NextGenPSD2 XS2A ჩარჩოს განხორციელების სახელმძღვანელო

1 სარჩევი

2 დოკუმენტის შესახებ

ეს დოკუმენტი წარმოადგენს NextGenPSD2 XS2A ჩარჩოს 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. დოკუმენტით დამატებით შეზღუდული საკითხების არაამომწურავი სია შემდეგია:

1) მომხმარებლის ავთენტიფიკაციის დასაშვები მეთოდები (მიუხედავად იმისა, რომ (1) და (2) იძლევა მომხმარებლის ძლიერი ავთენტიფიკაციის მეთოდების არჩევანის საშუალებას, წინამდებარე დოკუმენტი მოითხოვს მხოლოდ OAuth2 ავთენტიფიკაციას)
2) დოკუმენტების ფორმატი - წინამდებარე დოკუმენტი სავალდებულოდ აცხადებს JSON ფორმატის მხარდაჭერას

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 ᴍᴛᴀᴠʀᴜʟɪ (მთავრული) შრიფტით არიან გამოყენებული.

English	**ქართული**
MUST	უნდა
MUST NOT	არ უნდა
REQUIRED	სავალდებულოა
SHALL	აუცილებელია
SNALL 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
0.3	20.08.2020	საწყისი ვერსია.
0.4	01.09.2020	დაემატა ანგარიშის ინფორმაციის სერვისების დეტალური აღწერა. მომხმარებლის ძლიერი ავთენტიფიკაციის აღწერა გახდა უფრო დეტალური.
0.5	09.09.2020	აისახა საქართველოს ეროვნული ბანკისა და სხვადასხვა კომერციული ბანკების კომენტარები
0.6	16.09.2020	აისახა საქართველოს ეროვნული ბანკის დამატებითი კომენტარები - დაუშვებლად იქნა ცნობილი „გლობალური თანხმობა“ და დაზუსტდა სისტემის მონაწილეთათვის იდენტიფიკატორის მინიჭების წესი. ასევე დაემატა შეტყობინებებში თარიღის გადამოწმების წესი.

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:

PSDGE-NBG-სუფიქსი

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 პროვაიდერი 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

1. **აუცილებელია**, კავშირის არხი დამყარდეს TLS პროტოკოლის მიხედვით, TLS 1.2 ან უფრო მაღალის მიხედვით.
2. **აუცილებელია**, კავშირის დამყარებისას ორივე მხარემ ერთმანეთს წარუდგინოს X.509 სერტიფიკატები. ამ დოკუმენტის მიზნებისათვის **აუცილებელია**, თითოეულმა მხარემ იმოქმედოს ერთ-ერთი შემდგომი დასაშვები სცენარით:
   2.1. X.509 სერტიფიკატი ტექნიკურად სრულად აკმაყოფილებს (4)-ის მოთხოვნებს ვებსაიტის ავთენტიფიკაციის კვალიფიციური სერტიფიკატების მიმართ, შეიცავს 5.1 თავით განსაზღვრულ იდენტიფიკატორს და გაცემულია სერტიფიკატის ისეთი გამცემის მიერ, რომელიც აკმაყოფილებს საქართველოს კანონმდებლობით ღია ბანკინგისათვის საჭირო სერტიფიკატის გამცემისათვის წაყენებულ მოთხოვნებს.
   2.2. X.509 სერტიფიკატი ტექნიკურად არ აკმაყოფილებს (4)-ის მოთხოვნებს ან/და არ შეიცავს 5.1 თავით განსაზღვრულ იდენტიფიკატორს, თუმცა მისი გამოყენება შესაძლებელია TLS სესიებში კლიენტისა და სერვერის ავთენტიფიკაციისათვის და სერტიფიკატზე გაცემულია დამატებითი ინფორმაცია, რომელიც აკმაყოფილებს ამ დოკუმენტის 5.5 თავის 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 9 თავის ქვეთავებში).

5.3 OAuth2 კლიენტების დინამიკური რეგისტრაციის დამატებითი მოთხოვნები

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

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

შენიშვნა: ეს მოთხოვნა განპირობებულია, უპირველეს ყოვლისა, 5.5 თავის მოთხოვნების დაკმაყოფილების მიზნით, თუმცა დოკუმენტის შემდგომ ვერსიებში შეიძლება დაემატოს სხვა შესაძლებლობები, რათა მმპ-მა ამსმპ-ს მიაწოდოს დამატებითი ინფორმაცია.

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, სერტიფიკატის გამცემი შეთანხმებული უნდა იყოს საქართველოს ეროვნულ ბანკთან.

შენიშვნა: 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. შტამპის დატანის საკითხები განხილულია ამ დოკუმენტის 7.4 თავში.

აუცილებელია, ამსმპ-მა შეამოწმოს მმპ-ის მიერ განხორციელებული კვალიფიციური ელექტრონული შტამპი, როგორც კრიპტოგრაფიული თვალსაზრისით, ისე ამ დოკუმენტის 5.6 თავით მითითებული წესით.

თუ X.509 სერტიფიკატი ტექნიკურად არ აკმაყოფილებს (4)-ის მოთხოვნებს ან/და არ შეიცავს ამ დოკუმენტის 5.1 თავით განსაზღვრულ იდენტიფიკატორს, **აუცილებელია** მასზე გაცემული იყოს დამატებითი ინფორმაცია. დამატებითი ინფორმაციის გაცემისა და გამოყენების წესი რეგულირდება ამ დოკუმენტის 5.5 თავით.

5.5 არასტანდარტული სერტიფიკატების გამოყენება

// გადახვევაXS2A ჩარჩოდან

ამსმპ-სა და მმპ-ს უფლება აქვთ, ამ დოკუმენტთან თავსებადობის მიზნით გამოიყენონ ისეთი სერტიფიკატები, რომლებიც არ აკმაყოფილებენ (4)-ის მოთხოვნებს ან/და არ შეიცავენ ამ დოკუმენტის 5.1 თავით განსაზღვრულ იდენტიფიკატორს. ამ შემთხვევაში **აუცილებელია,** ამ თავით და მისი ქვეთავებით განსაზღვრული შესაბამისი მოთხოვნების დაკმაყოფილება.

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

ამსმპ-მა დინამიკური რეგისტრაციისა და ამ რეგისტრაციის მართვის შესაძლებლობა უნდა შესთავაზოს მმპ-ებს არააუცილებელი სახით (მაგ. მხოლოდ იმ შემთხვევისთვის, როდესაც მმპ-ს სურვილი აქვს გამოიყენოს არასტანდარტული სერტიფიკატი ან სურთ, დამატებითი ინფორმაცია: მაგ. ლოგოს მისამართი გაუგზავნონ ამსმპ-ს). კერძოდ, თუ მმპ იყენებს ვებსაიტების ავთენტიფიკაციის და კვალიფიციური ელექტრონული შტამპის ისეთ სერტიფიკატებს, რომლებიც აკმაყოფილებენ (4)-ის მოთხოვნებს და შეიცავენ 5.1 თავით განსაზღვრულ იდენტიფიკატორს, ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დაავალდებულოს მათი დინამიკური რეგისტრაცია და **აუცილებელია**, რომ ამსმპ-მა ყველა საჭირო ინფორმაცია ამოიღოს უშუალოდ სერტიფიკატებიდან.

აუცილებელია, დინამიკური რეგისტრაციისას ამსმპ-მა მმპ-ს მიანიჭოს იგივე იდენტიფიკატორი (client_id) რაც მკაცრად ემთხვევა მმპ-ს 5.1 თავით განსაზღვრულ იდენტიფიკატორს. **აუცილებელია**, მმპ-ს მიერ არასტანდარტული სერტიფიკატის გამოყენების შემთხვევაში ამსმპ-მა მისი იდენტიფიკატორი და სხვა ინფორმაცია ამოიკითხოს პროგრამული უზრუნველყოფის დასტურიდან (იხ. 5.5.2) და არ დაავალდებულოს მმპ-ს, წარმოადგინოს დამატებითი ინფორმაცია.

5.5.1 ავტორიზაციის სერტიფიკატები ამსმპ-ის და მმპ-ის ავთენტიფიკაციისათვის

თუ დაცული არხის დასამყარებლად ამსმპ-ის მიერ გამოყენებული X.509 სერტიფიკატი არ აკმაყოფილებს (4)-ის მოთხოვნებს ან/და არ შეიცავს 5.1 თავით განსაზღვრულ იდენტიფიკატორს, აუცილებელია მასზე გაცემული იყოს დამატებითი ავტორიზაციის (ატრიბუტის) სერტიფიკატი, (9) შესაბამისად. **აუცილებელია**, ატრიბუტის სერტიფიკატი აკმაყოფილებდეს შემდეგ მოთხოვნებს:

1) გაცემული იყოს საქართველოს ეროვნული ბანკის (ან შესაძლოა საქართველოს ეროვნული ბანკის მიერ განსაზღვრული სხვა ორგანიზაციის მიერ) და ხელმოწერილი იყოს ისეთი სერტიფიკატით, რომელსაც საქართველოს ეროვნული ბანკი უსასყიდლოდ მიაწვდის ყველა დაინტერესებულ მხარეს.
2) იყოს მოქმედი მისი გამოყენების მომენტისათვის.
3) მოქმედების ვადა არ აღემატებოდეს 3 საათს.
4) დაკავშირებული იყოს X.509 სერტიფიკატთან კრიპტოგრაფიული მეთოდით.
5) შეიცავდეს 5.1 თავით განსაზღვრულ იდენტიფიკატორს.
6) შეიცავდეს საგადახდო მომსახურების პროვაიდერის როლს (4)-ის 5.2.2 თავის შესაბამისად.

აუცილებელია, სერტიფიკატის კრიპტოგრაფიული კავშირი გულისხმობდეს ავტორიზაციის სერტიფიკატში Acinfo /Holder ჩანაწერის არსებობას, რომელშიც გამოყენებული იქნება baseCertificate ID და objectDisgestInfo. **აუცილებელია**, objectDigestInfo იყენებდეს SHA-256 an SHA-512 ჰეშირების მეთოდს.

აუცილებელია, ამსმპ-მა ეს სერტიფიკატი გამოაქვეყნოს შემდეგ მისამართზე:

https://სერვერის-საბაზისო-მისამართი-და-პორტი/.well-known/openbankinggeo/psd2.crt

სადაც „სერვერის-საბაზისო-მისამართი-და-პორტი“ აღნიშნავს იმ სერვერის საბაზისო მისამართს (hostname) და საჭიროებისამებრ პორტს, რომელთან კომუნიკაციაც დაცულია არასტანდარტული სერტიფიკატით.

თუ მმპ მის მიერ ამსმპ-სათვის წარდგენილ ჰიპერბმულებს (მაგ. ავთენტიფიკაციის შემდეგ მომხმარებლის გადასამისამართებელი ჰიპერბმული) იცავს არასტანდარტული სერტიფიკატით, **აუცილებელია**, მმპ-მა ამ თავში განსაზღვრული წესით დაიცვას ყველა აღნიშნული ჰიპერბმული.

5.5.2 პროგრამული უზრუნველყოფის დასტურის (Software Statement) გამოყენება კლიენტის მხარეს

თუ დაცული არხის დასამყარებლად მმპ-ის მიერ გამოყენებული X.509 სერტიფიკატი არ აკმაყოფილებს (4)-ის მოთხოვნებს ან/და არ შეიცავს 5.1 თავით განსაზღვრულ იდენტიფიკატორს, აუცილებელია მასზე გაცემული იყოს პროგრამული უზრუნველყოფის დასტური (Software Statement), საქართველოს ეროვნული ბანკის მიერ, რომელსაც მმპ წარუდგენს ამსმპ-ს დინამიკური რეგისტრაციისას.

