყოფის დონეზე დაცულობის მიმართ

აუცილებელია, მმპ-მა და ამსმპ-მა ინფორმაციის გაცვლისას შეტყობინებებზე დამატებით იყენებდნენ ციფრული ხელმოწერის ტექნოლოგიას, რომელიც ტექნოლოგიურად სრულ თანხვედრაში იქნება კვალიფიციური ელექტრონული შტამპის ტექნოლოგიასთან, იმ შემთხვევაშიც კი, თუ აღნიშნული არ იქნება საქართველოს კანონმდებლობით აღიარებული კვალიფიციური ელექტრონული შტამპი, **აუცილებელია**, გამონაკლისი შეეხებოდეს მხოლოდ სერტიფიკატის გამცემი ორგანოს სტატუსს საქართველოში და ამ შემთხვევაშიც, ამსმპ-ს/მმპ-ს მიერ სერტიფიკატის გამცემი შეთანხმებული უნდა იყოს საქართველოს ეროვნულ ბანკთან.

<u>შენიშვნა:</u> იმისათვის, რათა დაცული იყოს თავსებადობა (1)-*სა და* (2)-*თან შემდგომში აღნიშნული ტექნიკური ხელმოწერა დოკუმენტში მოხსენიებული იქნება როგორც „კვალიფიციური ელექტრონული შტამპი“.*

აუცილებელია, როგორც მმპ-ის მხრიდან ამსმპ-ის მიმართ გაგზავნილ, ისე ამსმპ-ის მიერ მმპ-სთვის გაგზავნილ პასუხებზე დაიტანებოდეს ელექტრონული შტამპი (9)-ის შესაბამისად. **აუცილებელია**, ამსმპ-მა და მმპ-მა შეამოწმონ კვალიფიციური ელექტრონული შტამპი როგოც წინამდებარე დოკუმენტის, ისე (9)-ის მოთხოვნების შესაბამისად.

5.5 ზოგადი მოთხოვნები სერტიფიკატების შემოწმების პროცესის მიმართ

ამ ქვეთავის მოთხოვნები ვრცელდება მიმდინარე თავში გამოყენებული ყველა სერტიფიკატის შემთხვევაში

1. **აუცილებელია,** კავშირის დამყარებისას მოხდეს სერტიფიკატის შემოწმება ყველა შემდგომი კრიტერიუმით:
   1.1. სერტიფიკატი გაცემულია ისეთი გამცემი ორგანოს მიერ, რომელიც აღიარებულია საქართველოში ღია ბანკინგის სერტიფიკატის სანდო გამცემად.
   1.2. სერტიფიკატის მოქმედება არ არის შეჩერებული ან გაუქმებული. **აუცილებელია**, შემოწმება დაეყრდნოს სერტიფიკატების ონლაინ სტატუსის პროტოკოლს (სოსპ, Online Certificate Status Protocol, OCSP) გამოყენება.
   1.3. **უმჯობესია**, დაცული საკომუნიკაციო არხის დამყარებისას კავშირის მონაწილე თითოეულ მხარეს (როგორც ამსმპ, ისე მმპ) გააჩნდეს OCSP Stapling-ის გამოყენების საშუალება. იმ შემთხვევაში, თუ კავშირის მონაწილე ერთი მხარე კავშირის დამყარების პროცესში მიუთითებს, რომ გააჩნია აღნიშნულის მხარდაჭერა, **აუცილებელია**, მეორე მხარემ დააბრუნოს სოსპ ყველა საჭირო პასუხი. წინააღმდეგ შემთხვევაში, **აუცილებელია** პირველმა მხარემ უარი თქვას დაცული კავშირის დამყარებაზე.
   1.4. **აუცილებელია**, დაცული იყოს სერტიფიკატების მოქმედების შემოწმების ყველა სათანადო მექანიზმი, მათ შორის სოსპ სერტიფიკატების მოქმედების შემოწმების წესი, რაც საერთაშორისო სტანდარტებითა და საუკეთესო პრაქტიკითაა განსაზღვრული.

5.6 ზოგადი მოთხოვნები ჰიპერბმულების შემოწმების მიმართ

აუცილებელია, მმპ-მა ამსმპ-ის სერვისების გამოძახების პროცესში შეამოწმოს ყველა ჰიპერბმული, რომელსაც ამსმპ მას დაუბრუნებს და დარწმუნდეს, რომ ის ნამდვილად ამ ამსმპ-ს ეკონტაქტება. კერძოდ:

1) **აუცილებელია**, API-სთან დაკავშირებული ჰიპერბმულების შემოწმება განხორციელდეს სერტიფიკატებში შესაბამისი ჩანაწერების (Common Name, Subject Alternate Name) შემოწმებისა და ამსმპ-ს ჰიპერბმულების შედარებით გზით
2) **აუცილებელია**, მომხმარებლის ავთენტიფიკაციის პროცესში OAuth2 სერვერის მეტაინფორმაციის (იხ. (10)) სისწორე დადასტურდეს ამსმპ-ს API პასუხების ავთენტურობის შემოწმების გზით, როგორც ეს განსაზღვრულია (11)-ით და API-ს აღმწერი სხვა შესაბამისი დოკუმენტაციით
3) **აუცილებელია**, OAuth2 ავტორიზაციის პროცესში გამოყენებული ჰიპერბმულების შემოწმება განხორციელდეს (12), (13) და სხვა შესაბამისი პროტოკოლების უსაფრთხოების საუკეთესო პრაქტიკების შესაბამისად

აუცილებელია, ამსმპ-მა შეამოწმოს მმპ-ს მიერ გადაცემული ყველა ჰიპერბმული და დარწმუნდეს, რომ ის ნამდვილად ამ მმპ-სთან ცვლის ინფორმაციას. **აუცილებელია**, შემოწმება ემყარებოდეს შემდეგ ძირითად პრინციპს:

1) **აუცილებელია**, გადამისამართების (Redirect) ტიპის ავთენტიფიკაციას გადაეცემოდეს TPP-Redirect-URI, როდესაც აღნიშნული პარამეტრი გათვალისწინებულია (2)-ით. მიუხედავად იმისა, რომ აღნიშნული პარამეტრი გადამისამართების ტიპის ავთენტიფიკაციისას ცალკეულ შემთხვევაში შეიძლება იყოს გამოცხადებული არააუცილებლად, წინამდებარე დოკუმენტთან თავსებადობის მიზნით მისი გადაცემა მმპ-ს მხრიდან **სავალდებულოა**.
2) **აუცილებელია**, ამსმპ-მა შეამოწმოს TPP-Redirect-URI და TPP-Nok-Redirect-URI (თუ ეს უკანასკნელი გადაცემულია მმპ-ს მხრიდან), კერძოდ შეადაროს იგი მმპ-ის სერტიფიკატში არსებულ ჩანაწერებს (Common Name, Subject Alternate Name)

6 მომხმარებლის ავთენტიფიკაცია და ავტორიზაცია

6.1 მომხმარებლის ავთენტიფიკაციის ძირითადი პრინციპები

აუცილებელია, API მოთხოვნების გამოძახებისას გამოიყენებოდეს OAuth2 პროტოკოლი, რომლის რეალიზაცია სრულად შეესაბამება (13) მოთხოვნებს.

შენიშვნა: API-ს აღმწერი დოკუმენტაცია ((11), (14) ან სხვა) განსაზღვრავს გამონაკლის შემთხვევებს, როდესაც OAuth2 ტოკენის გადაცემა აუცილებელი არ არის (მაგ. ისეთი პროცესების დასაწყისში, რომლებსაც აღნიშნული დოკუმენტაციით აუცილებლად მოჰყვება ავთენტიფიკაციის მოთხოვნა და, შესაბამისად, ტოკენის გაცემა), მაგალითად - ანგარიშის ინფორმაციის გაზიარებაზე თანხმობის გამოხატვის რეგისტრაცია, საგადახდო დავალების პირველადი რეგისტრაცია ამსმპ-ში და სხვა, თუმცა შემთხვევათა უმრავლესობაში მოითხოვება ტოკენის გადაცემა.

მიუხედავად იმისა, რომ წინამდებარე დოკუმენტით დასაშვებია (2)-ით განსაზღვრული სხვა ტიპის ავთენტიფიკაცია (Embedded, Decoupled), **აუცილებელია** ავთენტიფიკაციისა და ავტორიზაციის პროცესი საბოლოოდ დაიყვანებოდეს OAuth2-ის ტოკენებზე და API-სთან ურთიერთობისას გამოიყენებოდეს აღნიშნული ტოკენები. აღნიშნული რეგულირდება ამ დოკუმენტის 6.8 თავით.

ამ დოკუმენტის მიზნებისათვის, მომხმარებლის ავთენტიფიკაცია შეიძლება მოიხსენიებოდეს ორგვარად:

- მომხმარებლის ზოგადი ავთენტიფიკაცია მმპ-სა და ამსმპ-ს შორის დაცულ არხში - ნებმისმიერი ავთენტიფიკაცია, რომელიც შესაძლოა აკმაყოფილებდეს ან არ აკმაყოფილებდეს მარეგულირებელი კანონმდებლობის მოთხოვნებს მომხმარებლის ძლიერ ავთენტიფიკაციასთან დაკავშირებით;
- მომხმარებლის ძლიერი ავთენტიფიკაცია - ავთენტიფიკაცია, რომელიც აკმაყოფილებს მარეგულირებელი კანონმდებლობის მოთხოვნებს მომხმარებლის ძლიერ ავთენტიფიკაციასთან დაკავშირებით.

