VENDIM
Nr. 272, datë 2.5.2024

PËR MIRATIMIN E PROTOKOLLIT PËR NDËRLIDHJEN E SKEMAVE PËR IDENTIFIKIMIN ELEKTRONIK TË SHTETASVE TË BALLKANIT PERËNDIMOR

Në mbështetje të nenit 100 të Kushtetutës dhe të nenit 19, të ligjit nr. 43/2016, "Për marrëveshjet ndërkombëtare në Republikën e Shqipërisë", me propozimin e ministrit të Brendshëm, Këshilli i Ministrave

VENDOSI**:**

Miratimin e protokollit për ndërlidhjen e skemave për identifikimin elektronik të shtetasve të Ballkanit Perëndimor, sipas tekstit që i bashkëlidhet këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

ZËVENDËSKRYEMINISTËR
Belinda Balluku

PROTOKOLL
MBI NDËRLIDHJEN E SKEMAVE PËR IDENTIFIKIM ELEKTRONIK TË SHTETASVE TË BALLKANIT PERËNDIMOR

Ne, pjesëmarrësit e Ballkanit Perëndimor, të referuar bashkërisht si "Palët Kontraktuese" dhe individualisht si "Pala Kontraktuese",

në përputhje me nenin 8 të Marrëveshjes për Ndërlidhjen e Skemave për Identifikimin Elektronik të Shtetasve të Ballkanit Perëndimor, të nënshkruar, më 21 dhjetor 2021, në Tiranë (në vijim e referuar si Marrëveshja),

kanë rënë dakord si më poshtë:

Neni 1

Ky protokoll rregullon kushtet më të detajuara për zbatimin e Marrëveshjes për ndërlidhjen e skemave për identifikimin elektronik të shtetasve të Ballkanit Perëndimor, veçanërisht përshkrimin teknik të numrit të identifikimit të Ballkanit të Hapur dhe proceset e ndërlidhjes së zgjidhjeve të softeve kombëtarë që mundësojnë federimin e identiteteve elektronike sipas parimit të ndërlidhjes së skemave me shërbimet e Qeverisjes elektronike të Palëve të tjera Kontraktuese.

Neni 2

Kushtet e përmendura në nenin 1 të këtij protokolli përshkruhen hollësisht në dokumentin Open Balkan Identification Number (Numri Identifikues i Ballkanit të Hapur): Arkitektura e referencës teknike për zbatimin e Marrëveshjes "Ndërlidhja e skemave për identifikimin elektronik të shtetasve të Ballkanit Perëndimor", e cila i bashkëlidhet këtij Protokolli dhe është pjesë përbërëse e tij.

Neni 3

Palët kontraktuese do të krijojnë një grup të përbashkët pune për të diskutuar dhe zgjidhur të gjitha çështjet ligjore dhe teknike që dalin nga zbatimi i Marrëveshjes dhe këtij protokolli.

Palët kontraktuese do të caktojnë secila një person me detyrën për të udhëhequr dhe bashkëkryesuar takimet e Grupit të Përbashkët të Punës dhe për të përfaqësuar pikën kryesore të kontaktit për koordinimin e zbatimit të këtij protokolli.

Palët kontraktuese mund të caktojnë sa më shumë persona të nevojshëm si anëtarë të Grupit të Përbashkët të Punës për të përmbushur detyrimet e fushave të bashkëpunimit të përcaktuara në Marrëveshje dhe në këtë protokoll.

Palët Kontraktuese do të njoftojnë njëra-tjetrën nëpërmjet kanaleve të duhura për personat e caktuar të përmendur në paragrafin 2 të këtij neni dhe do të shkëmbejnë informacion mbi pikat e kontaktit, jo më vonë se 7 ditë nga data e nënshkrimit të këtij protokolli.

Neni 4

Për secilën Palë Kontraktuese, ky protokoll do të hyjë në fuqi në datën e marrjes së njoftimit të fundit me shkrim me të cilin Palët njoftojnë njëra-tjetrën, nëpërmjet depozituesit, për përfundimin e procedurave siç kërkohet nga legjislacioni i tyre i brendshëm për hyrjen në fuqi të këtij protokolli.

Palët mund ta ndryshojnë këtë protokoll me shkrim.