აუცილებელია, დოკუმენტი ციფრულად იყოს ხელმოწერილი საქართველოს ეროვნული ბანკის (ან საქართველოს ეროვნული ბანკის მიერ განსაზღვრული სხვა ორგანიზაციის) მიერ ისეთი სერტიფიკატის გამოყენებით, რომელსაც საქართველოს ეროვნული ბანკი უსასყიდლოდ მიაწვდის ყველა დაინტერესებულ მხარეს. ციფრული ხელმოწერისა და შესაბამისი სერტიფიკატების გავრცელების დამატებითი საკითხები ამ დოკუმენტით არ რეგულირდება.

აუცილებელია, პროგრამული უზრუნველყოფის განაცხადი შეიცავდეს ყველა იმ ველს, რომელსაც შეცავს სურათი 1: პროგრამული უზრუნველყოფის დასტურის მაგალითი

```
{
        "software_id": "65d1f27c-4aea-4549-9c21-60e495a7a86f",
        "software_roles": [
                "PISP",
                "AISP"
        ]
        "iss": "https://nbg.gov.ge",
        "sub": "PSDGE-NBG-99999999",
        "nbf": 1300419270,
        "exp": 1300819380,
        "token_endpoint_auth_method": "tls_client_auth",
        "client_name": "Example Client",
        "client_name#ka": "საჩვენებელი კლიენტი",
        "client_uri": "https://client.example.net/",
    "jwks": {
        "keys": [
            {
                "x5t#S256": [
                        "ac58a191de026f4ab6fd3b04293238ee2b50fa5fcc775f4a8f73139f7941e9ae"
                ],
               "use": "tls"
            },
            {
                "x5t#S256": [
                        "2fe0ff296ac2c5620f016ea8285e13f8d0f0a62ddf15ec69d5eb931b966e6e9a"
                ],
               "use": "sig"
            }
        ]
    },
}
```


სურათი 1: პროგრამული უზრუნველყოფის დასტურის მაგალითი.

სადაც:

1) software_id ველის მნიშვნელობას განსაზღვრავს საქართველოს ეროვნული ბანკი, შეხედულებისამებრ.
2) software_roles არის PSD2-ით განსაზღვრული დასაშვები ავტორიზაციის როლები (ერთი ან რამდენიმე). დასაშვები მნიშვნელობებია PISP, AISP, ASPSP, PIISP.
3) nbf არის დასტურის ძალაში შესვლის დრო (წამების რაოდენობა 1970 წლის 1 იანვრიდან, UTC დროის სარტყელში).
4) exp არის დასტურის ვადის გასვლის დრო (წამების რაოდენობა 1970 წლის 1 იანვრიდან, UTC დროის სარტყელში).
5) client_name და client_name#ka შეიცავენ კლიენტის დასახელებას ინგლისურ და ქართულ ენებზე. **შესაძლოა** ეროვნულმა ბანკმა განსაზღვროს თარგმანი სხვა ენაზეც, თუმცა აღნიშნული თარგმანის მხარდაჭერა მმპ-ს ან ამსმპ-ს მხრიდან **არააუცილებელია**.
6) jwks შეცავს JSON Web Key Set სტრუქტურას - იმ სერტიფიკატების ჰეშ-კოდებს, რომლის გამოყენებაც შესაძლებელია TLS სესიის დასამყარებლად ან შტამპის დასადებად (შესაბამისად, tls და sig მნიშვნელობები “use” ატრიბუტში). **აუცილებელია,** აღნიშნულ მასივში თითოეულ შემთხვევაში იყოს ერთადერთი ჩანაწერი.

5.5.3 არასტანდარტული სერტიფიკატების გადაცემა მმპ-ის დინამიკური რეგისტრაციისას

აუცილებელია, მმპ-მ დინამიკური რეგისტრაციისას გადასცეს ამსმპ-ს საკუთარი TLS და შტამპის სერტიფიკატებიდან ის სერტიფიკატები, რომლებიც არასტანდარტულია. **აუცილებელია**, ამსმპ-მა გააკონტროლოს თითოეული სერტიფიკატის სისწორე (ჰეშების შედარების გზით) პროგრამული უზრუნველყოფის დასტურის დოკუმენტის (იხ. 5.5.2) მიმართ.

5.5.4 ამსმპ-ის ელექტრონული შტამპის არასტანდარტული სერტიფიკატი

იმ შემთხვევაში, როცა ამსმპ-ის ელექტრონული შტამპის სერტიფიკატი სტანდარტული არ არის, **აუცილებელია** ამსმპ-მა საკუთარ თითოეულ სერვერზე, რომელიც პასუხებს ელექტრონულ შტამპს ამ სერტიფიკატებით ადებს, გამოაქვეყნოს პროგრამული უზრუნველყოფის დასტურის დოკუმენტი მისამართზე.

https://სერვერის-საბაზისო-მისამართი-და-პორტი/.well-known/openbankinggeo/statement-იდენტიფიკატორი.json

1) „სერვერის-საბაზისო-მისამართი-და-პორტი“ აღნიშნავს იმ სერვერის საბაზისო მისამართს (hostname) და საჭიროებისამებრ პორტს.
2) იდენტიფიკატორი არის 5.1-ით განსაზღვრული ამსმპ-ის უნიკალური იდენტიფიკატორი.

აუცილებელია, მმპ-მა ჩამოტვირთოს აღნიშნული დოკუმენტი და გამოიყენოს იგი, რათა გადაამოწმოს ამსმპ-ის მიერ გამოყენებული ელექტრონული შტამპის სერტიფიკატის დასაშვებობა ამ დოკუმენტის მიზნებისათვის.

5.6 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**, კავშირის მონაწილე თითოეულ მხარეს (როგორც ამსმპ, ისე მმპ) გააჩნდეთ 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 საერთასორისო სტანდარტებითა და საუკეთესო პრაქტიკებითაა განსაზღვრული.

5.7 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.

აუცილებელია, ამსმპ-მა შეამოწმოს მმპ-ს მიერ გადაცემული ყველა ჰიპერბმული და დარწმუნდეს რომ ის ნამდვილად ამ მმპ-ს ეკონტაქტება.

6 მომხმარებლის ავთენტიფიკაცია და ავტორიზაცია

ამ დოკუმენტის მიზნებისათვის, მომხმარებლის ავთენტიფიკაცია შეიძლება მოხდეს ორგვარად:

- მომხმარებლის ზოგადი ავთენტიფიკაცია მმპ-სა და ამსმპ-ს შორის არხში.
- მომხმარებლის ძლიერი ავთენტიფიკაცია.

აუცილებელია, ავთენტიფიკაციისა და ავტორიზაციისათვის გამოყენებული იქნას OAuth2 პროტოკოლი, რომლის რეალიზაცია სრულად შეესაბამება (10) მოთხოვნებს.

6.1 მომხმარებლის ზოგადი ავთენტიფიკაცია მმპ-სა და ამსმპ-ს შორის არხში

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. 9.1 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.

განსხვავებით დანარჩენი სერვისებისგან, თანხმობის გაცემის ტრანზაქციის (იხ. 9.1) ფარგლებში **აუცილებელია** მმპ-მ გამოიყენოს ერთ-ერთი შემდეგი მიდგომა:

1. არ გაუგზავნოს ამსმპ-ს OAuth2 ტოკენი თანხმობის მოთხოვნისას.
2. ამსმპ-ს გადასცეს თავად ამ ამსმპ-ს მიერ სხვა ტრანზაქციის (მაგ. სხვა თანხმობის გამოხატვის ტრანზაქციის) პროცესში გაცემული ტოკენი
3. ამსმპ-ს გადასცეს სხვა ისეთი ავტორიზაციის სერვერის მიერ გაცემული OAuth2 ტოკენი, რომლის გამცემიც წინასწარ აქვს შეთანხმებული ამსმპ-სთან.

აუცილებელია, ამსმპ-მა მხარი დაუჭიროს შემთხვევას, როდესაც მმპ არ წარუდგენს მას ტოკენს თანხმობის გაცემის ტრანზაქციისას. ამ შემთხვევაში ამსმპ-მა უნდა ჩათვალოს რომ მოთხოვნა შეეხება არაიდენტიფიცირებულ სმმ-ს და მოახდინოს მისი ავთენტიფიკაცია OAuth2 პროტოკოლის გამოყენებით და მიიღოს სმმ-ის დასტური აღნიშნულზე.

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 (იხ. ზემოთ).

<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 გაცემისას შემთხვევაში და ცნობილი იყო ამის შესახებ ამსმპ-სათვის თუ არა. თუმცა შესაძლოა ამსმპ-მა გარდაქმნას აღნიშნული ტოკენი მომხმარებლის ძლიერი ავთენტიფიკაციის ტოკენად 6.3-ით განსაზღვრული წესით.

6.2 მომხმარებლის ძლიერი ავთენტიფიკაცია

ამ დოკუმენტის მიზნებისათვის **აუცილებელია,** ამსმპ იყენებდეს OAuth2 პროტოკოლს გადამისამართებით. (2)-ში განსაზღვრული ძლიერი ავთენტიფიკაციის დანარჩენი მეთოდები (მაგ. „embedded”) მხარდაჭერილი არ არის. შესაბამისად, ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მოსთხოვოს მმპ-ს OAuth2-ისგან განსხვავებული პროტოკოლით მომხმარებლის ძლიერი ავთენტიფიკაციის პროცესის ინიცირება. **აუცილებელია**, OAuth2 პროტოკოლის რეალიზება სრულ თანხვედრაში იყოს როგორც (2)-ის მე-13 თავთან, ისე (10) მოთხოვნებთან.

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა მოითხოვოს მმპ-საგან ტოკენის მიღების დადასტურება, მან არ უნდა დააბრუნოს confirmation ტიპის ჰიპერლინკი _links სექციაში (მაგ. (2) -ის 5.3.1 და 6.3.1.1 თავის შესაბამისად). ამ მოთხოვნის მიუხედავად, **უმჯობესია** მმპ-ებს ჰქონდეთ აღნიშნული შესაძლებლობის მხარდაჭერა, (2)-სთან სრული თავსებადობის მიზნით.

6.3 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 გავლას, 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. 9.1) 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 (2)-ის შესაბამისად.
4) ავტორიზაციის რესურსი, რომელსაც ამსმპ უბრუნებს სმმ-ს (იხ. 10.1) 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.

7 API სტრუქტურა

აუცილებელია, მონაცემების მიმოცვლა სრულ თავსებადობაში იყოს (2)-თან, მათ შორის მისი 4.4 თავით განსაზღვრულ მოთხოვნებთან.

იმ შემთხვევებში, როდესაც (2)-დან კეთდება ბმა გაფართოებულ სერვისებზე, მაგ. (11)-ით აღწერილზე (მაგ.TPP-Notification-URI პარამეტრების გამოყენება) რეალიზაციისას უნდა მოხდეს იმის გათვალისწინება, რომ დოკუმენტის ეს ვერსია არ არეგულირებს მსგავს შესაძლებლობებს. აღნიშნული მიმართებები დარეგულირდება ამ დოკუმენტის შემდგომ ვერსიებში და ამან

შესაძლოა საფრთხე შეუქმნას უკვე შექმნილი ინტერფეისის თავსებადობას ამ დოკუმენტის შემდგომ ვერსიებთან.

ეს დოკუმენტი აწესებს დამატებით მოთხოვნებს, რომლებიც არ ეწინააღმდეგებიან აღნიშნულ სპეციფიკაციას, და შეზღუდვებს აწესებენ ისეთ საკითხებზე, სადაც (2) ითვალისწინებს მეტ თავისუფლებას ამსმპ-სათვის.