აუცილებელია, მომხმარებლის ზოგადი ავთენტიფიკაციისათვის მმპ-სა და ამსმპ-ს შორის არხში გამოიყენებოდეს OAuth2 პროტოკოლი, როგორც „წინარე ნაბიჯი“ (pre-step), როგორც ეს მითითებულია (2)-ის 4.3 თავით ყველა შეტყობინებისათვის, რომელსაც მმპ გადასცემს ამსმპ-ს. გამონაკლისს შეადგენს თანხმობის გაცემის ტრანზაქცია (იხ. **Error! Reference source not found.** თავი), რომლის მიმართ მოთხოვნები ამ თავითვე რეგულირდება.

შესაბამისად, **აუცილებელია** მმპ-ს მიერ გაგზავნილ ყველა შეტყობინებაში გათვალისწინებული იყოს ყველა იმ მოთხოვნის შესრულება, რომელიც (2)-ში მონიშნულია დათქმით „თუ OAuth2 გამოყენებული იქნა საგადახდო სერვისის მომხმარებლის ავთენტიფიკაციისათვის“ („if OAuth2 has been used as PSU authentication”). **აუცილებელია,** OAuth2 ტოკენი გადაეცემოდეს მოთხოვნის სათაურის (Header) პარამეტრში Authorization, ტიპით Bearer.

აუცილებელია, ტოკენი გაცემული იყოს უშუალოდ ამსმპ-ის მიერ, გარდა იმ შემთხვევისა როდესაც ამსმპ-სა და ტოკენის გამცემს შორის არსებობს შეთანხმება და ტოკენი გამოიყენება

მომხმარებლის ზოგადი ავთენტიფიკაციისათვის (როდესაც ტოკენის გამცემი ტოკენს ამსმპ-სათვის აუთსორსინგის მომსახურების გაცემის ფარგლებში გასცემს და კონკრეტულ შემთხვევაში მოქმედებს ამსმპ-ის სახელით, ეს ითვლება ამსმპ-ის მიერ ტოკენის გაცემად).

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა უარჰყოს თანხმობის გაცემის ტრანზაქცია მხოლოდ იმ მიზეზით, რომ მან ვერ ამოიკითხა მმპ-ის მიერ გაცემული ტოკენი, დაადგინა რომ აღნიშნული ტოკენი მისთვის უცნობი გამცემის მიერაა გაცემული ან გაცემულია მის მიერ მაგრამ გაუქმებულია სხვადასხვა მიზეზით. ამ შემთხვევაში **აუცილებელია**, ამსმპ მოიქცეს ზუსტად ისე, როგორც მოიქცეოდა მმპ-ს მიერ ცარიელი ტოკენის გადმოცემის შემთხვევაში.

<u>შენიშვნა:</u> თუ ტოკენი გაცემულია ამსმპ-საგან განსხვავებული მხარის მიერ, მაგრამ მის გამოყენებაზე არსებობს შეთანხმება მმპ-სა და ამსმპ-ს შორის, ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა განიხილოს ამ ტოკენის არსებობა მომხმარებლის ძლიერ ავთენტიფიკაციად, მიუხედავად იმისა, თუ რამდენი ავთენტიფიკაციის ფაქტორი იყო გამოყენებული აღნიშნული ტოკენი გაცემის შემთხვევაში და ცნობილი იყო ამის შესახებ ამსმპ-სათვის თუ არა. თუმცა შესაძლოა ამსმპ-მა გარდაქმნას აღნიშნული ტოკენი მომხმარებლის ძლიერი ავთენტიფიკაციის ტოკენად **Error! Reference source not found.**-ით განსაზღვრული წესით.

6.2 ავტორიზაციის რესურსის ცნება და ავტორიზაციის პროცესის აბსტრაქცია

ამ დოკუმენტის ფარგლებში ავტორიზაცია გულისხმობს მმპ-ის მიერ ამსმპ-ში რაიმე ქმედების ჩატარებაზე სმმ-ის მიერ თანხმობის მიღებას. აღნიშნული პროცესი წარიმართება ერთიდაიგივე სცენარით, მიუხედავად იმისა, რომ ავტორიზაცია სხვადასხვაგვარ საკითხებს (ინფორმაციის მიღებას ანგარიშებზე, ბარათებზე და სხვა, გადახდის ინიცირებას და ა.შ.) შეეხება.

ავტორიზაციის რესურსი არის ცნება, რომელიც გამოხატავს იმ ერთეულს, რომელზეც სმმ-მა უნდა გამოხატოს თანხმობა („მოახდინოს ავტორიზაცია“). წინამდებარე დოკუმენტის ამ ვერსიის მიზნისათვის, ავტორიზაციას დაქვემდებარებული ერთეული შეიძლება იყოს:

- ანგარიშის ინფორმაციის გაზიარებაზე მომხმარებლის თანხმობის მოთხოვნა (დოკუმენტი), რომელიც მმპ-მ დაარეგისტრირა ამსმპ-ში, იხ. (11)
- გადახდის ინიცირების მოთხოვნა, რომელიც მმპ-მ დაარეგისტრირა ამსმპ-ში, იხ. (11)
- ინიცირებული გადახდის გაუქმების მოთხოვნა, რომელიც მმპ-მ დაარესისტრირა ამსმპ-ში, იხ. (11)
- სხვა კომერციული ბანკიდან მომხმარებლის პერსონალური ინფორმაციის მიღების მოთხოვნა (დოკუმენტი), რომელიც მმპ-მ დაარესისტრირა ამსმპ-ში, იხ. (14)

<u>შენიშვნა:</u> წინამდებარე დოკუმენტის შემდგომ ვერსიებში ეტაპობრივად დაემატება სხვა ერთეულებიც.

ტექნიკური თვალსაზრისით, ავტორიზაციის რესურსი არის ჰიპერბმული, რომელიც ცალსახად მიუთითებს ერთეულს, რომელზეც ხდება თანხმობის გამოხატვა.

როდესაც ამსმპ-ს სისტემაში რეგისტრირდება თანხმობის გამოსახატი ერთეული (მაგ. ანგარიშის ინფორმაციის გაზიარებაზე მომხმარებლის თანხმობის მოთხოვნის დოკუმენტი), **აუცილებელია**, ამსმპ-მა წარმართოს ავტორიზაციის რესურსის შექმნის და შემდგომი მართვის პროცესი ჰიპერბმულების სექციის (_links) საშუალებით.

6.3 ავტორიზაციის რესურსის შექმნა არაცხადად

შესაძლოა, ამსმპ მხარს უჭერდეს სცენარს, რომელიც ითვალისწინებს ავტორიზაციის რესურსების არაცხადად შექმნას, როგორც ეს აღწერილია (2)-ში (ე.წ. „Implicit Start of the Authorisation Process“).

აღნიშნული წარმოადგენს ოპტიმიზაციას ისეთი შემთხვევებისათვის, როდესაც ამსმპ-ს აქვს ყველა სათანადო ინფორმაცია მომხმარებლის ავთენტიფიკაციის დასაწყებად. ამ დროს ამსმპ ავტომატურად ქმნის ავტორიზაციის ბმულს მაშინვე, როგორც კი ხდება ავტორიზაციას დაქვემდებარებული ერთეულის შექმნა ამსმპ-ს სისტემაში (მაგ. თანხმობის დოკუმენტის).

აუცილებელია, ამსმპ-მა აღნიშნული რესურსი დააბრუნოს ავტორიზაციას დაქვემდებარებული ერთეულის შექმნის მოთხოვნის პასუხად, _links სექციაში, როგორც scaStatus ტიპის ჰიპერბმული (*შენიშვნა: არ აგერიოთ scaStatus ატრიბუტში!*). და scaStatus შეიცავს უშუალოდ ავტორიზაციის რესურსის ჰიპერბმულს.

ამ ჰიპერბმულის მიღების შემდეგ **აუცილებელია**, მმპ-მა პირდაპირ დაიწყოს ავტორიზაციის პროცესი.

თუ მმპ-ს მიერ გადმოცემულია TPP-Explicit-Authorisation-Preferred=true პარამეტრი, **უმჯობესია** ამსმპ-მა გაითვალისწინოს აღნიშნული და არ შექმნას ავტორიზაციის რესურსი არაცხადად.

6.4 ავტორიზაციის რესურსების ცხადი შექმნა და დამატებითი ინფორმაციის მიწოდება ავტორიზაციისათვის

შესაძლოა, ამსმპ-მა მხარი არ დაუჭიროს ავტორიზაციის რესურსების არაცხად შექმნას (იხ. თავი 6.3). ასეთ შემთხვევაში აუცილებელია, ამსმპ-მა მხარი დაუჭიროს ავტორიზაციის რესურსების ცხად შექმნას წინამდებარე თავის შესაბამისაც. მეტიც, გადაწყვეტის ერთგვაროვნებისათვის **უმჯობესია** ამსმპ-მა ყველა შემთხვევაში გამოიყენოს ავტორიზაციის რესურსების ცხადი შექმნის მიდგომა.

მას შემდეგ, რაც მმპ-ს მოთხოვნით ამსმპ შექმნის ავტორიზაციას დაქვემდებარებული ერთეულს საკუთარ სისტემაში, აუცილებელია ამსმპ-მა დააბრუნოს ერთ-ერთი შემდეგი ჰიპერბმული _links სექციაში:

1) startAuthorization
2) startAuthorisationWithPsuIdentfication
3) startAuthorisationWithAuthenticationMethodSelection
4) startAuthorisationWithTransactionAuthorisation

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს startAuthorisation* ტიპის სხვა ჰიპერბმულები რომელიც (2)-ით არის განსაზღვრული, თუმცა არ არის მოხსენიებული ამ თავში.