Ky protokoll është lidhur për një periudhë kohore të pacaktuar dhe do të mbetet në fuqi për sa kohë që Marrëveshja mbetet në fuqi.

Origjinali i këtij protokolli në një kopje të vetme në gjuhën angleze do të depozitohet pranë Qeverisë së Republikës së Shqipërisë, si Depozitues i Marrëveshjes, e cila do t'i transmetojë një kopje të vërtetuar secilës Palë Kontraktuese.

Nënshkruar në Beograd, më _____, dy mijë e njëzet e katër

Nënshkruar nga Qeveria e Maqedonisë se Veriut
.....

Nënshkruar nga Qeveria e Shqipërisë
.....

Nënshkruar nga Qeveria e Serbisë
.....

ID E BALLKANIT TË HAPUR

Arkitektura e referencës teknike për zbatimin e Marrëveshjes "Ndërlidhja e skemave për identifikimin elektronik të shtetasve të Ballkanit Perëndimor"
Versioni final 2.0
Prill 2023

Përmbajtja

Parathënie

Ky dokument është përgatitur me synimin për të përcaktuar një arkitekturë teknike dhe Protokoll ndërveprimi ndërmjet sistemeve kombëtare të identifikimit elektronik të vendeve anëtare që marrin pjesë si një dokument në varësi të kontratës trepalëshe "Ndërlidhja e skemave për identifikimin elektronik të shtetasve të Ballkanit Perëndimor" (në vijim e referuar si Marrëveshja). Ai është produkt i informacionit, dokumenteve dhe konsensusit të arritur gjatë takimeve teknike të anëtarëve të grupit teknik të punës. Ai përmbledh përfundimet dhe fushëveprimin e projektit të zbatimit që do të mbështesë, por nuk kufizohet në zbatimin e nismës "Open Balkan ID number" "(Numri ID i Ballkanit të Hapur"). Parimet teknike dhe protokollet e ndërlidhjes duhet të mbështesin një shumëllojshmëri të gjerë shërbimesh qytetare nëse do të ketë baza politike dhe/ose ligjore nga përfaqësuesit përkatës.

Hyrje

Qëllimi i këtij dokumenti është të përcaktojë arkitekturën e ndërveprimit dhe protokollet teknike për të mundësuar elektronikisht autentifikimin e përdoruesve ndërkufitar të përdoruesve, duke përdorur skemat e regjistruara të identifikimit elektronik.

Anëtarët e grupit të punës të emëruar nga çdo vend shkëmbyen informacione dhe dokumente teknike në përpjekje për t'u njohur me sistemet e identifikimit elektronik dhe për t'u përpjekur të përcaktojnë arkitekturën e mundshme të ndërveprimit dhe protokollet themelore, me qëllim lidhjen e sistemeve përkatëse kombëtare të identifikimit elektronik për të mundësuar identifikimin e qytetarëve ndërkufitar, për të mbështetur iniciativën Open Balkan ID (ID e Ballkanit të Hapur) dhe për të krijuar kushtet për zgjerimin e ardhshëm të shërbimeve të ndryshme të disponueshme përmes portaleve kombëtare të shërbimeve elektronike.

Kjo arkitekturë dhe protokollet duhet të lejojnë portalet e shërbimeve të Qeverisjes Elektronike që të marrin, kërkojnë dhe përpunojnë të dhënat personale të identifikimit (në vijim të referuara si "Shërbimet") të qytetarëve të Palëve të tjera të kontratës në përputhje me ligjet kombëtare dhe me Marrëveshjen.

Pas përfundimit të fazës së analizës, pjesëmarrësit e projektit të fazës së analizës kanë përfunduar arkitekturën e përbashkët teknike dhe protokollet për të mbështetur shërbimet, siç specifikohet në këtë dokument.

Fizibiliteti teknik i dy arkitekturave të ndryshme është vlerësuar gjatë takimeve teknike.

Ky dokument nuk përcakton aktivitetet, burimet dhe skedulin e zbatimit të projektit, por fokusohet vetëm në arkitekturën teknike dhe protokollet për të krijuar një bazë për shkëmbimin e të dhënave të identitetit elektronik dhe atributeve shtesë (për shembull, numri i ID-së i Ballkanit të Hapur siç përcaktohet në Marrëveshje).