7.1 API რესურსების მისამართები

აუცილებელია, API რესურსების მისამართებს ჰქონდეთ შემდეგი სახე:

https://{provider}/{version}/v1/{service}{?query-parameters}

ველებს აქვთ შემდეგი მნიშვნელობა:

- {provider} სერვერის მისამართი (host) და გზა (path). **შესაძლოა** მისამართი ან/და გზა შეიცავდეს API ვერსიის იდენტიფიკატორს, ამსმპ-ს შეხედულებისამებრ.
- {version} ამ დოკუმენტის ვერსია. დოკუმენტის ვერსია მითითებულია პარაგრაფში 3
- v1 - ვერსია (2)-ის მიხედვით.
- {service} და {query-parameters} იხილეთ (2)

აღნიშნულ ფორმატს (2)-სგან განასხვავებს მხოლოდ ველი {version} რომელიც დამატებით ბმას აკეთებს ამ დოკუმენტის ვერსიაზე. **შესაძლოა** ამსმპ-ს ერთდროულად ჰქონდეს ამ დოკუმენტის სხვადასხვა ვერსიის შესაბამისი სერვისების მხარდაჭერა.

აუცილებელია, ამსმპ-მ ნათლად გამოჰყოს ერთმანეთისაგან სერვისის საწარმოო (production) და დანარჩენი (სატესტო, სადემონსტრაციო და ა.შ.) ვერსიები. **აუცილებელია**, გამოყოფა მოხდეს {provider} ველის მეშვეობით.

7.2 API მოთხოვნისა და პასუხის ფორმატი

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია**, მხარდაჭერილი იყოს მოთხოვნისა და პასუხის JSON ფორმატი. შესაძლოა, ამავე ინტერფეისის ფარგლებში ამსმპ-მ მხარი დაუჭიროს (2)-ით განსაზღვრულ სხვა ფორმატებს (მაგ. XML) და ამ შემთხვევაში **აუცილებელია,** აღნიშნული ცხადად იყოს მითითებული ამსმპ-ის ინტერფეისის დოკუმენტაციაში.

7.3 HTTP პასუხის კოდები და დამატებითი ინფორმაცია პასუხის შესახებ

აუცილებელია, ამსმპ-მა დააბრუნოს არამარტო HTTP პასუხის კოდები (აუცილებელია, აღნიშნული კოდები სრულ შესაბამისობაში იყოს (2)-თან, კერძოდ მის 4.12 თავის მოთხოვნებთან), ასევე გაფართოებული ინფორმაცია სტატუსის შესახებ, (2)-ის 4.13.2 თავის შესაბამისად.

7.4 ელექტრონული შტამპის განხორციელება მოთხოვნასა და პასუხზე

// გადახვევა XS2A ჩარჩოდან

აუცილებელია, HTTP მოთხოვნებზე, რომლებიც შეეხება API-ს გამოძახებას, მოთხოვნის ინიციატორმა კვალიფიციური ელექტრონული შტამპი დაიტანოს (2)-ის 4.2 თავის (Signing Messages at Application Layer) მსგავსად.

აუცილებელია, ჰეშ-კოდის გამოთვლისას და ხელმოწერის შექმნისას როგორც ამსმპ-მა ისე მმპ-მა გამოიყენოს მხოლოდ ის ალგორითმები, რაც აღნიშნული სტანდარტითაა დაშვებული.

აუცილებელია, მოთხოვნის ტანზე (request body) და პასუხის ტანზე (response body) ჰეშ-კოდის გამოთვლა მოხდეს (2)-ის 12.1 თავით განსაზღვრული წესით და **აუცილებელია**, შედეგი დაემატოს სათაურში სახელად „digest", ამავე თავით განსაზღვრული ფორმით.

ამ დოკუმენტთან თავსებადობის მიზნებისათვის **აუცილებელია** HTTP პროტოკოლზე ხელმოწერის ფორმატის ახალი ვერსიების გამოყენება. კერძოდ, **აუცილებელია** გამოყენებული იქნას (12) და მხოლოდ საჭიროებისამებრ (13).

წინამდებარე დოკუმენტთან თავსებადობის მიზნებისათვის, date ველის შეყვანა ხელმოსაწერი ატრიბუტების სიაში **აუცილებელია** (დასახელებულ სტანდარტებში წერია SHOULD და არა SHALL) როგორც მოთხოვნის, ისე პასუხის შემთხვევაში.

აუცილებელია, მოთხოვნაზე შტამპის დადებისას შტამპმა დაფაროს შემდეგი სათაურები:

1) Date
2) Content-Type (თუ ხდება მონაცემების გადაცემა)
3) Content-Length (თუ ხდება მონაცემების გადაცემა)
4) X-Request-Id
5) ყველა სათაური „PSU" პრეფიქსით, რაც (2)-ის შესაბამისად ეგზავნება ამსმპ-ს
6) სპეციალური (request-target) ფსევდო-სათაური, გამოთვლილი (12) -ის შესაბამისად
7) Digest

აუცილებელია, პასუხზე შტამპზე პასუხის დადებისას შტამპმა დაფაროს შემდეგი სათაურები:

1) Date
2) Content-Type (თუ ხდება მონაცემების გადაცემა)
3) Content-Length (თუ ხდება მონაცემების გადაცემა)
4) X-Request-Id
5) Digest

აუცილებელია, მმპ-მა საკუთარი სერტიფიკატი base64-ში კოდირებული ფორმით ჩაწეროს TPP-Signature-Certificate სათაურში, ხოლო ამსმპ-მა - ASPSP-Signature-Certificate სათაურში.

აუცილებელია, HTTP მოთხოვნაში და პასუხებში პასუხზე პასუხის გამცემმა ასევე დაიტანოს ელექტრონული შტამპი და ამ მიზნით შექმნას (12)-ის შესაბამისი Signature დასახელების მქონე სათაურში (მოთხოვნაში ან პასუხში). აღნიშნულ სათაურში აუცილებელია გამოყენებული იქნას შემდეგი მნიშვნელობები:

1) მოთხოვნაში keyId **აუცილებელია** დაგენერირდეს (2)-ის 12.2 თავის მოთხოვნათა შესაბამისად (ამსმპ-ს შემთხვევაშიც იგივე მოთხოვნა ვრცელდება)
2) Signature სათაურში **აუცილებელია** შედიოდეს keyId, Algorithm, Headers და Signature ველები

3) **აუცილებელია**, ხელმოწერა (Signature ველი სათაურში Signature) დათვლილი იყოს (12)-ის შესაბამისად

ელექტრონულ შტამპზე რომელიმე მხარემ **არავითარ შემთხვევაში** არ უნდა გამოიყენოს დროის კვალიფიციური აღნიშვნა, ვინაიდან ეს, ერთი მხრივ, ზრდის შეტყობინების ხელმომწერის დამოკიდებულებას გარე სერვისებზე და, მეორე მხრივ, შეტყობინების მიმღებს აიძულებს გადაამოწმოს დროის კვალიფიციური აღნიშვნის სისწორე.

აუცილებელია, სისტემის ყველა მონაწილე (ამსმპ და მმპ) ახდენდეს დროის სინქრონიზაციას საერთაშორისო კოორდინირებულ დროსთან (UTC).

აუცილებელია, სისტემის ყველა მონაწილემ (ამსმპ-მა და მმპ-მა) შეამოწმოს მიღებულ შეტყობინებებში არსებული თარიღის ველის მნიშვნელობა შეტყობინების დამუშავებამდე და შეადაროს საკუთარ სისტემაში დაფიქსირებულ დროს. იმ შემთხვევაში, თუ მიღებულ შეტყობინებაში დაფიქსირებული დრო უფრო მეტია, ვიდრე თავად მონაწილის სისტემაში დაფიქსირებული დრო და აღნიშნული სხვაობა 2 (ორ) წამს აღემატება, მოქმედებს შემდეგი წესი, შეტყობინება **არავითარ შემთხვევაში** არ უნდა დამუშავდეს.

8 გადახდის ინიცირების მომსახურება

გადახდის ინიცირების მომსახურება ამ დოკუმენტის ამ ვერსიით არ რეგულირდება და იგი განსაზღვრული იქნება შემდეგ ვერსიებში

9 ანგარიშის ინფორმაციის მომსახურება

ანგარიშის ინფორმაციის მომსახურებაში (2) მიჯნავს საბარათე და დანარჩენი ანგარიშების საინფორმაციო რესურსებს. ამ დოკუმენტთან თავსებადობის მიზნით **აუცილებელია**, ანგარიშების სერვისებმა (იხ. (2), თავი 4.11.2) დააბრუნონ იმ ანგარიშების ინფორმაციაც, რომელზედაც მიბმულია ერთი ან რამდენიმე პლასტიკური ბარათი (სადებეტო ან საკრედიტო). საბარათე ანგარიშების ინფორმაციის დაბრუნების წესი რეგულირდება ამ დოკუმენტის 9.3 თავით.

ამ დოკუმენტით ერთმანეთისგან განსხვავდება ღია ბანკინგისთვის გამოსადეგი (available) და ხელმისაწვდომი (accessible) ანგარიშები. კერძოდ:

- გამოსადეგი ანგარიში არის ანგარიში, რომლის გამოყენებაც შესაძლებელია XS2A ინტერფეისით საშუალებით, საქართველოს კანონმდებლობის შესაბამისად;
- ხელმისაწვდომი ანგარიში არის ისეთი გამოსადეგი ანგარიში, რომლის გამოყენებაზეც რაიმე სახის თანხმობაა გაცემული რაიმე სახის ინფორმაციის გაცემაზე და ეს თანხმობა აქტიურია.

9.1 მომხმარებლის თანხმობა ანგარიშების ინფორმაციის გაზიარებაზე

ამ დოკუმენტთან თავსებადია (2)-ის მე-6 თავით განსაზღვრული თანხმობის გამოხატვის მხოლოდ ორი სცენარი: დეტალური თანხმობა და ბანკის მიერ შეთავაზებული თანხმობა. სცენარების აღწერა მოცემულია ქვეთავებში. გლობალური თანხმობა (რომელიც ინფორმაციული

მიზნებისათვის აღწერილია 9.1.2 თავში) ამ დოკუმენტთან თავსებადი არ არის და **არავითარ შემთხვევაში** არ უნდა იქნას გამოყენებული.

მანამ, სანამ მისწვდება კონკრეტულ ანგარიშს/ანგარიშებს, **აუცილებელია** მმპ-მა შექმნას თანხმობის დოკუმენტი, რომელშიც აღწერს კონკრეტულად რა საკითხზე ითხოვს თანხმობას სმმ-ისგან (თანხმობის დოკუმენტების ზოგიერთი ფორმა მოცემულია ამ თავის შემდგომი ქვეთავებით) და გადასცეს იგი სარეგისტრაციოდ ამსმპ-ს 9.1.7 თავით განსაზღვრული წესით. შემდგომი მოქმედებები აღწერილია ხსენებულ თავში.

თანხმობის მიღების პროცესი შემდეგია:

1. მმპ-მა ქმნის თანხმობის რეგისტრაციისათვის საჭირო თანხმობის ობიექტი (იხ. ქვემოთ), როგორც ეს აღწერილია წინამდებარე თავის ქვეთავებში, ასევე (2)-ის 14.16 თავში და მე-6 თავში.
2. მმპ იძახებს ამსმპ-ის თანხმობის რეგისტრაციის სერვისს და აწვდის მას თანხმობის ობიექტს. გადაცემის წესი აღწერილია (2)-ის 6.3.1.1 თავში და ასევე წინამდებარე თავის ქვეთავებში.
3. ამსმპ არეგისტრირებს თავისთან თანხმობის ობიექტს, ანიჭებს მას სარეგისტრაციო იდენტიფიკატორს და იღებს ერთ-ერთ შემდეგ გადაწყვეტილებას ავტომატურ რეჟიმში:
   3.1. ავტომატური უარი.
   3.2. ავტომატური თანხმობა.
   3.3. მომხმარებლის ძლიერი ავთენტიფიკაციისა და თანხმობის გამოხატვის მოთხოვნა.
4. თუ ამსმპ-ის გადაწყვეტილება ავტომატური თანხმობაა, მმპ-ს შეუძლია თანხმობის ობიექტის იდენტიფიკატორი (რომელსაც ამსმპ-სგან მიიღებს) გამოიყენოს ანგარიშის ინფორმაციის გაზიარების სერვისებში (იხ. ამ თავის შესაბამისი ქვეთავები).
5. თუ ამსმპ-ის გადაწყვეტილება მომხმარებლის ძლიერი ავთენტიფიკაციის და თანხმობის გამოხატვის მოთხოვნაა, იგი უბრუნებს მმპს-ს პასუხს.