ყველა ზემოაღნიშნულ შემთხვევაში ამსმპ აბრუნებს ბმულს ავტორიზაციის რესურსის შესაქმნელ მისამართზე, რომელიც **აუცილებელია** მმპ-მა გამოიძახოს HTTP PUT მეთოდის დახმარებით, როგორც ეს აღწერილია (2)-ის 7.1 თავის მიხედვით.

როდესაც ამსმპ აბრუნებს startAuthorization ტიპის ჰიპერბმულს (და არა startAuthorizationWith* ტიპის ჰიპერბმულს), ეს ჯერ კიდევ არ ნიშნავს, რომ ამსმპ-ს აქვს ყველა ინფორმაცია ავტორიზაციის წარმატებით დასრულებისათვის. ამდენად, **აუცილებელია** მმპ-მა გააანალიზოს ამსმპ-ს მიერ დაბრუნებული პასუხი - ხომ არ ითხოვს ამსმპ გარკვეული დამატებითი ინფორმაციის წარმოდგენას _links სექციაში დაბრუნებული ჰიპერბმულებით.

როდესაც ამსმპ აბრუნებს startAuthorizationWith* ტიპის ჰიპერბმულებს, ეს იმთავითვე ნიშნავს, რომ ამსმპ-ს ხელთ არსებული ინფორმაცია არასაკმარისია სმმ-ის ავთენტიფიკაციის დასაწყებად და მმპ ვალდებულია, გარკვეული პარამეტრები გადასცეს ამსმპ-ს უშუალოდ ავტორიზაციის რესურსის შექმნის მოთხოვნისთანავე.

საბოლოოდ, როგორც startAuthorization, ისე startAuthorizationWith* ტიპის ჰიპერბმულებით დაბრუნებული მისამართების გამოძახების პასუხად, **შესაძლოა** მმპ-მა მიიღოს დამატებითი ინფორმაციის გადაცემის მოთხოვნა. კერძოდ, **შესაძლოა** ამსმპ-მა _links სექციაში დააბრუნოს, selectAuthenticationMethod, updatePsuIdentification ან სხვა. აღნიშნული საკითხი განხილული იქნება ამ დოკუმენტის შემდეგ ქვეთავებში.

6.5 ავტორიზაციის დასაშვები ტიპები, რომელიც შეიძლება მოითხოვოს ამსმპ-მა

ავტორიზაციის რესურსის როგორც ცხადი, ისე არაცხადი შექმნისას **აუცილებელია** ამსმპ-მა მმპ-ს დაუბრუნოს ინფორმაცია იმის თაობაზე, რა ტიპის ავტორიზაციის პროცედურა უნდა დაიწყოს მმპ-მა:

1) გადამისამართება (Redirect)
2) ჩაშენებული (Embedded)
3) განცალკევებული (Decoupled)

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია** გადამისამართების ტიპის ავტორიზაცია იყოს OAuth2 ტიპისა, ანუ ავტორიზაციის პროცესის წარმატებით დასრულებისას დაბრუნდეს შესაბამისი ტოკენები. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მოითხოვოს (2)-ით განსაზღვრული გადამისამართების ტიპის ავტორიზაცია oAuth2-ის გარეშე (მაგ. (2)-ის 5.1.1 თავით განსაზღვრული).

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია**, ჩაშენებული ტიპის ავტორიზაციამ მოითხოვოს ავთენტიფიკაცია მხოლოდ ერთი ფაქტორით. ამ ავთენტიფიკაციის პროცესში ამსმპ-მა მმპ-სგან **არავითარ შემთხვევაში** არ უნდა მოითხოვოს ან/და მიიღოს:

1) ცოდნაზე დამყარებული ფაქტორი (სტატიკური პაროლი ან PIN კოდი)
2) სტატიკური ბიომეტრიული მონაცემი (მაგ. თითის ანაბეჭდის გამოსახულება)

თუ ამსმპ მხარს უჭერს ჩაშენებული ტიპის ავტორიზაციას, **აუცილებელია** მან მოითხოვოს და მიიღოს მხოლოდ დინამიკურად შექმნილი ავთენტიფიკაციის მონაცემები (მაგალითად, ერთჯერადი SMS კოდი, ერთჯერადი კოდების გენერატორის მიერ გენერირებული ტოკენი, ბარათის მიერ შექმნილი კრიპტოგრამა და ა.შ.), რომელთა წარმოდგენაზე მმპ-ს დაუწესდება დროითი ლიმიტი, არაუმეტეს 5 (ხუთი) წუთისა.

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია**, ჩაშენებული და განცალკევებული ავტორიზაციის პროცესის ბოლოს მმპ-მა მოითხოვოს და მიიღოს შესაბამისი ტოკენები. ამრიგად, **აუცილებელია** ბიზნეს-შინაარსის მქონე API მეთოდების (მაგ. ანგარიშის ტრანზაქციების სია, გადახდის სტატუსის შემოწმება და ა.შ.) გამოძახება ყოველთვის უზრუნველყოფილი იყოს Access Token-ით, რომელიც შემდგომ გადაეცემა Authorization სათაურში, Bearer ტიპით.

6.6 ავტორიზაციის ტიპის არჩევა

ამ დოკუმენტთან თავსებადობის მიზნებისათვის, ავტორიზაციის დასაშვები ტიპები სხვადასხვაგვარად რეგულირდება იმის მიხედვით, თუ მერამდენე ავტორიზაცია ხორციელდება ავტოროზაციას დაქვემდებარებულ კონკრეტულ ერთეულზე:

1) პირველი ან/და ერთადერთი ავტორიზაცია
2) შემდგომი ავტორიზაცია (მაგ. იურიდიული პირების შემთხვევაში შემდგომი დამოწმება)

პირველი ან/და ერთადერთი ავტორიზაციის შემთხვევაში **აუცილებელია** გამოყენებული იქნას გადამისამართების ტიპის ავთენტიფიკაცია, გარდა შემდეგი გამონაკლისებისა:

1) ავტორიზაციის რესურსს შექმნისას Authorization სათაურში გადაეცა იმგვარი OAuth2 ტოკენი, რომლის შექმნისას გამოყენებული იყო „ცოდნის“ ტიპის ავთენტიფიკაცის ფაქტორი და მარეგულირებელი კანონმდებლობა ნებას რთავს ამსმპ-ს, ჩათვალოს რომ ავთენტიფიკაცია ხდება უწყვეტ სესიაში და მოითხოვოს მხოლოდ მეორე ფაქტორი. ასეთ შემთხვევაში **უმჯობესია** ამსმპ-მა მოითხოვოს ჩაშენებული ტიპის ავთენტიფიკაცია მეორე ფაქტორით (მაგ. SMS კოდით).

   შენიშვნა: აღნიშნული არ წარმოადგენს ამსმპ-ს ვალდებულებას და **შესაძლოა** ამის ნაცვლად ამსმპ-მა მოითხოვოს გადამისამართების ტიპის ავტორიზაცია მეორე ფაქტორით ან ორივე ფაქტორით;

2) ავტორიზაციას დაქვემდებარებული ერთეული დაბალი რისკის მატარებელია და მარეგულირებელი კანონმდებლობით ნებადართულია მისი ავტორიზაცია მხოლოდ მოკლე (არაუმეტეს 8 სიმბოლოსი) დროებითი (არაუმეტეს 3 წუთისა) ერთჯერადი კოდის გამოყენებით. ასეთ შემთხვევაში **უმჯობესია** ამსმპ-მა მოითხოვოს ჩაშენებული ტიპის ავთენტიფიკაცია ამ ტიპის ფაქტორით. **უმჯობესია** კოდი იყოს მოთხოვნა-პასუხზე (challenge-response) დაფუძნებული, თუ მარეგულირებელი კანონმდებლობით სხვა რამ არ არის განსაზღვრული;

   შენიშვნა: აღნიშნული სქემის რეალიზება არ წარმოადგენს ამსმპ-ს ვალდებულებას და **შესაძლოა** ამის ნაცვლად ამსმპ-მა მოითხოვოს გადამისამართების ტიპის ავტორიზაცია მეორე ფაქტორით ან ორივე ფაქტორით

3) მმპ-მა ცხადად მიუთითა, რომ არ სურს გადამისამართების ტიპის ავტორიზაცია და ამჯობინებს განცალკევებული ავტორიზაციის გამოყენებას, ანუ მმპ-მა ავტორიზაციის რესურსის შექმნისას სათაურში მმპ-მა მიუთითა TPP-Redirect-Preferred=false და TPP-

Decoupled-Preferred=true. ამ შემთხვევაში **აუცილებელია** ამსმპ-მა დაიწყოს განცალკევებული ტიპის ავტორიზაცია და მიუთითოს მმპ-სა და სმმ-ს რომ ავტორიზაცია უნდა გაგრძელდეს იმ სისტემაში, რომლითაც ამსმპ საკუთარ კლიენტურას სთავაზობს ანგარიშების სამართავად (ინტერნეტ ან/და მობილბანკში).

4) მმპ-მა ცხადად მიუთითა, რომ არ სურს არც გადამისამართების, არც განცალკევებული ავტორიზაციის გამოყენება, ანუ მმპ-მა ავტორიზაციის რესურსის შექმნისას სათაურში მმპ-მა მიუთითა TPP-Redirect-Preferred=false და TPP-Decoupled-Preferred=false. ამ დროს **შესაძლოა** ამსმპ-მა მმპ-ს შესთავაზოს ჩაშენებული ტიპის ძლიერი ავთენტიფიკაცია, როგორც განსაზღვრულია 6.12 თავით, თუ ამსმპ-ს ამის შესაძლებლობა გააჩნია. თუ ამსმპ-ს აღნიშნული საშუალება არ გააჩნია, **აუცილებელია** მან მოითხოვოს გადამისამართების ტიპის ავტორიზაცია.