Historiku

Versioni	Data	Detaje të Ndryshimit të Versionit
1.0.0.1-Draft	16.12.2021	Dokumentacioni fillestar i hartuar nga Maqedonia e Veriut
1.0.0.2-Draft	27.12.2021	Versioni i përditësuar pas takimit teknik të harmonizimit të zhvilluar më 23.12.2021
1.0.0.3-Draft	2.2.2022	Versioni i përditësuar me informacion LOA, diagrami dhe stile të përditësuara
1.0.0.4-Draft	22.2.2022	Versioni i përditësuar me formatin e numrit OB ID, certifikatën OB ID dhe shtojcën 1
1.0.0.5-Draft	20.4.2022	Përditësime shtesë në kodin ID
1.0.0.6-Draft	5.5.2022	Versioni i përditësuar me shtesa dhe pretendime të detyrueshme – Hartëzimi i fushëveprimit
1.0.0.7-Draft	10.5.2022	Versioni i përditësuar me një shtesë (Gjinia) dhe shtojca 2
1.0.0.8- Draft	23.5.2022	Versioni i përditësuar me shtimin e barkodit në certifikatën Open Balkan ID
2.0 – Final	4.4.2023	Versioni i përditësuar me paraqitje vizuale të përditësuar të certifikatës së lëshuar me numrin e ID-së së Ballkanit të hapur dhe rregullat e maskimit të përshkrimit të parametrit të kthimit API

Arkitektura

Aksesi i qytetarëve në portalin e shërbimeve elektronike të e-Qeverisjes në secilën Palë Kontraktuese do të mundësohet përmes konfigurimit të federimeve në nivel sistemi nëpërmjet Single Sign-On (në vijim referuar si SSO).

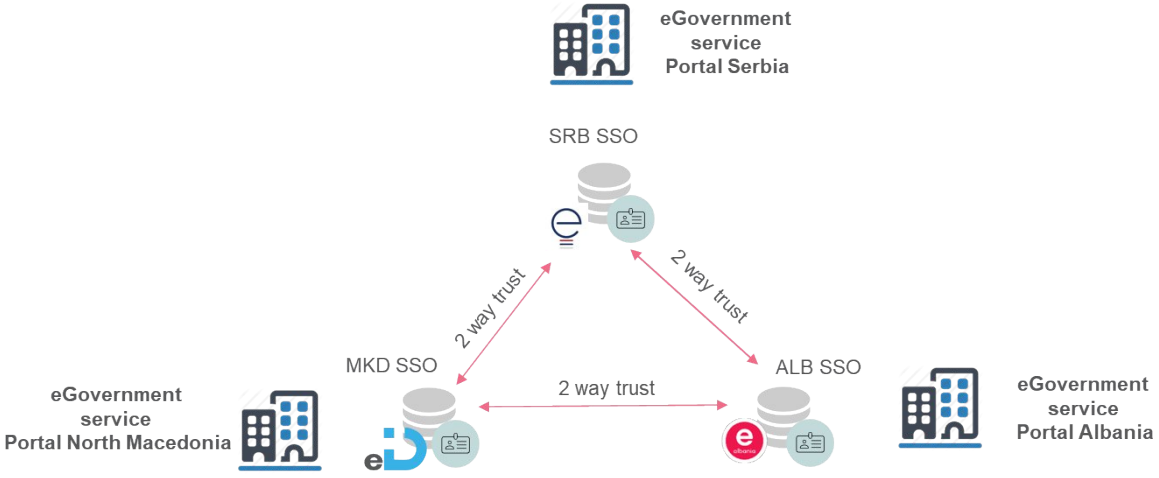


Figura 1. Architecture

SSO-ja është një shërbim përmes të cilit përdoruesit verifikohen dhe u lejohet aksesi në portalet e shërbimeve elektronike të e-Qeverisjes dhe ofruesit e tjerë të shërbimeve.

Çdo vend për momentin ka krijuar një ofrues të vetëm të identitetit online (IDP) për portalin kombëtar të shërbimeve elektronike, e-Qeverisja (Qeverisja Elektronike) dhe rekomandohet që arkitektura e identifikimit të federuar të konfigurohet për të mbështetur skenarët e autentifikimit të qytetarëve ndërkufitar.