9.1.1 დეტალური თანხმობის მოთხოვნის დოკუმენტი

აღნიშნული სცენარი ითვალისწინებს, რომ სმმ-ს აქვს შესაძლებლობა, მიაწოდოს ანგარიშის ნომრები მმპს-ს რაიმე მიზეზიდან გამომდინარე (მაგ. მმპ-მა მიიღო ანგარიშის ნომრები წინა ჯერზე თანხმობის გამოხატვით, სმმ-მა შეიყვანა ისინი ხელით, დაასკანერა ანგარიშის ნომრის შემცველი QR კოდი ინტერნეტ-ბანკში და ა.შ.).

სმმ-ის მონაწილეობით მმპ ქმნის თანხმობის დოკუმენტს, რომელსაც შეიძლება ჰქონდეს, მაგალითად, ქვემოთ მოცემული სახე:

```
{
   "access":{
      "accounts":[
         {
            "iban":"GE00UT0000000101904917"
```

```
            },
            {
               "iban":"GE00UT0000000101904918"
            }
         ],
         "balances":[
            {
               "iban":"GE00UT0000000101904919"
            }
         ],
         "transactions":[
            {
               "iban":"GE00UT0000000101904920"
            }
         ]
      },
      "frequencyPerDay":5,
      "recurringIndicator":true,
      "validUntil":"2020-09-10"
}
```


აღნიშნული დოკუმენტის აწყობა მთლიანად მმპ-ის ფუნქციებშია. ამის შემდეგ მმპ იძახებს ამსმპ-ის /v1/consents ფუნქციას (იხ. (2) თავი 6.3.1.1) და გადასცემს აღნიშნულ ობიექტს. ამსმპ არეგისტრირებს აღნიშნულ მოთხოვნას და აბრუნებს სხვადასხვა მონაცემებს, მათ შორის consentId, რომელიც საჭიროა ავტორიზაციის რესურსების შესაქმნელად (იხ. 10.1), შემდგომი ძლიერი ავთენტიფიკაციის მიზნით.

როდესაც ამგვარ თანხმობას ესაჭიროება მომხმარებლის ძლიერი ავთენტიფიკაცია, **აუცილებელია**, იგი მოხდეს ამსმპ-ს მხარეს.

აუცილებელია, ამსმპ-მა მხოლოდ უჩვენოს სმმ-ს თანხმობის ობიექტი ვიზუალურად და არ მისცეს მისი ცვლილების შესაძლებლობა. თუ სმმ არ ეთანხმება ამგვარი უფლების მიცემას, მან ცხადად უნდა უარჰყოს აღნიშნული უფლების გაცემა.

აუცილებელია, ამსმპ-მა შეინახოს სმმ-ის მიერ თანხმობის გამოხატვის ფაქტი საკუთარ სისტემაში.

9.1.2 გლობალური თანხმობის მოთხოვნის დოკუმენტი

აღნიშნული მსგავსია „დეტალური თანხმობისა“, უბრალოდ სმმ აძლევს მმპ-ს თანხმობას გლობალურად, ყველა ანგარიშის ყველანაირ ინფორმაციაზე, მმპ თავის მხარეს ქმნის თანხმობის დოკუმენტს და აღნიშნული გადაეცემა ამსმპ-ს რეგისტრაციისათვის. შემდეგ პროცესს წარმართავს ამსმპ. კერძოდ, იგი მომხმარებელს გაატარებს ძლიერ ავთენტიფიკაციას, ხოლო შემდგომ მოსთხოვს, გამოხატოს საერთო თანხმობა მმპ-სათვის ინფორმაციის გადაცემაზე. მაგალითად:

```
{
    "access":{
        "allPsd2":"allAccounts"
    },
    "frequencyPerDay":3,
    "recurringIndicator":true,
    "validUntil":"2021-11-10"
}
```

აღნიშნული თანხმობის გამოხატვის ტექნიკური აღწერა მითითებულია (2)-ის 6.3.1.2 თავის „Consent Request for Access to all Accounts for all PSD2 defined AIS – Global Consent“ პარაგრაფში. ასევე არსებობს `"allPsd2":"allAccountsWithOwnerName"` ვარიანტი, რაც გულისხმობს იმას, რომ თანხმობა გაცემულია ანგარიშის მფლობელის სახელის დაბრუნებაზეც.

ამ დოკუმენტის მიზნებისათვის მმპ-მა **არავითარ შემთხვევაში** არ უნდა გაგზავნოს გლობალური თანხმობის მოთხოვნის დოკუმენტი და იმ შემთხვევაში, თუ ამსმპ მიიღებს მსგავს დოკუმენტს რომელიმე მმპ-სგან, **აუცილებელია**, ამსმპ-მა დააბრუნოს შეცდომა.

9.1.3 ამსმპ-ში გამოხატული თანხმობის ინიცირების დოკუმენტი

აღნიშნული სცენარის შემთხვევაში სმმ-ისაგან თანხმობის მიღების პროცესი სრულად ხდება სმმ-სა და ამსმპ-ს შორის.

სცენარის ინიცირებას, როგორც ყველა სხვა შემთხვევაში, აქაც იწყებს მმპ, თუმცა განსხვავებით დეტალური თანხმობისაგან (იხ. 9.1.1 თავი), იმ JSON დოკუმენტში რომელიც ამსმპ-ს გადაეცემა, "access" ატრიბუტში გადაეცემა "accounts", "balances" ან/და "transactions" ქვე-ატრიბუტები , ისე, რომ გადაცემულთაგან ყველა შეიცავს ცარიელ მასივს(„[]“) რაც ამსმპ-სათვის იმის მანიშნებელია, რომ მმპ-მა არ იცის, კონკრეტულად რომელ ანგარიშებზე საჭიროებს იგი თანხმობას სმმ-ისგან.

მაგალითად:

```
{
    "access":{
        "accounts":[
        ],
```

```
        "balances":[

        ],

        "transactions":[

        ]

    },

    "frequencyPerDay":12,

    "recurringIndicator":true,

    "validUntil":"2020-10-15"

}
```

აუცილებელია, ამსმპ-მა მოითხოვოს მომხმარებლის ძლიერი ავთენტიფიკაცია.

აუცილებელია, ამსმპ-მა მოსთხოვოს სმმ-ს დეტალური ან საერთო თანხმობა იმ მონაცემებზე, რომლებისთვისაც მმპ-მა გადმოსცა ცარიელი მასივი. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა გახადოს საერთო თანხმობა აუცილებელი - მან საშუალება უნდა მისცეს სმმ-ს, არ გასცეს თანხმობა რომელიმე ანგარიშზე.

აუცილებელია, ამსმპ-მა შეინახოს სმმ-ის მიერ თანხმობის გამოხატვის ფაქტი საკუთარ სისტემაში.

იმ შემთხვევაში, თუ "accounts", "balances" ან/და "transactions" ქვე-ატრიბუტებიდან რომელიმე შეიცავს არა ცარიელ მასივს, არამედ კონკრეტულ სიას (იხ. 9.1.1), **უმჯობესია** ამსმპ-მა არ მისცეს საშუალება სმმ-ს, თანხმობის გამოხატვის პროცესში შეცვალოს შესაბამისი მონაცემები.

მმპ-ს შეუძლია შეიტყოს თანხმობის შესახებ მოგვიანებით, შესაბამისი სერვისული გამოძახებით. აღნიშნული თანხმობის გამოხატვის ტექნიკური აღწერა მითითებულია (2)-ის 6.3.1.2 თავის „Consent Request without Indication of Accounts – Bank Offered Consent“ პარაგრაფში.

9.1.4 ყველა გამოსადეგ ანგარიშის ინფორმაციის მოთხოვნაზე თანხმობის დოკუმენტი

აღნიშნული წარმოადგენს სპეციალურ სცენარს, როდესაც მმპ-ს ესაჭიროება მიიღოს წვდომა სმმ-ის ყველა გამოსადეგი ანგარიშის სიაზე (ბალანსებისა და ტრანზაქციების გარდა). აღნიშნული სცენარის მხარდაჭერა **აუცილებელია**.

```
{

    "access":{

        "availableAccounts":"allAccounts"

    },

    "recurringIndicator":false,

    "validUntil":"2017-08-06",

    "frequencyPerDay":"1"

}
```

შესაძლოა, დამატებით ამსმპ-მა მხარი დაუჭიროს ამ სცენარის შემდეგ მოდიფიკაციებს:

- `"availableAccounts":"allAccountsWithOwnerName"` – ყველა გამოსადეგი ანგარიში და მფლობელის სახელი თითოეული მათგანისათვის. ეს საკითხი დამატებით რეგულირდება **Error! Reference source not found.** თავით.
- `"availableAccountsWithBalance":"allAccounts"` – ყველა გამოსადეგი ანგარიში და მათი ბალანსები.
- `"availableAccountsWithBalance":"allAccountsWithOwnerName"` – ყველა გამოსადეგი ანგარიში, მათი ბალანსები და მფლობელთა სახელები. ეს საკითხი დამატებით რეგულირდება **Error! Reference source not found.** თავით.

აუცილებელია, მხარდაჭერილი იყოს availableAccounts მოთხოვნა, მნიშვნელობით allAccounts.

კომბინირებული სერვისები წინამდებარე დოკუმენტის ამ ვერსიის მიზნებისათვის, **აუცილებელია**, combinedServiceIndicator ველში მიეთითოს მნიშვნელობა false, ვინაიდან გადახდის ინიცირების მომსახურება ამ ვერსიაში განსაზღვრული არ არის.

9.1.5 დამატებითი ინფორმაციის გაზიარების მოთხოვნის წესი

ინფორმაციის მოთხოვნაზე თანხმობის დოკუმენტში (2) მხარს უჭერს access ატრიბუტში ქვე-ატრიბუტს additionalInformation. აღნიშნული ატრიბუტის გამოყენების საკითხი, ასევე მისი ზოგიერთი ალტერნატივის გამოყენება განისაზღვრება ამ თავის ქვეთავებში მითითებული წესით.

უმჯობესია, ანგარიშის მფლობელის სახელის გამოთხოვაზე არსებობდეს ცხადად გამოხატული თანხმობა. მაგალითად, თუ ამსმპ მიიღებს თანხმობას გამოსადეგი ანგარიშების სიაზე `"availableAccounts":"allAccounts"` ფორმით (როგორც ეს 9.1.4 თავით არის განსაზღვრული), მან არ დაუბრუნოს მპპ-ს ანგარიშის მფლობელის ინფორმაცია.

9.1.5.1 წინასწარ ცხადად განსაზღვრული ანგარიშის მფლობელის სახელი

აუცილებელია, მხარდაჭერილი იყოს ანგარიშის მფლობელის სახელის მოთხოვნაის შესაძლებლობა (ownerName ველის მოთხოვნის შესაძლებლობა), როგორც ეს (2)-ის 14.17 თავითაა განსაზღვრული.