თუ ავტორიზაციას დაქვემდებარებულ ერთეულს ესაჭიროება ერთზე მეტი ავტორიზაცია (მაგ. იურიდიული პირების შემთხვევაში), **აუცილებელია**, მმპ-ს მხრიდან მეორე ავტორიზაციის რესურსის შექმნისთანავე ამსმპ-მა მოითხოვოს განცალკევებული ტიპის ავტორიზაცია და შემდგომი პროცესი განაგრძოს იმ სისტემაში, რომელსაც სთავაზობს საკუთარ კლიენტურას ანგარიშების სამართავად (ინტერნეტ ან/და მობილბანკში). მმპ-ს მართვა დაუბრუნდება მას შემდეგ, რაც ავტორიზაციის პროცესი დასრულდება (ყველა პასუხისმგებელი პირი დაამოწმებს ოპერაციას), როგორც ეს (2)-ით არის განსაზღვრული. ანუ მიუხედავად იმისა, თუ რამდენი დასტური ესაჭიროება კონკრეტულ ავტორიზაციას დაქვემდებარებულ ერთეულს სინამდვილეში ამსმპ-ს თვალთახედვით, **აუცილებელია** რომ მმპ-ს თვალთახედვით ეს იყოს ჯამურად ორი ავტორიზაციის რესურსი, რომელთაგან პირველის ავტორიზება მოახდენს ოპერაციის ინიციატორი, ხოლო დანარჩენი მოქმედი პირები ჯამურად, ამსმპ-ს სპეციფიკური წესით მოახდენენ მეორის ავტორიზებას. მეტიც, მმპ-ს მხრიდან ახალი ავტორიზაციის რესურსის მოთხოვნის შემთხვევაშიც კი, ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა შექმნას მესამე და შემდგომი ავტორიზაციის რესურსი.

აუცილებელია, ამსმპ-ს იმ სისტემათაგან, რომლითაც იგი საკუთარ კლიენტურას (ინტერნეტ ბანკი, მობილბანკი და სხვა) სთავაზობს ანგარიშების სამართავად, სულ მცირე ერთი იყოს აღჭურვილი იმ შესაძლებლობით, რომ დაამუშავოს განცალკევებული ტიპის ავტორიზაციის მოთხოვნები, მარეგულირებელ კანონმდებლობასთან სრულ შესაბამისობაში.

შესაძლოა მმპ-მა ამსმპ-ს ავტორიზაციის შექმნის პროცესში გადასცეს Authorization სათაური, შესაბამისი ტოკენით. თუ აღნიშნული ტოკენი მოქმედია, ავტორიზაციას დაქვემდებარებული ერთეულის შინაარსიდან გამომდინარე, მარეგულირებელი კანონმდებლობით განსაზღვრულ შემთხვევებში ამსმპ-ს შეუძლია:

1) ავტომატურად მოახდინოს ავთენტიფიკაცია, ტოკენზე დაყრდნობით
2) მოითხოვოს ავთენტიფიკაცია და ავტორიზაცია მხოლოდ მეორე ფაქტორით, ამ დოკუმენტის 6.9 თავის შესაბამისად.
3) მოახდინოს მომხმარებლის ავთენტიფიკაცია (მათ შორის ძლიერი ავთენტიფიკაცია) ისე, რომ ყურადღება არ მიაქციოს ტოკენის არსებობას.

6.7 OAuth2-ის გამოყენება გადამისამართების ტიპის ავთენტიფიკაციის შემთხვევაში

აუცილებელია, გადამისამართების (Redirect) ავთენტიფიკაციის შემთხვევაში OAuth2 პროტოკოლის რეალიზება სრულ თანხვედრაში იყოს როგორც (2)-ის მე-13 თავთან, ისე (13) მოთხოვნებთან. **აუცილებელია**, მომხმარებლის ძლიერი ავთენტიფიკაცია ეყრდნობოდეს Authorization Code Grant -ს (12)-ის მიხედვით.

როდესაც გამოყენებულია OAuth2 პროტოკოლი გადამისამართების ტიპის ავტორიზაციის შემთხვევაში, ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მოითხოვოს მმპ-საგან ტოკენის მიღების დადასტურება, რაც იმაში გამოიხატება, რომ მან არ უნდა დააბრუნოს confirmation ტიპის ჰიპერბმული _links სექციაში (მაგ. (2) -ის 5.3.1 და 6.3.1.1 თავის შესაბამისად).

6.8 OAuth2-ის გამოყენება გადამისამართებისგან განსხვავებული ტიპის ავთენტიფიკაციისას

// გადახვევა XS2A ჩარჩოდან

აუცილებელია, ამსმპ-ს OAuth2 ავტორიზაციის სერვისს გააჩნდეს შესაძლებლობა, გასცეს Client Credentials Grant ტიპის ტოკენი ჩაშენებული (Embedded) და განცალკევებული (Decoupled) ავთენტიფიკაციის შემთხვევაში.

მას შემდეგ, რაც დასრულდება (2)-ის შესაბამისი განსაზღვრული ავთენტიფიკაციის პროცესი **აუცილებელია**, სტატუსის ბოლოწერტილმა (მაგ. /v1/consents/{consentId}/status) დააბრუნოს ჰიპერბმულების (_links) სექცია, და მასში მითითებული იყოს OAuth2 სერვერის მეტაინფორმაციის ჰიპერბმული 8.2 თავის შესაბამისად.

აუცილებელია, მმპ-მა OAuth2 Scope პარამეტრი მიუთითოს ზუსტად იგივე წესით, როგორც მითითებული იქნებოდა გადამისამართების ტიპის ავტორიზაციისას (იხ. (2)-ის მე-13 თავი).

აუცილებელია, მმპ-მა მოითხოვოს OAuth2 ტოკენი ჩაშენებული და განცალკევებული ავტორიზაციის გავლის შემდეგ, თუ მას აღნიშნული ტოკენი უკვე მიღებული არ აქვს იმავე Scope-სათვის. **აუცილებელია**, მმპ-მა ტოკენი მოითხოვოს client_credential ტიპის grant-ით. თუ მმპ-ს აღნიშნული Scope-სათვის ტოკენი უკვე მიღებული აქვს და იგი აქტიურია, **შესაძლოა** ამსმპ-მა მას იგივე ტოკენი დაუბრუნოს.

აუცილებელია, დაცული იყოს ყველა ის უსაფრთხოების მოთხოვნა, რომელიც განსაზღვრულია (13)-ით და პირდაპირ არაა დაკავშირებული Authorization Code Grant ტიპის ავტორიზაციასთან.

აუცილებელია, მომხმარებლის OAuth2 ავტორიზაციის შემდეგ კლიენტის (მმპ-ის) ავთენტიფიკაცია და ავტორიზაცია მოხდეს 5.2 თავის შესაბამისად და პროტოკოლად გამოყენებული იყოს (5).

6.9 მომხმარებლის ზოგადი ავთენტიფიკაციის გარდაქმნა მომხმარებლის ძლიერ ავთენტიფიკაციად

შესაძლოა, ამსმპ-მა გამოიყენოს მის ხელთ არსებული ზოგადი ავთენტიფიკაციის ტოკენი (იხ. 6.1) და განიხილოს მისი წარმოდგენა ერთი ფაქტორის მეშვეობით ავთენტიფიკაციის გასავლელად, რათა სმმ-ს გაუმარტივოს ძლიერი ავთენტიფიკაციის გავლის პროცესი ამ თავით განსაზღვრული წესით და ძლიერი ავთენტიფიკაციის პროცესში მოსთხოვოს მხოლოდ ერთი ფაქტორის გამოყენება (მაგალითად, ჩათვალოს ზოგადი ავთენტიფიკაციის ტოკენის წარმოდგენა იმ ფაქტის დადასტურებად, რომ მომხმარებელს გავლილი აქვს ავთენტიფიკაცია სახელითა და პაროლით და ძლიერი ავთენტიფიკაციისათვის მოითხოვოს მხოლოდ SMS კოდით დადასტურება).

ამგვარი ოპტიმიზაციის რეალიზების შემთხვევაში **აუცილებელია**, თანხმობის გაცემის ტრანზაქციის ფარგლებში (იხ. **Error! Reference source not found.**) პროცესი შემდეგნაირად წარიმართოს:

1) მმპ იწყებს თანხმობის გაცემის ტრანზაქციის ინიცირებას და გადასცემს ტოკენს Authorization სათაურში.
2) ამსმპ არეგისტრირებს თანხმობის გაცემის ტრანზაქციას და აკავშირებს მას პირველ ბიჯში მოცემულ ტოკენთან.
3) ამსმპ იწყებს OAuth2 ძლიერი ავთენტიფიკაციის პროცესს ამ დოკუმენტით დასაშვები წესით.
4) ავტორიზაციის რესურსი, რომელსაც ამსმპ უბრუნებს სმმ-ს (იხ. 6.2) მოითხოვს შემცირებული რაოდენობის (თუმცა ძლიერი ავთენტიფიკაციისათვის აუცილებელი) ფაქტორებით ავთენტიფიკაციას. მაგალითად, ამსმპ-ის ავტორიზაციის სერვერი არ სთავაზობს სმმ-ს მომხმარებლის სახელისა და პაროლის შეყვანას და სთხოვს მხოლოდ SMS კოდის გაგზავნა-დადასტურებას.
5) ავთანტიფიკაციის პროცესის წარმატებით დასრულების შემდეგ გენერირდება ძლიერი ავთენტიფიკაციის OAuth2 ტოკენი 6.8 თავის ან 6.9 თავის შესაბამისად (იმის მიხედვით, თუ რომელი ტიპის ავთენტიფიკაცია იყო არჩეული)

6.10 startAuthorisationWithPsuIdentfication და სმმ-ის საიდენტიფიკაციო მონაცემების შეყვანა

იმ შემთხვევაში, როდესაც ავტორიზაციას დაქვემდებარებული ერთეულის შექმნის პასუხად ამსმპ აბრუნებს startAuthorisationWithPsuIdentfication ტიპის ჰიპერბმულს, ან ავტორიზაციის პროცესში, startAuthorisation (ან მისი რომელიმე მოდიფიკაციის) გამოძახების პასუხად _links სექციაში ბრუნდება updatePsuIdentification, მმპ-სათვის ეს მოასწავებს რომ ამსმპ მისგან ითხოვს მომხმარებლის საიდენტიფიკაციო მონაცემების შეყვანას.