Identifikimi i federuar lejon që autentifikimi dhe autorizimi i përdoruesit të menaxhohen nga çdo vend anëtar për qytetarët e tij, ndërsa lejon shkëmbimin e sigurt të informacionit të kërkuar për identifikimin e përdoruesit në sistemet e qeverisjes elektronike të Palëve të tjera Kontraktuese.

Një federim mund të shprehet si një marrëveshje ndërmjet Palëve Kontraktuese që i besojnë njëra-tjetrës. Në lidhjet dypalëshe mund të ketë besim të drejtpërdrejtë mes palëve. Si rrjedhojë, do të krijohen 3 lidhje dypalëshe.

Një ent në federim duhet të jetë i aftë të besojë se entitetet e tjera me të cilat po ndërvepron i përkasin të njëjtës lidhje. Ai duhet gjithashtu të jetë i aftë të besojë se informacioni që entitetet e tjera publikojnë për veten e tyre nuk janë dëmtuar gjatë transportit dhe se ai i përmbahet politikave të ndërlidhjes.

Rrjedha logjike e procesit të autentifikimit

Diagrami i mëposhtëm tregon ecurinë e autentifikimit të shtetasve të huaj në një Portal vendas të e-Qeverisjes (Qeverisja Elektronike).

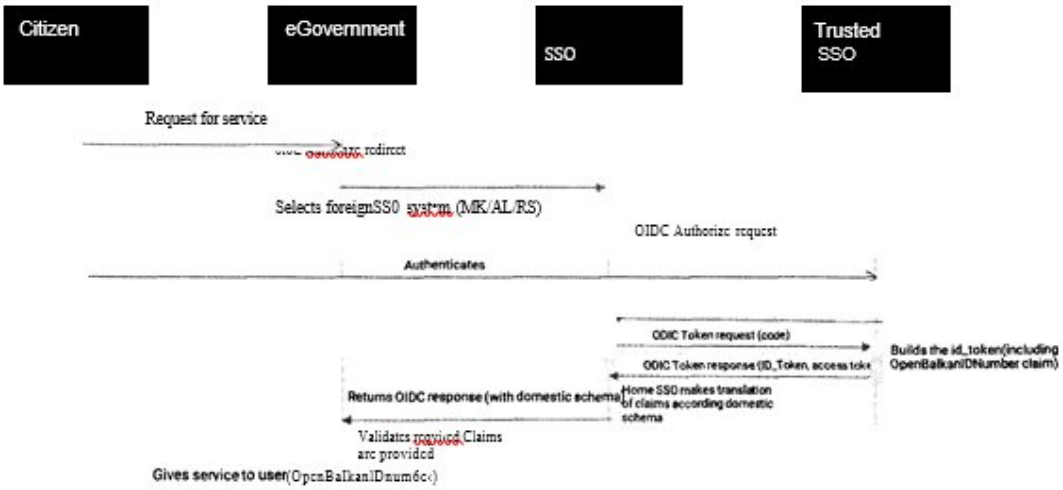


Figura 2. Rrjedha logjike e autentifikimit

Protokolli

Të gjitha sistemet SSO duhet të mbështesin autentifikimin e përdoruesit bazuar në specifikimet OpenID Connect 1.0 (OIDC) të ndërtuara në krye të specifikimit OAuth 2.0 (IETIF RFC 6749).

OpenID Connect 1.0 është një shtresë e thjeshtë identiteti në krye të protokollit OAuth 2.0. Ai u mundëson *klientëve* të verifikojnë identitetin e Përdoruesit Fundor bazuar në autentifikimin e kryer nga një Server Autorizimi, si dhe të marrin informacionin bazë të profilit për Përdoruesin Fundor në një mënyrë të ndërveprueshme dhe të ngjashme me REST.

Zinxhirët e besueshmërisë të federimit OpenID Connect 1.0 mbështeten mbi JSON Web Token (JWT) të nënshkruar në mënyrë kriptografike.

OIDC Nyjat fundore të serverit të autorizimit

Të gjitha sistemet SSO duhet të mbështesin minimalisht nyjat fundore të mëposhtme, siç përcaktohen nga standardi OIDC.