9.1.5.2 ანგარიშის მფლობელის სახელი გამოსადეგი ანგარიშების მოთხონისას

უმჯობესია, მხარდაჭერილი იყოს WithOwnerName სუფიქსის მქონე (მაგ. allAccountsWithOwnerName) ვარიანტები availableAccounts, availableAccountWithBalance და allPsd2 ატრიბუტებში, (2)-სთან მეტი თავსებადობის და მომხმარებლის მეტი კომფორტის მიზნით. **უმჯობესია,** ownerName ველის გამოთხოვაზე არსებობდეს ცხადად გამოხატული თანხმობა და ამგვარი თანხმობის არარსებობის შემთხვევაში ამსმპ-მა არ დაუბრუნოს მპპ-ს ეს ინფორმაცია.

9.1.5.3 სანდო ბენეფიციარების სია

დოკუმენტის ამ ვერსიასთან თავსებადობის მიზნებისათვის ამსმპ-მა **მხარი არავითარ შემთხვევაში** არ უნდა დაუჭიროს სანდო ბენეფიციარების სიის გაზიარებას (2)-ის 14.17 თავით განსაზღვრული წესით (ატრიბუტის სახელი „trustedBeneficiaries“) და მმპ-ის მხრიდან აღნიშნულზე თანხმობის მოთხოვნაზე დააბრუნოს შესაბამისი შეცდომის კოდი.

9.1.6 მულტისავალუტო ანგარიშებზე გამოხატული თანხმობა

მულტისავალუტო ანგარიშზე, მიუხედავად იმისა რომ იგი საქართველოს კანონმდებლობის შესაბამისად წარმოადგენს ერთ ანგარიშს და გააჩნია ერთი იდენტიფიკატორი,

აუცილებელია, მულტისავალუტო ანგარიშზე გამოხატული თანხმობა ვრცელდებოდეს მასზე, როგორც ერთიან ანგარიშზე. **აუცილებელია**, ამსმპ-მა მმპ-ს მიაწოდოს ინფორმაცია ამ დოკუმენტის შესაბამისად იმგვარად, რომ შესაძლებელი იყოს ანგარიშის იდენტიფიცირება როგორც მულტისავალუტო ანგარიშისა, ასევე იმის დადგენა თუ კონკრეტულად რომელი ვალუტის გამოყენებაა შესაძლებელი ამ მულტისავალუტო ანგარიშზე.

შესაძლოა, ამსმპ-მა მხარი დაუჭიროს მულტისავალუტო ანგარიშის „დანაწევრებას“ ისე, რომ საშუალება მისცეს მმპ-ს, მიიღოს სმმ-ის თანხმობა მულტისავალუტო ანგარიშთან დაკავშირებულ კონკრეტულ ვალუტასთან მიმართებაში. აღნიშნული გულისხმობს, მაგალითად, ანგარიშზე დეტალური თანხმობის მოთხოვნისას (იხ. 9.1.1 თავი) ვალუტის კოდის მითითებასაც.

თუ ამსმპ მხარს უჭერს მულტისავალუტო ანგარიშის „დანაწევრებას“, ერთ ვალუტასთან მიმართებაში გაცემული თანხმობა **არავითარ შემთხვევაში** არ უნდა გულისხმობდეს თანხმობას სხვა ვალუტასთან მიმართებაში.

თუ ამსმპ მხარს არ უჭერს მულტისავალუტო ანგარიშის „დანაწევრებას“, **აუცილებელია** ანგარიშზე დეტალური თანხმობის მოთხოვნისას (იხ. 9.1.1 თავი) მან სმმ-ს თანხმობა გამოახატინოს იმის მიუხედავად, გადმოეცა თუ არა ანგარიშის ნომერთან ერთად ანგარიშის ვალუტა.

9.1.7 თანხმობის მოთხოვნის სერვისი

სერვისი აღწერილია (2)-ის 6.3.1 თავით. **აუცილებელია,** აღნიშნული სერვისის მხარდაჭერა წინამდებარე დოკუმენტის მიმდინარე ვერსიასთან თავსებადობის მიზნით.

მას შემდეგ, რაც მმპ შექმნის თანხმობის ობიექტს და გადასცემს მას ამსმპ-ს, **აუცილებელია** ამსმპ-მა დააბრუნოს ერთ-ერთი შემდეგი პასუხი:

1) თანხმობის მოთხოვნის ავტომატური უარყოფა.
2) თანხმობის მოთხოვნის ავტომატური დაკმაყოფილება.
3) მომხმარებლის თანხმობის მოთხოვნა ძლიერი ავთენტიფიკაციის.

იმ შემთხვევაში, თუ თანხმობის ობიექტის დაკმაყოფილება საჭიროებს რამდენიმე მომხმარებლის მიერ გამოხატულ თანხმობას (მაგ. კორპორაციულ კონტექსტში), წინამდებარე დოკუმენტის ამ ვერსიის მიზნებისთვის **აუცილებელია**, მოხდეს მოთხოვნის ავტომატური უარყოფა. ანუ წინამდებარე დოკუმენტის ამ ვერსიისათვის (2)-ის 6.3.4 თავით განსაზღვრული შესაძლებლობა **არავითარ შემთხვევაში** არ უნდა იქნას გამოყენებული. აღნიშნული მხარდაჭერილი იქნება შემდგომ ვერსიებში.

9.1.7.1 თანხმობის მოთხოვნის ავტომატური დაკმაყოფილება

შესაძლოა, ამსმპ-მა პირდაპირ დააბრუნოს მნიშვნელობა consentStatus=valid და არ დააბრუნოს ASPSP-SCA-Approach იმ შემთხვევაში, როდესაც დაკმაყოფილებულია ყველა შემდეგი პირობა:

1) Authorization-ში გადმოცემულია OAuth2 ტოკენი, რომელიც ვალიდურია და მისი საშუალებით შესაძლებელია სმმ-ის იდენტიფიკაცია საქართველოს კანონმდებლობით განსაზღვრული რწმუნების დონით, ასეთის არსებობის შემთხვევაში.
2) საქართველოს კანონმდებლობა უფლებას ანიჭებს ამსმპ-ს, ჩათვალოს აღნიშნული ტოკენის წარდგენა მომხმარებლის მიერ გამოხატულ თანხმობად ანგარიშების გაცემაზე.

ყველა სხვა შემთხვევაში, წინამდებარე დოკუმენტის ამ ვერსიის მიზნებისათვის ამსმპ-მა არავითარ შემთხვევაში არ უნდა დააბრუნოს consentStatus=valid და მოითხოვოს მომხმარებლის ძლიერი ავთენტიფიკაცია.

9.1.7.2 თანხმობის ავტორიზაცია მომხმარებლის ძლიერი ავთენტიფიკაციის საფუძველზე

იმ შემთხვევაში, თუ ამსმპ-ს ესაჭიროება მომხმარებლის ძლიერი ავთენტიფიკაცია თანხმობის დასადასტურებლად, **აუცილებელია**, ამსმპ-მა დააბრუნოს მხოლოდ OAuth ვარიანტი, კერძოდ:

1) **აუცილებელია**, ველში ASPSP-SCA-Approach დაბრუნდეს REDIRECT
2) **აუცილებელია**, ჰიპერბმულების სექციაში (_links) დაბმულდეს scaOAuth ჰიპერბმული, რომელიც მიუთითებს ამსმპ-ის OAuth2 სერვერის მეტაინფორმაციაზე, რომელიც თავის მხრივ **აუცილებელია** დაფორმირდეს (14)-ის მიხედვით.

იმისათვის, რომ განხორციელდეს მომხმარებლის ძლიერი ავთენტიფიკაცია, მმპ-ს ესაჭიროება მიიღოს „ავტორიზაციის რესურსი“. „ავტორიზაციის რესურსის“ შექმნის პროცესს სრულად წარმართავს ამსმპ, ჰიპერბმულების სექციაში დაბრუნებული სხვადასხვა კონფიგურაციების მეშვეობით. აღნიშნული აღწერილია ამ დოკუმენტის 10.1 თავით. მას შემდეგ, რაც „ავტორიზაციის რესურსი“ მიღებული იქნება, **აუცილებელია** მოხდეს მომხმარებლის ძლიერი ავთენტიფიკაცია და თანხმობის მიღება ამ დოკუმენტის მე- 10 თავში მითითებული წესით.

9.1.8 თანხმობის შესაბამისობა მოთხოვნილ ინფორმაციასთან

იმ შემთხვევაში, თუ თანხმობა არასაკმარისია, **აუცილებელია** გამოძახებამ დააბრუნოს CONSENT_INVALID და არა „შემცირებული“ დოკუმენტი მნიშვნელობა (მაგ. თუ თანხმობა არაა გაცემული ბალანსების დაბრუნებაზე, withBalance პარამეტრის გამოყენება უნდა დასრულდეს CONSENT_INVALID ტიპის შეცდომით).

9.1.9 თანხმობების ტექნიკური გაერთიანება

უმჯობესია, ამსმპ-მა არ მოსთხოვოს მმპ-ს მომხმარებლის ძლიერი ავთენტიფიკაცია იმ თანხმობის მოთხოვნაზე, თუ მმპ-ს უკვე მიღებული აქვს რამდენიმე თანხმობა, რომელთა გაერთიანება მოიცავს მმპ-ს მიერ მოთხოვნილ თანხმობას და თუ ამ თანხმობათაგან თითოეულის ვადა და ჯერადობა უდრის ან აღემატება მოთხოვნილი თანხმობის ვადას და ჯერადობას. იმ შემთხვაში, თუ ამსმპ-ს აღნიშნული ფუნქციონალი აქვს რეალიზებული, **აუცილებელია**, ამსმპ-მა აღნიშნულ თანხმობას მიანიჭოს უნიკალური იდენტიფიკატორი ისევე, როგორც მიანიჭებდა ნებისმიერ სხვა თანხმობას.

9.1.10 თანხმობის მართვის სერვისები

აუცილებელია, ამსმპ-მა მხარი დაუჭიროს (2)-ის 6.3.2, 6.3.3, 6.4 თავით განსაზღვრულ სერვისებს (თანხმობის სტატუსი, თანხმობის ინფორმაცია, თანხმობის გათხოვა).

9.2 საბანკო ანგარიშების ინფორმაციის სერვისები

9.2.1 თანხმობა და ავტორიზაცია

აუცილებელია, ყველა სერვისს გადაეცემოდეს Authorization და Consent-ID სათაურები.

აუცილებელია, Authorization სათაურში გადმოცემული Bearer ტოკენი იყოს იგივე, რაც გამოყენებული იქნა Consent-ID სათაურში მითთებული თანხმობის დადასტურებისას, თუ აღნიშნული ტოკენი მოქმედია. ხოლო ტოკენის ვადის გასვლის შემთხვევაში **აუცილებელია**, Authorization სათაურში გადაეცეს იგივე ტოკენის Refresh Token-ით გახანგრძლივების შედეგი.

9.2.2 ანგარიშის ნომრების ტოკენიზაცია

აუცილებელია, ResourceID მნიშვნელობები (იხ. (2) თავი 14.19) იყოს ტოკენიზებული, უნიკალური ტოკენებით, რათა URI-ებიდან არ მოხდეს ანგარიშის ნომრების გაჟონვა.

აუცილებლია, ტოკენიზაციის პროცესში გამოყენებული იყოს ცალმხრივი ალგორითმი, რათა გამოირიცხოს ტოკენიდან ანგარიშის რაიმე მახასიათებლის აღდგენა. **რეკომენდებულია** ტოკენის ჩაწერის ფორმად UUID-ის (იხ. (15)) გამოყენება.

9.2.3 ანგარიშების სია

სერვისი აღწერილია (2)-ის 6.5.1 თავით. **აუცილებელია,** აღნიშნული სერვისის მხარდაჭერა წინამდებარე დოკუმენტის მიმდინარე ვერსიასთან თავსებადობის მიზნით.