აღნიშნულ ორ მიდგომას შორის განსხვავება ისაა, რომ startAuthorisationWithPsuIdentfication შემთხვევაში სმმ-ის საიდენტიფიკაციო მონაცემების გადაცემა ხდება ავტორიზაციის რესურსის შექმნის პროცესში, ხოლო მეორე შემთხვევაში ავტორიზაციის რესურსი უკვე შექმნილია, თუმცა საჭიროებს შევსებას ინფორმაციით.

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მოითხოვოს აღნიშნული, როდესაც მიმდინარეობს გადამისამართების ტიპის ავტორიზაცია. ან როდესაც სხვა ტიპის ავტორიზაცია მიმდინარეობს და მმპ-ს მხრიდან Authorization სათაურში გადაცემულია ტოკენი და ის ხარვეზიანი არ არის.

მომხმარებლის და კორპორატიული იდენტიფიკატორი, რომელიც უნდა გადაეცეს, შესაბამისად, PSU-ID და PSU-Corporate-ID სათაურში, უნდა გადაეცეს (15)-ით განსაზღვრული ფორმატის შესაბამისად:

1) 3-სიმბოლოიანი პრეფიქსი - იდენტიფიკატორის ტიპი
2) 2 სიმბოლო - გამცემი ქვეყნის კოდი
3) მინუს-სიმბოლო: „-“
4) იდენტიფიკატორი

ფიზიკური პირების შემთხვევაში დასაშვები პრეფიქსები და იდენტიფიკატორების ფორმატირების მაგალითები, რაც უნდა გადაეცეს PSU_ID ველში:

ტიპი	პრეფიქსი	მაგალითი
პასპორტის ნომერი	PAS	PASGE-11AB12345678
პირადობის მოწმობის ნომერი	IDC	IDCGE-12IA12345
პირადი ნომერი	PNO	PNOGE-012345678901

ცხრილი 3: ფიზიკური პირის იდენტიფიკატორები

თუ ფიზიკური პირის იდენტიფიკატორი არასაკმარისია, **აუცილებელია** მმპ-მა ასევე გადასცეს კორპორაციის იდენტიფიკატორი PSU_Corporate_ID სათაურში.

ქვემოთ მოყვანილია დასაშვები პრეფიქსები და იდენტიფიკატორის ფორმატირების მაგალითები იურიდიული პირებისათვის:

ტიპი	პრეფიქსი	მაგალითი
კომპანიის სარეგისტრაციო კოდი	NTR	NTRGE-0123456789

ცხრილი 4: ორგანიზაციის იდენტიფიკატორები

იმ შემთხვევაში, თუ გამოძახება მოხდა მხოლოდ PSU_ID პარამეტრით (მაგ. ამ ფიზიკურ პირს აქვს როგორც პირადი ანგარიში, ისე ემსახურება რომელიმე კორპორატიულ მომხმარებელს) და ამსმპ დასამოწმებელი ოპერაციის კონტექსტიდან ვერ დაადგენს, პირადი პროფილით მოქმედებს სმმ თუ კორპორატიულით, **აუცილებელია** ამსმპ-მა დააბრუნოს CORPORATE_ID_INVALID შეცდომა და psuMessage ველში მიუთითოს ნათელი ინსტრუქცია სმმ-ისათვის. აღნიშნული შეცდომის პასუხად მმპ-ს შეუძლია:

1) გადასცეს PSU_Corporate_ID სათაურში იგივე მნიშვნელობა რაც PSU_ID -ში, რაც იმის მანიშნებელია რომ სმმ პირადი პროფილის ფარგლებში მოქმედებს;
2) გადასცეს PSU_Corporate_ID სათაურში ორგანიზაციის იდენტიფიკატორი, რაც იმის მანიშნებელი იქნება, რომ სმმ ორგანიზაციული პროფილის ფარგლებში მოქმედებს.

6.11 startAuthorisationWithAuthenticationMethodSelection და ავთენტიფიკაციის მეთოდის შერჩევა

იმ შემთხვევაში, როდესაც ავტორიზაციას დაქვემდებარებული ერთეულის შექმნის პასუხად ამსმპ აბრუნებს startAuthorisationWithAuthenticationMethodSelection ტიპის ჰიპერბმულს, ან ავტორიზაციის პროცესში, startAuthorisation (ან მისი რომელიმე მოდიფიკაციის) გამოძახების პასუხად _links სექციაში ბრუნდება selectAuthenticationMethod, მმპ-სათვის ეს მოასწავებს რომ ამსმპ მისგან ითხოვს მომხმარებლის საიდენტიფიკაციო მონაცემების შეყვანას.

აღნიშნულ ორ მიდგომას შორის განსხვავება ისაა, რომ startAuthorisationWithAuthenticationMethodSelection შემთხვევაში ავთენტიფიკაციის მეთოდის გადაცემა ხდება ავტორიზაციის რესურსის შექმნის პროცესში, ხოლო მეორე შემთხვევაში ავტორიზაციის რესურსი უკვე შექმნილია, თუმცა საჭიროებს შევსებას ინფორმაციით.

აუცილებელია, ამსმპ-მა ბმულთან ერთად იმავე პასუხში დააბრუნოს არაცარიელი scaMethods მასივი და **აუცილებელია**, მმპ-მა შესთავაზოს სმმ-ს ერთ-ერთი მეთოდის არჩევა.

იმის მიხედვით, რომელი მიდგომა იყო განხორციელებული, აუცილებელია მმპ-მა ამსმპ-ს არჩეული მეთოდი გადასცეს ან ავტორიზაციის რესურსის შექმნის ბმულზე, რაც startAuthorisationWithAuthenticationMethodSelection-ით მიიღო, ან ავტორიზაციის მეთოდის ასარჩევ ბმულზე რომელიც selectAuthenticationMethod -ით მიიღო. შესავალი პარამეტრები (HTTP მოთხოვნის ტანი) ორივე შემთხვევაში აღწერილია (2)-ის 7.2.3 თავით.

მას შემდეგ, რაც ამსმპ მიიღებს ინფორმაციას ავთენტიფიკაციის მეთოდის შესახებ, მან ჰიპერბმულებით უნდა განაგრძოს ურთიერთობა მმპ-სთან, როგორც ეს აღწერილია (2)-ით.

თუ ამსმპ- ითხოვს ჩაშენებულ ავთენტიფიკაციას, ანუ ASPSP-SCA-Approach=EMBEDDED, მაშინ **აუცილებელია** მან _links სექციაში დააბრუნოს authoriseTransaction ტიპის ჰიპერბმული (და ასევე challenge ინფორმაცია, თუ არჩეულია შეკითხვა-პასუხის ტიპის ავთენტიფიკაციის მეთოდი). ამ ჰიპერბმულზე მმპ ატვირთავს სმმ-ის მიერ მითითებულ ერთჯერად კოდს, როგორც ეს მითითებულია (2)-ის 7.3 თავით.

თუ ამსმპ ითხოვს გადამისამართების ტიპის ავთენტიფიკაციას, **შესაძლოა** მან ავთენტიფიკაციიის მეთოდის არჩევის ოპერაცია გამოიყენოს იმისათვის, რათა მოახდინოს მომხმარებლის ზოგადი ავთენტიფიკაციის გარდაქმნა მომხმარებლის ძლიერ ავთენტიფიკაციად - კერძოდ, ამსმპ-ს შეუძლია დააბრუნოს OAuth პროტოკოლის ისეთი პარამეტრები, რომლებიც უზრუნველყოფენ მომხმარებლისთვის მხოლოდ SMS OTP ან სხვა მეორე ფაქტორის მოთხოვნას, დაეყრდნობიან რა Authorization სათაურში გადმოცემული OAuth2 ტოკენს როგორც პირველი ფაქტორით ავთენტიფიკაციას. აღნიშნული ოპტიმიზაცია **არააუცილებელია** და ამის ნაცვლად ამსმპ-ს შეუძლია ჩაატაროს სრულფასოვანი (ორფაქტორიანი) ავთენტიფიკაციის პროცესი.

6.12 startAuthorisationWithTransactionAuthorisation და ტრანზაქციის ავტორიზაციის ინფორმაციის მიწოდება

იმ შემთხვევაში, როდესაც ავტორიზაციას დაქვემდებარებული ერთეულის შექმნის პასუხად ამსმპ აბრუნებს startAuthorisationWithTransactionAuthorisation ტიპის ჰიპერბმულს, ან

ავტორიზაციის პროცესში, startAuthorisation (ან მისი რომელიმე მოდიფიკაციის) გამოძახების პასუხად _links სექციაში ბრუნდება authoriseTransaction, მმპ-სათვის ეს მოასწავებს რომ ამსმპ მისგან ითხოვს ტრანზაქციის დადასტურების ინფორმაციის შეყვანას. აღნიშნული ვრცელდება მხოლოდ ჩაშენებულ (Embedded) ავტორიზაციაზე.