Nyjat fundore	**Përdorimi**
autorizimi_pika fundore	Ndërveproni me pronarin e burimit dhe merrni një grant autorizimi.
token_pika fundore	Merrni një shenjë aksesi dhe/ose ID, duke paraqitur një dhënie autorizimi ose token (s shenjë)_ rifreskimi.
informacion i përdoruesit_pika fundore	Kthimi i pretendimeve për përdoruesin përfundimtar të verifikuar.

Nyjat fundore	Përdorimi
përfundimi_sesionit_pika fundore	Përfundoni sesionin e lidhur me ID-në e dhënë.
jwks_uri	Pika përfundimtare e marrjes së çelësit të nënshkrimit të token (shenjës) JWT

Tabela 1. Pikat fundore të serverit të autorizimit

Të gjitha nyjat fundore në këtë faqe fillojnë me një server autorizimi, megjithatë URL-ja për atë server ndryshon në varësi të nyjës fundore dhe llojit të serverit të autorizimit. Ju keni dy lloje të serverëve të autorizimit për të zgjedhur: test dhe ambientin e prodhimit (live).

OAuth 2.0 (OIDC) autorizimi

Të gjitha sistemet SSO duhet të mbështesin rrjedhën e mëposhtme të kodit të autorizimit me lloje të shumta përgjigjesh, siç përcaktohet në protokollin OAuth 2.0.

Kërkesa për autorizim do të mbështesë llojet e mëposhtme të përgjigjeve

Identifikuesi	Përshkrimi
Kodi	Kodi i autorizimit siç specifikohet në OpenID Connect 1.0
id_token, token	Kjo është e detyrueshme pasi nyja fundore e Token (Shenjës) nuk do të përdoret për shkëmbimin e kërkesave shtesë të përcaktuara në këtë dokument.

Tabela 2. Llojet e përgjigjeve të mbështetura të rrjedhës së autorizimit

Çdo SSO do të mbështesë llojet e përgjigjeve të kombinuara, një kërkesë tipike është dhënë në shembullin më poshtë:

```
GET /authorize?
response_type=code%id_token%20token%token
&client_id=s6BhdRkqt3
&Scope= openbalkanid%20profile%20openid%20email
&redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
&state=af0ifjsldkj HTTP/1.1
 Host: server.example.com
```

Shkëmbimi i të dhënave të shtetasve

Të gjitha kërkesat për të dhënat e qytetarëve për ndërlidhjen do të ndahen përmes kërkesave të përfshira në id_token dhe të autorizuara përmes përdorimit të qëllimit përkatës.

Mund të kërkohet përkthimi i kërkesave për sistemet e SSO-ve vendase pasi sistemet e SSO-ve të secilit vend kanë specifika të ndryshme të kërkesave dhe skema të tyre.

Sistemi SSO i çdo vendi do të duhet të zbatojë përkthimin për çdo ofrues të kërkesave për të shmangur ndryshimet në sistemet ekzistuese të integruara me sistemin e tyre SSO dhe për të garantuar transparencë ndaj portaleve vendase të shërbimeve elektronike.

Kërkesat e reja për përdoruesit mund të specifikohen në mënyrë shtesë, me qëllim që përkthimi të mund të zbatohet në sistemet vendase të SSO-ve.

Qëllimet

Klientët e OpenID Connect përdorin vlerat e fushës së veprimit, siç përcaktohen në 3.3 të OAuth 2.0 [RFC6749] për të specifikuar se cilat privilegje aksesi kërkohen për Token-et (Shenjat) e Aksesit. Fushat e lidhura me Token-et (Shenjat) e Aksesit përcaktojnë grupe specifike informacioni që do të vihen në dispozicion si kërkesa/vlera.