თუ Consent-ID სათაურში გადაცემული იდენტიფიკატორი მიუთითებს გამოსადეგი ანგარიშების თანხმობაზე (იხ. 9.1.4 თავი), **აუცილებელია** ამსპმ-მა დააბრუნოს ყველა გამოსადეგი ანგარიში. სხვა შემთხვევაში **აუცილებელია**, ინფორმაცია დაბრუნდეს ხელმისაწვდომ ანგარიშებზე, რომელზე გაცემული იყო თანხმობა.

ამსმპ-მა ინფორმაციის დაბრუნებისას **არავითარ შემთხვევაში** არ უნდა დააბრუნოს ის დეტალური ინფორმაცია, რომლის გაცემაზე თანხმობა გამოხატული არ ყოფილა Consent-ID სათაურში გადმოცემული მნიშვნელობით მითითებულ თანხმობაში. ქვემოთ მოცემული სია მიუთითებს რამდენიმე მაგალითზე:

1. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს balances ელემენტები გამოსადეგ ანგარიშზე, თუ გაცემული თანხმობა არ არის availableAccountsWithBalance ტიპის (ანუ არის availableAccounts ტიპის).
2. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს transactions ელემენტები გამოსადეგ ანგარიშებზე.

3. ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს balances ელემენტი ხელმისაწვდომ ანგარიშზე, თუ აღნიშნულ ანგარიშზე ბალანსების გაცემაზე თანხმობა არც ცხადად ყოფილა გამოხატული (იხ. 9.1.1 და 9.1.3 თავი). იგივე წესი ვრცელდება ტრანზაქციებსა და ანგარიშის მფლობელის სახელზეც.
4. თუ ანგარიში მულტისავალუტოა და თანხმობა გაცემულია მულტისავალუტო ანგარიშის დონეზე, **აუცილებელია**, დაბრუნდეს როგორც სავალუტო „ქვეანგარიშები“, ისე თავად მულტისავალუტო ანგარიშის შესახებ ინფორმაცია. **აუცილებელია**, მულტისავალუტო ანგარიშის ვალუტაში მითითებული იყოს “XXX”.
5. თუ ანგარიში მულტისავალუტოა და თანხმობა გაცემულია არა მთლიანად ამ ანგარიშზე, არამედ მის შესაბამის ერთ ან რამდენიმე ვალუტაზე, მულტისავალუტო ანგარიშის ინფორმაცია **არავითარ შემთხვევაში** არ უნდა დაბრუნდეს.
6. თანხმობის არსებობის შემთხვევაში ჰიპერბმულის დაბრუნება **აუცილებელია** ბალანსებისთვისაც და ტრანზაქციებისთვისაც.

როდესაც ამ თავის მოთხოვნების დასაკმაყოფილებლად ამსმპ აბრუნებს რამდენიმე ჩანაწერს მულტისავალუტო ანგარიშთან დაკავშირებით, **აუცილებელია**, ყველა მათგანს ჰქონდეს ერთიდაიგივე მნიშვნელობა ResourceId ველში.

ამსმპ-სათვის გასაგზავნი ინფორმაციის და დასაბრუნებელი პასუხების მაგალითები მოცემულია (2)-ის 6.5.1 თავში.

9.2.4 ანგარიშის დეტალები

სერვისი აღწერილია (2)-ის 6.5.2 თავით. **აუცილებელია** აღნიშნული სერვისის მხარდაჭერა წინამდებარე დოკუმენტის მიმდინარე ვერსიასთან თავსებადობის მიზნით.

აუცილებელია, მხარდაჭერილი იყოს ის შემთხვევა, როდესაც მოთხოვნისას Account-ID პარამეტრში გადაეცემა ანგარიშების სიის მიერ (იხ. 9.2.3 თავი) დაბრუნებული ResourceID მნიშვნელობა.

თუ ანგარიში მულტისავალუტოა, **აუცილებელია** ვალუტაში ამსმპ-მა დააბრუნოს XXX.

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს balances ჰიპერბმული, თუ Consent-ID სათაურში გადაცემული იდენტიფიკატორი არ მიუთითებს ისეთ ბალანსების გაცემასთან დაკავშირებულ თანხმობაზე. იგივე ეხება transactions ჰიპერბმულს და დამატებით ინფორმაციას. თანხმობის არსებობის შემთხვევაში ჰიპერბმულის დაბრუნება **აუცილებელია**.

აუცილებელია, ყველა იმ ანგარიშისათვის რომელზე ნაშთის ცვლილებაც შესაძლებელია მოხდეს ელექტრონული არხებით (მათ შორის საბარათე ოპერაციების მეშვეობით), ანგარიშების დეტალებში დაბრუნდეს balances ელემენტი, თუ თანხმობა ითვალისწინებს ბალანსის ინფორმაციის გაცემასაც. ასეთი ანგარიშებისათვის **აუცილებელია**, სულ მცირე, შემდეგი ბალანსის ტიპების დაბრუნება balances ელემენტის შიგნით: interimAvailable, interimBooked.

9.2.5 ანგარიშის ბალანსი

სერვისი აღწერილია (2)-ის 6.5.3 თავით. **აუცილებელია** აღნიშნული სერვისის მხარდაჭერა წინამდებარე დოკუმენტის მიმდინარე ვერსიასთან თავსებადობის მიზნით.

აუცილებელია, მხარდაჭერილი იყოს ის შემთხვევა, როდესაც მოთხოვნისას account-ID პარამეტრში გადაეცემა ანგარიშების სიის მიერ (იხ. 9.2.3 თავი) დაბრუნებული resourceID მნიშვნელობა.

თუ ანგარიში მულტისავალუტოა, **აუცილებელია** ბალანსი დაბრუნდეს თითოეულ ვალუტაში რაც განსაზღვრულია აღნიშნულ მულტისავალუტო ანგარიშზე.

აუცილებელია, დაბრუნდეს, სულ მცირე, შემდეგი ბალანსის ტიპები: closingBooked და interimAvailable.

უმჯობესია, ამსმპ-მა დააბრუნოს account კომპონენტი, (2) -ის მომდევნო ვერსიების მხარდაჭერის მიზნით.

9.2.6 ანგარიშის ტრანზაქციების სია

სერვისი აღწერილია (2)-ის 6.5.4 თავით. **აუცილებელია,** აღნიშნული სერვისის მხარდაჭერა წინამდებარე დოკუმენტის მიმდინარე ვერსიასთან თავსებადობის მიზნით.

აუცილებელია, მხარდაჭერილი იყოს ის შემთხვევა, როდესაც მოთხოვნისას account-ID პარამეტრში გადაეცემა ანგარიშების სიის მიერ (იხ. 9.2.3 თავი) დაბრუნებული resourceID მნიშვნელობა.

თუ ანგარიში მულტისავალუტოა, **აუცილებელია** ვალუტაში ამსმპ-მა დააბრუნოს ტრანზაქციები ყველა „ქვეანგარიშზე“.

აუცილებელია, მხარდაჭერილი იყოს ტრანზაქციების სიის გამოძახება პარამეტრებით dateFrom და dateTo.

უმჯობესია, მხარდაჭერილი იყოს ტრანზაქციების სიის გამოძახების ის ვარიანტი, როდესაც გადმოეცემა მხოლოდ dateFrom.

უმჯობესია, მხარდაჭერილი იყოს ტრანზაქციების სიის ის ვარიანტი, როდესაც პარამეტრად არ გადმოეცემა dateFrom და გადმოეცემა entryReferenceFrom, ხოლო აღნიშნული მოთხოვნის საპასუხოდ ამსმპ დააბრუნებს ტრანზაქციებს, რომელიც მოხდა entryReferenceFrom -ით მითითებული ტრანზაქციის (ანუ ტრანზაქციის, რომელსაც დეტალებში entryReference ექნებოდა ამ პარამეტრის ტოლი, იხ 9.2.9 თავი) შემდეგ.

აუცილებელია ამსმპ-ს ჰქონდეს პარამეტრი dateTo-ს მხარდაჭერა (ტრანზაქციების მოთხოვნა მითითებულ თარიღამდე), თუმცა აღნიშნული პარამეტრის გადაცემა გამოძახებისას უნდა იყოს **არააუცილებელი**, რათა მმპ-მ მოითხოვოს სერვისის გამოძახების მომენტამდე.

აუცილებელია, მხარდაჭერილი იყოს booked მნიშვნელობა bookingStatus პარამეტრში, სერვისის გამოძახებისას. **აუცილებელია**, მხარდაჭერილი იყოს pending მნიშვნელობა bookingStatus პარამეტრში, სერვისის გამოძახებისას ისეთი ანგარიშისათვის, რომლის ნაშთის ცვლილებაც

შეიძლება მოხდეს ელექტრონული არხებით, ონლაინ რეჟიმში (მათ შორის საბარათე ოპერაციებით). მნიშვნელობები both და information **არააუცილებელია**.

თუ თანხმობა გამოცხადებულია ბალანსების მიწოდებაზე და მოთხოვნილი არ არის bookingStatus=information, **აუცილებელია** balances სექცია დაფორმირდეს შემდეგი წესის დაცვით:

1) თუ bookingStatus-ად მოთხოვნილია “booked” ან “both” (თუ მხარდაჭერილია) **აუცილებელია** დაბრუნდეს openingBooked და closingBooked ტიპის ბალანსები.
2) თუ bookingStatus-ად მოთხოვნილია “pending” ან „both” (თუ მხარდაჭერილია) **აუცილებელია** დაბრუნდეს interimBooked და interimAvailable ტიპის ბალანსები.
3) **აუცილებელია**, თითოეული ბალანსი ასახავდეს მიმდინარე პორციის ინფორმაციას (და არა მთელი ამონაწერისას).

9.2.7 ტრანზაქციების ინფორმაციის დაყოფა პორციებად

თუ დასაბრუნებელი ტრანზაქციების საერთო რაოდენობა აღემატება 50-ს, **აუცილებელია** ამსმპ-მა პასუხი დააბრუნონ დანაწილებული ფორმით. მმპ და ამსმპ შეიძლება ხელშეკრულების საფუძველზე შეთანხმდნენ აღნიშნული მოთხოვნის გაუქმებაზე ან ლიმიტის შეცვლაზე.

აუცილებელია, ამსმპ-მა მხარი დაუჭიროს დანაწილებული ფორმით პასუხის დაბრუნების სულ მცირე შემდეგ სცენარს:

1) პორციაში იყოს 50 ან უფრო ნაკლები ტრანზაქცია.
2) პირველი პორციისათვის ჰიპერბმულების სექციაში (_links) მითითებულია first და next ტიპის ჰიპერბმულები.
3) შუალედური (არც პირველი, არც უკანასკნელი) პორციისათვის ჰიპერბმულების სექციაში მითითებულია first და next ჰიპერბმულები.
4) ბოლო პორციისათვის ჰიპერბმულების სექციაში მითითებულია მხოლოდ first ჰიპერბმული.
5) ჰიპერბმული first ყველა შემთხვევაში მიუთითებს ზუსტად იგივე მისამართს, რა მისამართის გამოყენებითაც მოხდა ტრანზაქციების სიის გამოძახება.

უმჯობესია, next ჰიპერბმულში, რომელსაც მმპ-ს დაუბრუნებს, ამსმპ-მა საკუთარი სერვისს გადასცემს entryReferenceFrom პარამეტრი.