აღნიშნულ ორ მიდგომას შორის განსხვავება ისაა, რომ startAuthorisationWithTransactionAuthorisation შემთხვევაში ტრანზაქციის დადასტურების ინფორმაციის გადაცემა ხდება ავტორიზაციის რესურსის შექმნის პროცესში, ხოლო მეორე შემთხვევაში ავტორიზაციის რესურსი უკვე შექმნილია, თუმცა საჭიროებს შევსებას ინფორმაციით.

აუცილებელია, ამ ტიპის ავტორიზაციის მოთხოვნის პროცესში ამსმპ-მ მმპ-ს მიაწოდოს ინფორმაცია არჩეული ავტორიზაციის მეთოდის შესახებ (ველი chosenScaMethod) რათა მმპ-მა სმმ-სგან მიიღოს ტრანზაქციის დადასტურების ინფორმაციის (მაგ. ერთჯერადი SMS კოდის) შეყვანა და გადასცეს იგი ამსმპ-ს, როგორც ეს აღწერილია (2)-ის 7.3 თავით.

აღნიშნულ სცენარის განხორციელებისას ვრცელდება დამატებითი შეზღუდვები:

1. **აუცილებელია**, ავთენტიფიკაციის ტიპი იყოს ერთ-ერთი შემდეგი:
   1.1. SMS_OTP - ამსმპ აგენერირებს ერთჯერად კოდს და უგზავნის მას მომხმარებელს SMS-ით
   1.2. PHOTO_OTP - ამსმპ აგენერირებს ფოტოს (მაგ. QR კოდს), რომლის სკანირება და დამუშავება და ამის საფუძველზე ტრანზაქციის დადასტურების ინფორმაციის გენერირება შეუძლია ამსმპ-ს მიერ მომხმარებლისთვის მიწოდებულ პროგრამას (მაგ. მობილბანკს) ან მოწყობილობას
   1.3. PUSH_OTP - მსგავსია SMS OTP-სი, თუმცა ნაცვლად SMS არხისა, ამსმპ მომხმარებელს ერთჯერად კოდს უგზავნის შეტყობინების სახით, სმარტფონში არსებულ სპეციალურ პროგრამაში (მაგ. მობილბანკში)
   1.4. SMTP_OTP - მსგავსია SMS OTP-სი, თუმცა ამსმპ მომხმარებელს ერთჯერად კოდს უგზავნის ელექტრონული ფოსტის გამოყენებით
   1.5. CHIP_OTP - მოწყობილობა, რომელსაც შეუძლია დააგენერიროს ტრანზაქციის დადასტურების ინფორმაცია კრიპტოგრაფიული ოპერაციის საფუძველზე. მოწყობილობის გამოყენების დამატებითი მოთხვნები რეგულირდება
2. **აუცილებელია**, ამსმპ-მა დაუბრუნოს „გამოწვევა“ (challenge) მმპ-ს.
3. **აუცილებელია**, მმპ-მა „გამოწვევა“ უჩვენოს სმმ-ს ეკრანზე
4. **აუცილებელია**, ერთჯერადი SMS კოდით (SMS_OTP), ელფოსტით (SMTP_OTP) ან Push ნოტიფიკაციიის (PUSH_OTP) ტიპის ავთენტიფიკაციის შემთხვევაში „გამოწვევა“ იყოს არანაკლებ 6 სიმბოლოსგან (ლათინური ასოებისა და ციფრების კომბინაცია) შემდგარი. **აუცილებელია**, ეს „გამოწვევა“ ტრანზაქციის დადასტურების ინფორმაციასთან (ერთჯერადი კოდი) ერთად გაიგზავნოს სმმ-თან ცალკე არხით.
5. PHOTO_OTP ტიპის შემთხვევაში „გამოწვევა“ **არავითარ შემთხვევაში** არ უნდა დაბრუნდეს განცალკევებული URL-ით (imageLink ველი, იხ. (2) თავი 14.10), არამედ კოდირებული ინფორმაცია დაბრუნდეს image ველით. თავად სურათი **არავითარ შემთხვევაში** არ უნდა შეიცავდეს ვებ-მისამართს. **აუცილებელია**, სურათში ინფორმაცია განთავსებული იყოს დაშიფრულად, რათა მისი გაშიფვრა შესაძლებელი იყოს მხოლოდ ამსმპ-ს მობილბანკით, როდესაც სურათი მობილური ტელეფონის კამერის მეშვეობით დასკანერდება. სურათის

სკანირების პასუხად მობილბანკმა უნდა დააგენერიროს ერთჯერადი კოდი - ტრანზაქციის დადასტურების ინფორმაცია და უჩვენოს იგი სმმ-ს.

6. **აუცილებელია**, ტრანზაქციის დადასტურების ინფორმაცია სმმ-მა შეიყვანოს მმპ-ს სისტემაში და ამსმპ-მ მიიღოს იგი უშუალოდ მმპ-სგან. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მიიღოს ეს მონაცემი რაიმე სხვა გზით.
7. **აუცილებელია**, ტრანზაქციის დადასტურების ინფორმაცია (მაგ. ერთჯერადი SMS კოდი) დაკავშირებული იყოს კონკრეტულ ავტორიზაციის რესურსთან და შეუძლებელი იყოს მისი გამოყენება სხვა ავტორიზაციის რესურსისათვის
8. **აუცილებელია**, ტრანზაქციის დადასტურების ინფორმაცია იყოს მოკლევადიანი (არაუმეტეს 5 წუთისა), რის შემდეგაც მისი გამოყენება იყოს შეუძლებელი
9. **შესაძლოა**, PHOTO_OTP და მისი დადასტურება გამოყენებული იქნას ორფაქტორიანი ავთენტიფიკაციის ფორმით, თუ დაცული იქნება მომხმარებლის ძლიერი ავთენტიფიკაციისადმი წაყენებული ყველა მოთხოვნა.

6.12.1 CHIP_OTP ტიპის ჩაშენებული ავთენტიფიკაციის გამოყენების დამატებითი მოთხოვნები

ჩაშენებული ტიპის ავთენტიფიკაციის შემთხვევაში **შესაძლოა** გამოყენებული იქნას რაიმე მოწყობილობა, რომელშიც უსაფრთხოდ ინახება კრიპტოგრაფიული მასალა (მაგ. დახურული ან საიდუმლო გასაღები) და რომელსაც შეუძლია კრიპტოგრაფიული გარდაქმნების მეშვეობით შექმნას ტრანზაქციის დადასტურების ინფორმაცია, რომელსაც მომხმარებელი მიაწვდის მმპ-ს, ხოლო ეს უკანასკნელი კი გადასცემს ამსმპ-ს.

უმჯობესია, მოწყობილობას გააჩნდეს საშუალება, ტრანზაქციის დადასტურების ინფორმაცია დააგენერიროს კრიპტოგრაფიული გასაღებისა და ამსმპ-დან მიღებული „გამოწვევის“ საფუძველზე. ეს დოკუმენტი არ აწესებს რაიმე სპეციალურ მოთხოვნას „გამოწვევასთან“ დაკავშირებით.

შენიშვნა: თავად „გამოწვევა“ შეიძლება შეიყვანოს მომხმარებელმა ხელით (მაგ. სპეციალური მოწყობილობის კლავიატურის მეშვეობით) ან მოწყობილობას გადასცეს მმპ-მა (მაგ. EMV ბარათს გადასცეს ბარათის წამკითხველის გამოყენებით).

თუ მოწყობილობა მხარს არ უჭერს „გამოწვევის“ მიღებას, CHIP_OTP **არავითარ შემთხვევაში** არ უნდა იქნას გამოყენებული ისეთი ოპერაციების დასამოწმებლად, რომლებისთვისაც მარეგულირებელი კანონმდებლობის შესაბამისად მოთხოვნილია ტრანზაქციის ინფორმაციასთან დინამიკური ბმა. **უმჯობესია**, ამ მოწყობილობის გამოყენება საერთოდ არ მოხდეს ჩაშენებული ტიპის ავთენტიფიკაციაში.

შენიშვნა: გადამისამართების ან განცალკევებული ტიპის ავთენტიფიკაციის შემთხვევაში ეს დოკუმენტი არ კრძალავს ისეთი მოწყობილობის გამოყენებას, რომლებსაც არ აქვთ „გამოწვევის“ მხარდაჭერა, ვინაიდან ინფორმაციის შეყვანა ხდება ამსმპ-ს მიერ კონტროლირებად გარემოში და გარე მხარეებს არ აქვთ (ან შეზღუდული აქვთ) წვდომა მოწყობილობის მიერ გენერირებულ მიმდევრობებზე.

6.13 ავთენტიფიკაციისა და ავტორიზაციის პროცესში ენების გამოყენების საკითხები

აუცილებელია, ამსმპ-ს გააჩნდეს, სულ მცირე, ქართული ენის მხარდაჭერა.

უმჯობესია, მმპ-მა ავტორიზაციას დაქვემდებარებული ერთეულის რეგისტრაციისას მიუთითოს Accept-Language სათაური. ამ სათაურის გადმოცემისას **აუცილებელია** ამსმპ-მა უპირატესობა მიანიჭოს მმპ-ის მიერ განსაზღვრულ პრიორიტეტებს, მის მიერ მხარდაჭერილი ენების სიმრავლის ფარგლებში და ყველა შეტყობინება და ვიზუალური ფორმა გამოიტანოს ამ ენაზე.

თუ მმპ-ის მოთხოვნაში Accept-Language სათაური მითითებული არ არის, ამსმპ-ს შეუძლია ენა აირჩიოს საკუთარი შეხედულებისამებრ (მათ შორის **შესაძლოა** ამსმპ-მა ივარაუდოს მომხმარბლის ენა PSU-* სათაურებზე დაყდნობით).