Të tria sistemet duhet që minimalisht të mbështesin dhe t'i japin njëri-tjetrit akses në fushat e mëposhtme:

Fusha e veprimit	Përshkrimi
openid	Fusha e detyrueshme për marrjen e token të ID-së.
profile	Kërkesat/vlerat e mbuluara nga ky fushëveprim si pjesë e id_token, janë Kërkesat/vlerat përcaktohen në seksionin e hartës së fushës së kërkesave.
email	Këkesa/vlera e mbuluar nga kjo fushë si pjesë e id_token është vullnetare, por çdo sistem SSO duhet të mbështesë ofrimin e email-it dhe/oremail_verified. Çdo vend duhet të specifikojë disponueshmërinë dhe politikën e lidhur me këto të dhëna.
openbalkanid	Kërkesat/vlerat e mbuluara nga kjo fushëveprimi si pjesë e id_token
pidn	Fusha e përdorur për të menaxhuar shkëmbimin e numrave unikë të qytetarit si pjesë e

Fusha e veprimit	Përshkrimi
	kodit ID
Dateofbirth	Fusha e përdorur për të menaxhuar kërkesën e datës së lindjes si pjesë e kodit ID

Tabela 3. Fushat e detyrueshme të veprimit

Është rënë dakord që të dhënat e kërkuara duhet të përfshihen në id_token siç specifikohet në specifikimin OIDC 1.0. Token ID përfaqësohet si një JSON Web Token (JWT). Nuk është e detyrueshme që nyjat fundore standarde userinfo_endpoint të përmbajë kërkesa shtesë të përcaktuara nga shtrirja e zgjeruar (Openbalkanid Scope).

Pretendimet – Hartëzimi i fushës së veprimit

Çdo vend duhet të japë informacion minimal për kërkesat e mëposhtme të shkëmbyera si pjesë e id_token.

Kërkesa	Përshkrimi	URI	Qëllimi	
First Name	Emri	Të specifikohet nga secili vend	*profili, openbalkanid*	
Last Name	Mbiemri	Të specifikohet nga secili vend	*profili, openbalkanid*	
Gender	Gjinia	Të specifikohet nga secili vend	*profili, openbalkanid*	
E-mail	Emaili i konfirmuar	Të specifikohet nga secili vend	*profili, openbalkanid*	
Country	2 gërma nga kodi i shtetit "MK", "AL", "RS"	Të specifikohet nga secili vend	*openbalkanid*	
loa	Niveli i sigurisë siç përcaktohet në ligjet kombëtare të identifikimit elektronik. Vlerat e mundshme "ANONIM", "I ULËT", "THELBËSOR", "I LARTË"	Të specifikohet nga secili vend	*openbalkanid*	
obid	Siç parashikohet në seksionin OpenBalkanID Number.	Të specifikohet nga secili vend	*openbalkanid*	
Numri Unik	Numri unik	Të specifikohet nga secili vend	*pidn*	
Date of birth	Datëlindja	Të specifikohet nga secili vend	*datëlindja*	

Tabela 4. Hartëzimi i pretendimeve/fushës së veprimit

Në rast se emri dhe mbiemri janë në alfabetin e brendshëm, secila palë do të përdorë standardin ICAO Doc 9303 në kërkesat e shkëmbyera:
https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

ID e Ballkanit të Hapur

Çdo shtet anëtar do të zbatojë procesin e tij për lëshimin e numrit të ID-së së Ballkanit të Hapur në portalin e Qeverisjes Elektronike, në mënyrë që të mbështesë shkëmbimin e tij mbi protokollin e rënë dakord.

Autoritetet përgjegjëse për lëshimin e ID-së së Ballkanit të Hapur në Palët Kontraktuese, janë:

- Zyra për Teknologji Informative dhe Qeverisje Elektronike në Republikën e Serbisë;
- Ministria e Shoqërisë së Informacionit dhe Administratës në Republikën e Maqedonisë së Veriut;
- Drejtoria e Përgjithshme e Gjendjes Civile në Republikën e Shqipërisë.

Një qytetar që merr numrin e identifikimit të Ballkanit të Hapur në portalin e tij/saj kombëtar të Qeverisjes elektronike, merr një certifikatë elektronike ID të Ballkanit të Hapur që përmban të dhëna personale. Të dhënat brenda certifikatës dhe formatit të Open Balkan ID janë specifikuar në shtojcën 1 të këtij dokumenti. Emri i rënë dakord i kërkesës është "bid" dhe duhet të jepet brenda id_token kur bëhet kërkesa për autorizim që përmban fushat e openbalkanid.