9.2.8 საინფორმაციო სახის „ტრანზაქციების“ მხარდაჭერა

მუდმივი საგადასახადო დავალებების პარამეტრების ან (2)-ში განსაზღვრული სხვა საინფორმაციო სახის ტრანზაქციების მმპ-სთვის მხარდაჭერა (პარამეტრი bookingStatus=information წინამდებარე დოკუმენტის ამ ვერსიის მიზნებისათვის არააუცილებელია და დაბრუნებული ინფორმაციის მოცულობა ამ დოკუმენტით არ რეგულირდება. აღნიშნული პარამეტრის მხარდაჭერისას ამსმპ-მა აუცილებელია სრულად იხელმძღვანელოს მხოლოდ (2)-ით. თუმცა მუდმივი საგადასახადო დავალების ფარგლებში შექმნილი კონკრეტული ტრანზაქციები **აუცილებელია** მმპ-ს მიეწოდოს ისეთივე ფორმით, რა

ფორმითაც ნებისმიერი სხვა ტრანზაქცია ანგარიშზე (bookingStatus=booked, pending ან both შემთხვევებში).

9.2.9 ანგარიშზე გატარებული ტრანზაქციების მინიმალური ინფორმაციის მოთხოვნები

ნებისმიერი ტრანზაქციისათვის ამსმპ-მა სერვისით დააბრუნოს, სულ მცირე, შემდეგი ველები (2)-ის 14.24 თავით განსაზღვრული ჩამონათვალიდან:

სახელი	ტიპი	აუცილებლობა	კომენტარი
entryReference	Max35Text	**აუცილებელია**	ტრანზაქციის იდენტიფიკატორი, რომელსაც მმპ საჭიროებისამებრ მიაწვდის სმმ-ს და რომლის გამოყენება ასევე შესაძლებელი იქნება ინფორმაციის ნაწილობრივი დაბრუნებისთვის, თუ მხარდაჭერილი იქნება ამსმპ-ის მიერ
transactionAmount	Amount	**აუცილებელია**	ტრანზაქციის თანხა და ვალუტა, ფორმატირებული (2)-ის 14.3 წესის შესაბამისად (სადებეტო ტრანზაქცია აღინიშნება უარყოფითი მნიშვნელობით, საკრედიტო ტრანზაქცია - დადებითით)
valueDate	ISODate	**აუცილებელია**	დღე, როდესაც: 1) თანხა გახდა ხელმისაწვდომი ანგარიშის მფლობელისათვის (საკრედიტო ტრანზაქციის შემთხვევაში) ან 2) შეწყვიტა ხელმისაწვდომობა (სადებეტო ტრანზაქციის შემთხვევაში
bookingDate	ISODate	პირობითი	დღე, როდესაც ტრანსაქცია აისახა ბალანსში. ანგარიშზე გატარებული ტრანზაქციების სიაში (“booked” სია)

			აღნიშნული ველის დაბრუნება **აუცილებელია**
currencyExchange	ReportExchangeRate ტიპის მასივი	პირობითი	თუ ტრანზაქცია გატარდა სხვა ვალუტაში, აღნიშნული ველი **აუცილებელია**
remittanceInformationUnstructured	Max140Text	პირობითი	**აუცილებელია** ამსმპ-მა დააბრუნოს ამ ორი მნიშვნელობიდან ერთ-ერთი, თუ მის სისტემაში აღნიშნული ინფორმაცია არსებობს და ის რაიმე სხვა გზით ხელმისაწვდომია სმმ-ისთვის. თუ ამსმპ-სა და მმპ-ს შორის სხვაგვარად არაა შეთანხმებული, **აუცილებელია**, ამსმპ-მა დააბრუნოს remittanceInformationUnstructuredArray, რათა სრულფასოვნად ასახოს მის სისტემაში დაცული ინფორმაცია. თუ არსებობს, მმპ-სთან შეთანხმება, ამსმპ-ს უფლება აქვს დააბრუნოს remittanceInformationUnstructured მონაცემი და გახადოს სრული ინფორმაცია ხელმისაწვდომი 9.2.10 თავის მიხედვით
remittanceInformationUnstructuredArray	Max140Text ტიპის მასივი	პირობითი	
additionalInformation	Max500Text	პირობითი	**აუცილებელია** ამსმპ-მა დააბრუნოს ეს ინფორმაცია, თუ თუ მის სისტემაში იგი არსებობს და რაიმე სხვა გზით ხელმისაწვდომია სმმ-ისთვის.
transactionId	String	პირობითი	**აუცილებელია** მხოლოდ იმ შემთხვევებისათვის, როდესაც გათვალისწინებულია დამატებითი ინფორმაციის დაბრუნება ცალკე გამოძახებით (მაგ. ამსმპ გადმოსცემს remittanceInformationUnstructured
_links	Links	**არააუცილებელი**	**შესაძლოა** ამსმპ-მა დააბრუნოს transactionDetails ტიპის ჰიპერბმული, რათა მმპ-ს გაუადვილოს ტრანზაქციის

			დეტალებზე წვდომა 9.2.10 თავის მიხედვით.

ცხრილი 3: ველები ტრანზაქციის ინფორმაციაში

ყველა დანარჩენი ველი, რომელიც (2)-ით არის განსაზღვრული, **არააუცილებელია**, თუ მათი არდაბრუნება არ ეწინააღმდეგება საქართველოს კანონმდებლობას. **უმჯობესია**, ამსმპ-მა დააბრუნოს ყველა ის ველი, რომელსაც იგი ხელმისაწვდომს ხდის სმმ-ისთვის სხვა არხების გამოყენებით.

9.2.10 ტრანზაქციის დეტალების სერვისი

აღნიშნული სერვისი აღწერილია (2)-ის 6.5.5 თავში. აღნიშნული სერვისის მხარდაჭერა **არააუცილებელია**, თუ ამსმპ სრულყოფილად აბრუნებს 9.2.9 თავში განსაზღვრულ ინფორმაციას (მაგ. ბრუნდება remittanceInformationUnstructured და არა remittanceInformationUnstructuredArray). თუ ინფორმაცია სრულყოფილად არ ბრუნდება ამსმპ-ს მიერ (წესებიც განსაზღვრულია 9.2.9 თავით), მაშინ აღნიშნული სერვისი მხარდაჭერა **აუცილებელია**.

9.3 საბარათე ანგარიშების ინფორმაციის სერვისები

საბარათე ანგარიშების სერვისები მოცემულია (2)-ის 6.6 თავში. წინამდებარე დოკუმენტთან თავსებადობის მიზნებისათვის, აგრეთვე მომხმარებლებისათვის კომფორტის შესაქმნელად **უმჯობესია** მათი მხარდაჭერა.

ზემოაღნიშნულის შესაბამისად, ყველა აუცილებელი მოთხოვნა რომელიც ამ თავის ქვეთავებშია მითითებული, აუცილებელი იქნება მხოლოდ იმ შემთხვევაში, როდესაც საბარათე ანგარიშების სერვისები მხარდაჭერილი იქნება ამსმპ-ის მიერ.

აღნიშნული სერვისების მხარდაჭერის შემთხვევაშიც **აუცილებელია**, ამსმპ-მა ამ ანგარიშებზე წვდომას მხარი დაუჭიროს როგორც ჩვეულებრივ საბანკო ანგარიშებზე წვდომის ფორმითაც (იხ. 9.2).

9.3.1 საბარათე ანგარიშებზე წვდომის ზოგადი სქემა

ვინაიდან წინამდებარე დოკუმენტის მიმდინარე ვერსიისათვის (2) მხარს არ უჭერს ერთ საბარათე ანგარიშზე რამდენიმე ბარათის არსებობის შემთხვევას, თავსებადობის შენარჩუნების მიზნით **აუცილებელია** შემდეგი მოთხოვნების დაკმაყოფილება საბარათე ანგარიშების (card-accounts) სერვისებში (იხ. (2), თავი 6.6):

1. **შესაძლოა**, საბარათე ანგარიშის სერვისებში ამსმპ არ დაეყრდნოს IBAN-ის მეშვეობით იდენტიფიცირებული საბანკო ანგარიშის მიმართ გამოხატულ თანხმობას და ამ საბანკო ანგარიშზე მიბმულ ბარათებზე თანხმობის მიღება მოითხოვოს ცალკე. თუ ამსმპ ამ გზას აირჩევს, **აუცილებელია** შემდეგი მოთხოვნების დაკმაყოფილება:
   1.1. **აუცილებელია**, ამსმპ-მა დააბრუნოს ბარათების ინფორმაცია „გამოსადეგი ანგარიშების სიის“ დაბრუნებისას (რა დროსაც უნდა დააბრუნოს maskedPan ტიპის მითითება);

1.2. **აუცილებელია,** ამსმპ-მა მხარი დაუჭიროს ბარათის შემთხვევაში თანხმობის გამოხატვის ყველა იმ ფორმას, რასაც მხარს უჭერს საბანკო ანგარიშებისათვის. აუცილებელია, თანხმობის მართვის პროცესებში ამსმპ-მა სმმ-ს ბარათის ნომერი უჩვენოს მასკირებული სახით იმგვარად, რომ სმმ-ს არ გაუძნელდეს კონკრეტული ბარათის იდენტიფიცირება და თანხმობასა თუ უარზე გაცნობიერებული გადაწყვეტილების მიღება;

1.3. **შესაძლოა**, ამსმპ-მა „ბანკში გამოხატული თანხმობის“ შემდეგ მმპ-ს მიაწოდოს ბარათის ნომრები არა მასკირებული სახით (maskedPan), არამედ ტოკენიზებულ ფორმით (pan) თუმცა ამ დროს **აუცილებელია**, ამსმპ-მა უზრუნველყოს აღნიშნული ტოკენიზებული მნიშვნელობის და კონკრეტულ ბარათთან მისი ცალსახა კავშირის ეფექტიანი გაზიარება სმმ-ისათვის (მაგ. ინტერნეტ-ბანკში ჩვენების გზით) შესაბამისი თანხმობის მოქმედების ვადის განმავლობაში;

2. **აუცილებელია,** საბარათე ანგარიშების სერვისებში გამოყენებული resourceId ველის (და, შესაბამისად, account-id პარამეტრის) მნიშვნელობა უნიკალურად მიუთითებდეს კონკრეტულ ბარათს და დარჩეს უცვლელი, სულ მცირე, ამ ბარათზე გაცემული აქტიური თანხმობის გამოყენების ვადის განმავლობაში. აღნიშნული მნიშვნელობა **არავითარ შემთხვევაში** არ უნდა ემთხვეოდეს შესაბამისი საბანკო ანგარიშის ტოკენიზებულ იდენტიფიკატორს საბანკო ანგარიშზე წვდომის (accounts) სერვისებში

3. მნიშვნელობა, რომელიც გამოყენებული იქნება როგორც resourceId/account-id, **არავითარ შემთხვევაში** არ უნდა ამჟღავნებდეს ბარათის ნომერს (Primary Account Number, PAN). **აუცილებელია**, იგი იყოს ტოკენიზებული საბარათე მონაცემების თანამედროვე სტანდარტებისა და საუკეთესო პრაქტიკების შესაბამისად ისე, რომ ამავდროულად არ დაირღვეს (2)-ის მოთხოვნები.

4. // გადახვევა XS2A ჩარჩოდან
აუცილებელია, თითოეული საბარათე ანგარიშის ინფორმაცია ჰიპერბმულების სექციაში (_links) აბრუნებდეს account ტიპის მითითებას, რომელიც მიუთითებს შესაბამის საბანკო ანგარიშის დეტალებზე (იხ. (4) თავი 6.5.2). **აუცილებელია**, ანგარიშის იდენტიფიკატორი იყოს ტოკენიზებული და ტოკენი დარჩეს უცვლელი, სულ მცირე, როგორც საბარათე ანგარიშისთვის გამოხატულ, ისე თავად ამ საბანკო ანგარიშზე გამოხატული თანხმობის გამოყენების ვადის განმვალობაში. იმ შემთხვევაში, თუ ბარათი მულტისავალუტო საბანკო ანგარიშზეა მიბმული, **აუცილებელია,** ჰიპერბმული აბრუნებდეს მულტისავალუტო ანგარიშის ინფორმაციას. **აუცილებელია**, ჰიპერბმული დაბრუნდეს მიუხედავად იმისა, აქვს თუ არა გამოხატული მომხმარებელს თანხმობა გაცემული ამ კონკრეტულ ანგარიშზე (მაგ. იმ შემთხვევაში, როცა ამსმპ ასხვავებს ერთმანეთისაგან ანგარიშზე IBAN-ით გამოხატულ თანხმობასა და ბარათზე გამოხატულ თანხმობას).