7 გამოყენების შესაძლო სცენარები (ინფორმაციული)

აღნიშნულ თავში განსაზღვრული გამოყენების სცენარები არ წარმოადგენს სავალდებულო მოთხოვნას და ისინი მოყვანილია მხოლოდ დოკუმენტში მითითებული საკითხების უკეთ აღქმისათვის.

7.1 სმმ-ის მიერ პერსონალური ფინანსების მართვის ვებ სისტემაში საკუთარი საბანკო ანგარიშების მიბმა, პერსონალური კომპიუტერის საშუალებით

წინაპირობა: ნინო, რომელსაც გააჩნია კომერციულ ბანკში მიმდინარე ანგარიში, რეგისტრირდება პერსონალური ფინანსების მართვის სისტემაში (პფმ სისტემაში), რომელიც არის ლიცენზირებული მმპ. ნინო იყენებს ვებგვერდებს და მუშაობს პერსონალური კომპიუტერით, ბროუზერის გამოყენებით.

1. ნინო ჩამონათვალიდან ირჩევს სასურველ კომერციულ ბანკს და აჭერს ღილაკს „ანგარიშების სია ნაშთებით“
2. პფმ სისტემა (2)-ის შესაბამისად ქმნის თანხმობის მოთხოვნის დოკუმენტს (იხ (2)-ის 6.3.1.2 თავი) რომელშიც მითითებულია რომ საჭიროა ყველა გამოსადეგი ანგარიშების სიის მოთხოვნა, ნაშთებით ("availableAccountsWithBalance":"allAccounts") და არეგისტრირებს მას კომერციული ბანკის ღია ბანკინგის API-ში
   2.1. ვინაიდან ეს ნინოს პირველი ოპერაციაა, მას არ გააჩნია OAuth2 ტოკენი, ამიტომ პფმ სისტემა ღია ბანკინგის API-ში რეგისტრაციისას არ გადასცემს Authorization სათაურს
   2.2. ვინაიდან პფმ სისტემას ვებ ბროუზერით მუშაობს, ის არ გადასცემს ღია ბანკინგის API-ს TPP-Redirect-Preferred და TPP-Decoupled-Preferred სათაურებს
3. კომერციული ბანკის ღია ბანკინგის API არეგისტრირებს თანხმობის მოთხოვნას და იღებს გადაწყვეტილებას, რომ სმმ-მა უნდა გაიაროს მომხმარებლის ძლიერი ავთენტიფიკაცია OAuth2-ის გამოყენებით
4. კომერციული ბანკის ღია ბანკინგის სისტემა პფმ სისტემას თანხმობის მოთხოვნის რეგისტრირებულ იდენტიფიკატორს consentId ველით, ხოლო _links სექციაში აბრუნებს scaOAuth ჰიპერბმულს ბანკის OAuth2 სერვერის მეტაინფორმაციაზე
5. პფმ სისტემა იღებს OAuth2 სერვერის მეტაინფორმაციას და Authorization Code Flow-ს გამოყენებით (იხ. (12)) იწყებს მოთხოვნის ავტორიზაციის ინიცირებას

6. კომერციული ბანკის OAuth2 სერვერზე ხდება მომხმარებლის ძლიერი ავთენტიფიკაცია და ნინოს შეჰყავს იქ თავისი სახელი და პაროლი, ასევე ნინო თანხმობის აცხადებს პფმ სისტემისათვის ანგარიშების სიის გაზიარებაზე, რასაც ადასტურებს SMS კოდით. შედეგად, კომერციული ბანკის ნინოს ამისამართებს უკან, პფმ სისტემაში
   6.1. ნინოს ბროუზერი ბრუნდება პფმ სისტემაში
   6.2. პფმ სისტემას უბრუნდება ავტორიზაციის კოდი
   6.3. ავტორიზაციის კოდის საშუალებით პფმ სისტემა იღებს ავთენტიფიკაციის ტოკენს
7. პფმ სისტემა აანალიზებს ავთენტიფიკაციის ტოკენს, ამოწმებს მის სისწორეს და იყენებს ტოკენს კომერციული ბანკიდან ანგარიშების სიისა და ნაშთების გამოსათხოვად.

7.2 სმმ-ის მიერ კომერციული ბანკის ფრონტ-ოფისში თანხმობის გაცემა მეორე კომერციულ ბანკში არსებულ ანგარიშების სიაზე

წინაპირობა: ლევანი, რომელიც უცხო მოქალაქეა, თუმცა საქართველოში გააჩნია მუდმივი ბინადრობის მოწმობა და საქართველოს შესაბამისი ორგანოების მიერ მინიჭებული აქვს პირადი ნომერი 11122233344, მივიდა კომერციული ბანკის (ბანკი 1) სერვის-ცენტრში და გახდა კლიენტი. ლევანს სურს აიღოს სესხი ამ ბანკში. ვინაიდან მას ხელფასი სხვა კომერციულ ბანკში (ბანკი 2) ერიცხება, ბანკი 1-ის ოპერატორი სთავაზობს ლევანს, სესხის განაცხადს ასევე თან დაურთოს ინფორმაცია ბანკი 2-ში არსებული ანგარიშებისა და ბრუნვების თაობაზე. ვინაიდან ლევანს არ ახსოვს ანგარიშის ნომრები ბანკი 2-ში და არც მობილბანკი აქვს დარეგისტრირებული, ბანკი 1-ის ოპერატორი ირაკლი სთავაზობს მისი ანგარიშების სიის გამოთხოვას ბანკი 2-დან. ლევანი სიტყვიერად თანხმდება.

1. ირაკლი (ბანკი 1-ის ოპერატორი) ჩამონათვალიდან ირჩევს ბანკი 2-ს და იწყებს ანგარიშების სიის გამოთხოვის პროცესს
2. ბანკი 1-ის სისტემა (2)-ის შესაბამისად ქმნის თანხმობის მოთხოვნის დოკუმენტს (იხ (2)-ის 6.3.1.2 თავი) რომელშიც მითითებულია რომ საჭიროა ყველა გამოსადეგი ანგარიშების სიის ერთჯერადი მოთხოვნა, ნაშთების გარეშე ("availableAccounts":"allAccounts") და არეგისტრირებს მას ბანკი 2-ის ღია ბანკინგის API-ში
   2.1. ბანკი 1-ის სისტემა მხარს არ უჭერს ძველი ტოკენების ხელახლა გამოყენებას. ამიტომ იგი ბანკი 2-ის ღია ბანკინგის API-ში რეგისტრაციისას არ გადასცემს Authorization სათაურს
   2.2. ვინაიდან ბანკი 1-ის სისტემა წინამდებარე დოკუმენტის მიხედვითაა რეალიზებული, იგი ბანკი 2-ის ღია ბანკინგის API-ს გადასცემს PSU_ID=PNOGE-11122233344
   2.3. ვინაიდან ლევანი ფიზიკურადაა მისული სერვისცენტრში, ბანკი 1-ის სისტემა ბანკი 2-ის ღია ბანკინგის API-ს გადასცემს TPP-Decoupled-Preferred=true და TPP-Redirect-Preferred=false სათაურებს
3. ბანკი 2-ის ღია ბანკინგის API არეგისტრირებს მოთხოვნას და ვინაიდან მოთხოვნა დაბალრისკიანია, ნაცვლად განცალკევებული ავთენტიფიკაციისა, იწყებს ჩაშენებულ ავთენტიფიკაციას. გამომდინარე იქიდან, რომ ლევანს მხოლოდ SMS OTP აქვს გააქტიურებული:
   3.1. ბანკი 2 უბრუნებს ბანკი 1-ს ავტორიზაციის რესურსის მისამართს startAuthorisationWithTransactionAuthorisation საშუალებით. ავთენტიფიკაციის ტიპში მითითებულია SMS_OTP, ხოლო გამოწვევა (challenge) არის “aab437”

3.2. ბანკი 2 ლევანს მობილური ტელეფონის ნომერზე უგზავნის SMS შეტყობინებას „თქვენი SMS კოდია 37891, დაუსახელეთ იგი ბანკი 1-ს, თუ გამოწვევის კოდად გეტყვიან aab437-ს“