9.3.2 საბარათე ანგარიშებზე ინფორმაციის დაბრუნების წესი

ამ დოკუმენტთან თავსებადობის მიზნებისათვის, ყველა მოთხოვნა, რომელიც განსაზღვრულია საბანკო ანგარიშებისათვის 9.2 თავით, ძალაშია საბარათე ანგარიშებისთვისაც.

10 მომხმარებლის ძლიერი ავთენტიფიკაცია და თანხმობის გამოხატვა

10.1 ავტორიზაციის რესურსის ცნება და მისი შექმნის პროცესი

ავტორიზაციის რესურსი არის ჰიპერბმული, რომელიც ცალსახად აღწერს ერთეულს, რომელზეც ხდება თანხმობის გამოხატვა.

- წინამდებარე დოკუმენტის ამ ვერსიის მიზნისათვის, ეს ერთეულია ანგარიშის ინფორმაციის გაზიარებაზე მომხმარებლის თანხმობის მოთხოვნა (დოკუმენტი), რომელიც ამსმპ-ში უკვე რეგისტრირებულია 9.1.7 თავში მითითებული წესით.
- წინამდებარე დოკუმენტის შემდგომ ვერსიებში ეტაპობრივად დაემატება სხვა ერთეულებიც (მაგ. ერთეულოვანი გადახდა, გადახდის გაუქმება და სხვა).

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

კერძოდ, წინამდებარე დოკუმენტის ამ ვერსიის მიზნებისათვის **აუცილებელია**, ამსმპ-მა მხარი დაუჭიროს მხოლოდ შემდეგ ვარიანტებს ჰიპერბმულების სექციაში:

1) დააბრუნოს scaStatus ტიპის ჰიპერბმული (*შენიშვნა: არ აგერიოთ scaStatus ატრიბუტში!*)

   ეს ნიშნავს, რომ ამსმპ-ს აქვს ყველა სათანადო ინფორმაცია მომხმარებლის ძლიერი ავთენტიფიკაციის დასაწყებად და scaStatus შეიცავს უშუალოდ ავტორიზაციის რესურსის ჰიპერბმულს. ამ ჰიპერბმულის მიღების შემდეგ **აუცილებელია**, მმპ-მა პირდაპირ დაიწყოს OAuth ავტორიზაციის პროცესი.

2) დააბრუნოს startAuthorization ტიპის ჰიპერბმული.

   ეს ნიშნავს, რომ ამსმპ-ს აქვს ყველა სათანადო ინფორმაცია მომხმარებლის ძლიერი ავთენტიფიკაციის დასაწყებად, თუმცა ავტორიზაციის რესურსის შექმნა ცხადად უნდა მოითხოვოს მმპ-მა. ავტორიზაციის რესურსების შექმნა აღწერილია 10.2 თავით. ავტორიზაციის რესურსის წარმატებით შექმნის შემდეგ **აუცილებელია**, მმპ-მა პირდაპირ დაიწყოს OAuth ავტორიზაციის პროცესი.

3) დააბრუნოს startAuthorisationWithAuthenticationMethodSelection ტიპის ჰიპერბმული
   ეს ნიშნავს, რომ ამსმპ-მა ავტომატურ რეჟიმში ვერ გადაწყვიტა, რა ტიპის ავთენტიფიკაცია უნდა გაატაროს მომხმარებელს, მმპ-მა უნდა მოითხოვოს ავტორიზაციის რესურსის ცხადად შექმნა, რა დროსაც ამსმპ დააბრუნებს selectAuthenticationMethods ჰიპერბმულს (და შესაბამის დამატებით ინფორმაციას). ავტორიზაციის რესურსების შექმნა აღწერილია 10.2 თავით, selectAuthenticationMethods ჰიპერბმულის დამუშავების წესი აღწერილია ქვემოთ.

4) დააბრუნოს selectAuthenticationMethods ტიპის ჰიპერბმული

   ამ შემთხვევაში **აუცილებელია**, ამსმპ-მა იმავე პასუხში დააბრუნოს არაცარიელი scaMethods მასივი და **აუცილებელია**, მმპ-მა შესთავაზოს მომხმარებელს ერთ-ერთი მეთოდის არჩევა, ხოლო არჩეული მეთოდი გადასცეს selectAuthenticationMethods ჰიპერბმულზე ისე, როგორც ეს აღწერილია (2)-ის 7.2.3 თავით.

   თუ ავთენტიფიკაციის მეთოდის არჩევა წარმატებულია, **აუცილებელია** ამსმპ-მა აღნიშნულის დასრულების შემდეგ დააბრუნოს scaStatus ჰიპერბმული და OAuth2 სერვერის პარამეტრები, როგორც ეს წინამდებარე თავშია მითითებული და **აუცილებელია**, მმპ-მა პირდაპირ დაიწყოს OAuth ავტორიზაციის პროცესი.

   უმჯობესია ამ მეთოდის გამოყენება startAuthorisationWithAuthenticationMethodSelection ტიპის ჰიპერბმულის დაბრუნებასთან შედარებით.

შესაძლოა ავთენტიფიკაციიის მეთოდის არჩევა selectAuthenticationMethods ჰიპერბმულის მეშვეობით (startAuthorisationWithAuthenticationMethodSelection შუალედური რგოლით ან პირდაპირ) ამსმპ-მა გამოიყენოს იმისათვის, რათა მოახდინოს მომხმარებლის ზოგადი ავთენტიფიკაციის (რაც Authorization სათაურში გადმოცემული OAuth2 ტოკენით გამოიხატება) გარდაქმნა მომხმარებლის ძლიერ ავთენტიფიკაციად, როგორც ეს აღწერილია ამ დოკუმენტის 6.3 თავით, კერძოდ დააბრუნოს OAuth პროტოკოლის ისეთი პარამეტრები, რომლებიც უზრუნველყოფენ მხოლოდ მეორე ფაქტორით ავთენტიფიკაციას. თუმცა **შესაძლოა** ამსმპ-მა აღნიშნულის მისაღწევად გამოიყენოს ამ თავის მოთხოვნებთან თავსებადი რაიმე სხვა მეთოდი.

ამსმპ-მა **არავითარ შემთხვევაში** არ უნდა დააბრუნოს startAuthorisation* ტიპის სხვა ჰიპერბმულები, გარდა იმისა რაც წინამდებარე თავში იყო აღწერილი.

10.2 ავტორიზაციის რესურსების შექმნის სერვისი

თუ ავტორიზაციის რესურსი ავტომატურად არ შექმნილა იმ ერთეულის რეგისტრაციის პროცესში, რომელზეც უნდა მოხდეს თანხმობის გამოხატვა (მაგ. ანგარიშის ინფორმაციის გაზიარებაზე მომხმარებლის თანხმობის მოთხოვნის რეგისტრაციისა), რასაც მიუთითებს ჰიპერბმულების სექციაში დაბრუნებული scaStatus ტიპის ჰიპერბმული, აუცილებელია მმპ-მა ცხადი გამოძახებით შექმნას ავტორიზაციის რესურსი.

ავტორიზაციის რესურსის შექმნის სერვისი აღწერილია (2)-ის 7.4 სერვისის გამოძახებისას (ამ სერვისის მხარდაჭერა და ავტორიზაციის რესურსების ცხადი შექმნის მიდგომის გამოყენება **რეკომენდებულია**). კერძოდ, **აუცილებელია**, ამსმპ-მა დააბრუნოს აღნიშნული სერვისის მისამართი startAutorisation (ან მისი მოდიფიკაცია startAuthorisationWithAuthenticationMethodSelection) ტიპის ჰიპერბმულით. ჰიპერბმულის ტიპის მიხედვით **აუცილებელია** შემდეგი:

1) startAutorisation - თუ გამოძახება წარმატებით შესრულდა, **აუცილებელია**, შეიქმნას ავტორიზაციის რესურსი და დაუბრუნდეს იგი მმპ-ს.

2) startAuthorisationWithAuthenticationMethodSelection - თუ გამოძახება წარმატებით შესრულდა, **აუცილებელია** ამსმპ-მა პასუხში მმპ-ს დაუბრუნოს selectAuthenticationMethods ტიპის ჰიპერბმული და არაცარიელი scaMethods მასივი. აღნიშნული შემთხვევის დამუშავების წესი აღწერილია 10.1 თავით.

10.3 თანხმობის გამოხატვა მომხმარებლის ძლიერი ავთენტიფიკაციის შემდეგ

მომხმარებლის ძლიერი ავთენტიფიკაციის მოთხოვნები მოცემულია ამ დოკუმენტის 6.2 თავით. მას შემდეგ, რაც მომხმარებელი გაივლის ავთენტიფიკაციას, **აუცილებელია** ამსმპ-მა მას მოსთხოვოს თანხმობის გამოხატვა და ამ თავში მოცემულია თანხმობის მინიმალური მოთხოვნები. **შესაძლოა**, ამსმპ-მა აღნიშნული მოთხოვნები გააფართოვოს შეხედულებისამებრ.

10.3.1 თანხმობის გამოხატვა ანგარიშის ინფორმაციის გაზიარებაზე

თუ ანგარიშის ინფორმაციის გაზიარების თანხმობის მოთხოვნისას მმპ-მა წარმოადგინა კონკრეტული ანგარიშის ნომრები ან ბარათის მასკირებული ნორმები (ანუ მოითხოვა დეტალური თანხმობა, როგორც ეს განსაზღვრულია 9.1.1 თავით), **აუცილებელია** ამსმპ-მა აჩვენოს სმმ-ს ყველა შესაბამისი ანგარიში და ბარათი, რომელზეც ხდება თანხმობის გამოხატვა.

თუ ამსმპ მხარს უჭერს საბარათე ანგარიშების სერვისებს (იხ. 9.3 თავი) და მმპ-მა წარმოადგინა ტოკენიზებული ბარათის ნომერი დეტალური თანხმობის გამოხატვის პროცესში, **აუცილებელია**, ამსმპ-მა იგი გადაიყვანოს მასკირებულ ნომერში და ისე აჩვენოს სმმ-ს, რათა სმმ-მა ნათლად აღიქვას, კონკრეტულად რომელ ბარათთან დაკავშირებულ ანგარიშზე აძლევს თანხმობას მმპ-ს.

თუ მმპ-მა წარმოადგინა ყველა გამოსადეგი ანგარიშის მიღებაზე თანხმობის მოთხოვნა (იხ. 9.1.4 თავი) **აუცილებელია** ამსმპ-მა სმმ-ს ეკრანზე გამოტანილი ინფორმაციის სახით შეატყობინოს ყველა იმ ანგარიშის და ბარათის შესახებ, რომლის ინფორმაციაც გაუზიარდება მმპ-ს.

თუ მმპ თანხმობის გამოხატვის პროცესში მოითხოვს ანგარიშის ნაშთებზე ან ტრანზაქციებზე წვდომას (მაგ. დეტალური თანხმობის მოთხოვნისას), **აუცილებელია** ამსმპ-მა თანხმობის გამოხატვის პროცესში სმმ-ს უჩვენოს ანგარიშის ნაშთი (მიმდინარე ნაშთი ან მიმდინარე საოპერაციო დღის დასაწყისისთვის დაფიქსირებული ნაშთი).

11 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 1.3.6 2020 წლის 3 თებერვალი.

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

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

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

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

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

14. ***RFC8414 (OAuth 2.0 Authorization Server Metadata).***

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