4. ირაკლი, რომელსაც ბანკი 1-ის სისტემამ ეკრანზე უჩვენა გამოწვევა “aab437”, ეუბნება ლევანს: თქვენ მიიღებდით SMS კოდს, გამოწვევის კოდია “aab437”, გთხოვთ დამისახელოთ SMS კოდი
5. ლევანი ირაკლის უსახელებს SMS კოდს 37891 , რომელიც ირაკლის შეჰყავს ბანკი 1-ის სისტემაში
6. ბანკი 1-ის სისტემა ბანკი 2-ის სისტემაში იძახებს ავტორიზაციას 3.1- ბიჯზე მიღებულ ბმულზე და გადასცემს SMS კოდს 37891.
7. ბანკი 2-ის სისტემა ამოწმებს რომ SMS კოდი 37891 სწორია და ავტორიზაცია წარმატებით სრულდება
8. ბანკი 1-ის სისტემა, რომელიც მუდმივად ამოწმებდა ბანკი 2-ში თანხმობის მოთხოვნის სტატუსს, იღებს ინფორმაციას რომ თანხმობა წარმატებით იქნა გაცემული
   8.1. ბანკი 1-ის სისტემა ითხოვს ბანკი 2-ისგან ავტორიზაციის ტოკენს Client Credentials Flow გამოყენებით, როგორც ეს განსაზღვრულია (12)-ით
   8.2. ბანკი 1-ის სისტემა ტოკენის გამოყენებით უკავშირდება ბანკი 2-ის სისტემას და ითხოვს ლევანის ანგარიშების სიას, ნაშთების გარეშე
   8.3. ლევანის ანგარიშების სია უბრუნდება ირაკლის
9. ვინაიდან ლევანს ბანკი 2-ში აქვს 10 ანგარიში, ის ვერ იხსენებს, რომელია მისი სახელფასო ანგარიში
10. ირაკლი სთავაზობს ლევანს, გაგზავნოს ბანკი 2-ში ზოგადი მოთხოვნა ანგარიშებსა და ამონაწერებზე და ლევანმა სურვილისამებრ გახსნას წვდომა. ლევანი სიტყვიერად თანხმდება
11. ირაკლი კვლავ იწყებს თანხმობის გამოთხოვნის პროცედურას. ამჯერად ბანკი 2-ში უნდა გაიგზავნოს ბანკის მიერ შეთავაზებული თანხმობის მოთხოვნა (2)-ის მიხედვით
12. ბანკი 1-ის სისტემა (2)-ის შესაბამისად ქმნის თანხმობის მოთხოვნის დოკუმენტს (იხ (2)-ის 6.3.1.2 თავი) რომელშიც მითითებულია რომ საჭიროა ყველა გამოსადეგი ანგარიშების სიის ერთჯერადი მოთხოვნა, ნაშთების გარეშე ("availableAccounts":"allAccounts") და არეგისტრირებს მას ბანკი 2-ის ღია ბანკინგის API-ში
    12.1. ბანკი 1-ის სიტემა კვლავ არ გადასცემს ბანკი 2-ის ღია ბანკინგის API-ში Authorization სათაურს
    12.2. ვინაიდან ბანკი 1-ის სისტემა წინამდებარე დოკუმენტის მიხედვითაა რეალიზებული, იგი ბანკი 2-ის ღია ბანკინგის API-ს გადასცემს PSU_ID=PNOGE-11122233344
    12.3. ვინაიდან ლევანი ფიზიკურადაა მისული სერვისცენტრში, ბანკი 1-ის სისტემა ბანკი 2-ის ღია ბანკინგის API-ს გადასცემს TPP-Decoupled-Preferred=true და TPP-Redirect-Preferred=false სათაურებს
13. ბანკი 2-ის სისტემა იღებს ბანკი 1-ის მოთხოვნას და ადგენს რა, რომ აღნიშნულ ოპერაციას ესაჭიროება მომხმარებლის ძლიერი ავთენტიფიკაცია. ამიტომ ბანკი 1 იწყებს განცალკევებული ტიპის ავთენტიფიკაციას
    13.1. ბანკი 1-ის სისტემას უბრუნდება ავტორიზაციის ტიპი DECOUPLED და შეტყობინება „სთხოვეთ მომხმარებელს, დაადასტუროს ოპერაცია ინტერნეტ ბანკით“
    13.2. ლევანი იღებს SMS შეტყობინებას „თქვენს ინტერნეტ ბანკში ახალი ოპერაციაა დასადასტურებლად. გთხოვთ შეხვიდეთ და დაადასტუროთ იგი“

14. ირაკლი სთხოვს ლევანს, რომ ის შევიდეს ბანკი 2-ის ინტერნეტ ბანკში დასადასტურებლად. ლევანი პასუხობს, რომ ვინაიდან მას არ აქვს სმარტფონი, ამჟამად მოკლებულია ინტერნეტ ბანკში შესვლის შესაძლებლობას
15. ირაკლი პასუხად ლევანს აცნობებს, რომ ეს პრობლემას არ წარმოადგენს, ლევანს შეუძლია დაადასტუროს ანგარიშების გამოთხოვნა სახლიდან და როცა ის ამას იზამს, სესხის განაცხადს შემდგომი მსვლელობა მიეცემა
16. ბანკი 1-ის სისტემა განუწყვეტლივ ამოწმებს ავტორიზაციის სტატუსს
17. ლევანი მიდის სახლში, ხსნის ინტერნეტ-ბანკს, ირჩევს სასურველ ანგარიშებს და აძლევს ბანკი 1-ს ანგარიშებზე, ტრანზაქციებსა და ნაშთებზე წვდომის უფლებას
18. ბანკი 1-ის სისტემა, რომელიც მუდმივად ამოწმებდა ბანკი 2-ში თანხმობის მოთხოვნის სტატუსს, იღებს ინფორმაციას, რომ თანხმობა წარმატებით იქნა გაცემული
    18.1. ბანკი 1-ის სისტემა ითხოვს ბანკი 2-ისგან ავტორიზაციის ტოკენს Client Credentials Flow გამოყენებით, როგორც ეს განსაზღვრულია (12)-ით
    18.2. ბანკი 1-ის სისტემა ტოკენის გამოყენებით უკავშირდება ბანკი 2-ის სისტემას და ითხოვს ლევანის ანგარიშების სიას, ნაშთების გარეშე
    18.3. ლევანის განაცხადის სტატუსი ავტომატურად იცვლება და განაცხადი იგზავნება კრედიტ ოფიცერთან.

8 დამატებითი გაფართოებები

ამ თავით მითითებულია სხვადასხვა გაფართოებები რომლებიც საჭიროა წინამდებარე დოკუმენტით განსაზღვრული ფუნქციების მხარდასაჭერად.

8.1 ჰიპერბმულების პრეფიქსების განსაზღვრა

თუ ამსმპ ან მმპ ჰიპერბმულების (_links) სექციაში აბრუნებს ამ დოკუმენტით განსაზღვრულ რაიმე ჰიპერბმულს (მაგ. psuPreOAuth), **აუცილებელია** მან ჰიპერბმულების (_links) სექციაში აღწეროს აღნიშნული პრეფიქსი. **უმჯობესია**, პრეფიქსი იყოს ofge.

აუცილებელია პრეფიქსი აღიწეროს შემდეგი ფორმატით:

```
"_links": {
  . . .
  "curies": [{
       "name": "ofge",
       "href": "https://openfinance.ge/relations/{rel}",
       "templated": true
  }]
  . . .
}
```

თუ ჰიპერბმულების სექციაში ამ დოკუმენტით განსაზღვრული არც ერთი ჰიპერბმული არ ბრუნდება, ამ აღწერის დაბრუნება **არარეკომენდებულია**.

8.2 ჰიპერბმული psuPreOAuth

ჰიპერბმული psuPreOAuth განკუთვნილია იმისათვის, რომ შესაძლებელი გახდეს (10)-ის მიხედვით ფორმატირებული OAuth2 სერვერის მეტაინფორმაციის დაბრუნება OAuth2 ტოკენის მისაღებად.

აუცილებელია ჰიპერბმული აღიწეროს 8.1-ის მიხედვით აღწერილი პრეფიქსის გამოყენებით (**აუცილებელია**, პრეფიქსის აღწერა მითითებული იყოს ჰიპერბმულების სექციაში), (16)-ის შესაბამისად.

ამსმპ-მა psuPreOAuth ჰიპერბმული **არავითარ შემთხვევაში** არ უნდა გამოიყენოს scaOAuth ჰიპერბმულის ჩასანაცვლებლად.

აღწერის მაგალითი:

```
"_links": {
  . . .
  "curies": [{
       "name": "ofge",
       "href": "https://openfinance.ge/relations/{rel}",
       "templated": true
  }]
  . . .
  "ofge:psuPreOAuth": {
       "href":  "https://www.testbank.com/oauth/.well-known/oauth-authorization-server-preauth"
  }
  . . .
}
```

9 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. **ETSI.** TS 119 495 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366. ETSI TS 119 495.

5. ***RFC 8705 (OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens).***

6. ***RFC 7591 (OAuth 2.0 Dynamic Client Registration Protocol).***

7. ***OpenID Connect Dynamic Client Registration 1.0.***

8. ***RFC 7592 (OAuth 2.0 Dynamic Client Registration Management Protocol).***

9. საქართველოს საბანკო ასოციაცია. ***JSON Web Signature (JWS) განხორციელების სახელმძღვანელო ღია ბანკინგისათვის.*** **ვერსია 0.5.**

10. ***RFC 8414 (OAuth 2.0 Authorization Server Metadata).***

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

12. ***RFC 6749 (The OAuth 2.0 Authorization Framework).***

13. ***Financial-grade API - Part 1: Read-Only API Security Profile.***

14. საქართველოს საბანკო ასოციაცია. ***კომერციულ ბანკებს შორის მომხმარებლის სარეგისტრაციო ინფორმაციის გაცვლის პროგრამული ინტერფეისის აღწერა.*** **ვერსია 0.1.**

15. ETSI. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. V1.1.1 (2016-02). ETSI EN 319 412-1.

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

17. ***RFC 4122 (A Universally Unique IDentifier (UUID) URN Namespace).***

18. ***RFC 5755 (An Internet Attribute Certificate Profile for Authorization).***

19. Signing HTTP Messages, draft-ietf-httpbis-message-signatures-00. [ინტერნეტი] https://tools.ietf.org/html/draft-ietf-httpbis-message-signatures-00.

20. Signing HTTP Messages, draft-cavage-http-signatures-12. [ინტერნეტი] https://tools.ietf.org/html/draft-cavage-http-signatures-12.

21. The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface. ***NextGenPSD2 XS2A Framework, Extended Services, Resource Status Notification Service.*** **2019 წლის 1 მარტი.**

22. —. NextGenPSD2 XS2A Framework, Extended Services, AIS for Single Cards. 2020 წლის 14 12.

23. —. NextGenPSD2 XS2A Framework, Extended Services,Multiple Consents Management. 1.0 2020 წლის 30 10.