Formati i prefiksit të kodit të vendit me 2 numra + 11 numra:

Republika e Serbisë – 81 XXXXXXXXXXX

Maqedonia e Veriut – 89 XXXXXXXXXXX

Republika e Shqipërisë – 55 XXXXXXXXXXX

Algoritmi që do të përdoret për gjenerimin dhe verifikimin e numrave OBID është algoritmi Luhn: https://en.wikipedia.org/wiki/Luhn_algorithm, duke përjashtuar kodin e shtetit (2 shifrat e para nuk janë pjesë e kontrollit).

Secila Palë duhet të sigurojë ndërfaqe për dy Palët e tjera për vërtetimin e certifikatave të ID-së së Ballkanit të Hapur, të lëshuara. Specifikimi i ndërfaqes do të dakordësohet si shtesë gjatë zbatimit.

Protokolli për kontrollin e obid dhe marrjen e informacionit shtesë të kërkuar nga ofruesit e shërbimeve (shembull: Ministria e Brendshme për lëshimin e numrit unik të shtetasit për të huajt) do të specifikohet shtesë.

Niveli i sigurisë

Niveli i sigurisë është një faktor i rëndësishëm në sistem dhe shpeshherë ka mospërputhje në interpretimin, zbatimin dhe disponueshmërinë e sistemeve që e mbështesin atë midis vendeve pjesëmarrëse.

Përkufizimi i nivelit të pranueshëm të sigurisë nuk i nënshtrohet përkufizimit në këtë Dokument. Niveli i sigurisë do të përfaqësohet si vlerë e vetme me vlerat e mëposhtme.

- ANONIM
- I ULËT
- THELBËSOR
- I LARTË

Informacioni në nivel teknik do të shkëmbehet si pjesë e id_token kur bëhet një kërkesë me *openbalkanid* Scope. Emri i kërkesës është pranuar të jetë "loa".

Duke qenë se niveli i sigurisë është i garantuar (si rrjedhojë, i besuar) nga sistemet kombëtare të SSO-së, informacionet shtesë mbi politikën për çdo nivel do të shkëmbehen dhe dakordësohet ndërmjet vendeve. Nuk ka mundësi teknike për automatizimi për validimin teknik të kuptimit aktual të këtyre niveleve. Si rrjedhojë, protokolli teknik për ndërlidhje do të ketë vetëm mjete teknike për shkëmbimin e këtij informacioni.

Nivelet e sigurisë së Republikës së Shqipërisë

Niveli	**Përshkrimi i politikave**
ANONIM	*E pazbatueshme*
I ULËT	*E pazbatueshme*
SUBSTANCIAL	*Përdoruesit identifikohen me emrin e përdoruesit dhe fjalëkalimin.* *Në procesin e regjistrimit, të dhënat e ofruara kontrollohen në kohë reale me gjendjen civile kombëtare për qytetarët dhe regjistrin tregtar për bizneset. Përdoruesit duhet të plotësojnë të dhëna specifike të njohura vetëm prej tyre dhe gjithashtu pajisen me një kod 4 shifror përmes sms-ve dhe linkut të aktivizimit të dërguar përmes postës elektronike e-mail.*
I LARTË	*Përdoruesit identifikohen me certifikatë dixhitale*

Tabela 5. Niveli i politikës së sigurimit në Shqipëri

Referencat e rregullores

https://cesk.gov.al/wp-content/uploads/2016/04/ligji107.pdf

Nivelet e sigurisë në Maqedoninë e Veriut

Niveli	**Përshkrimi i politikave**
ANONIM	*Online me adresë të vlefshme e-maili* *Përdoruesit identifikohen me adresë të vlefshme e-maili.* *Për krijimin e profilit bazë të përdoruesit, psh. regjistrimi dhe vërtetimi i përdoruesit të eID-së në nivel anonim sigurie, përdoruesit i nevojitet vetëm një adresë e vlefshme e-maili. Në formularin e regjistrimit, përdoruesi regjistron e-mail dhe fjalëkalim të vlefshëm, si dhe konfirmimin e fjalëkalimit. Pas këtij procesi një e-mail dërgohet në adresën e postës elektronike të kërkuar për qëllime verifikimi dhe regjistrimi në nivel anonim sigurie.* *Duke u regjistruar me sukses vetëm me adresë e-maili, krijohet profili bazë i përdoruesit dhe mund të përdoret për aplikim për shërbime elektronike që nuk kërkojnë verifikim dhe vërtetim të identitetit të përdoruesit.* *Pasja e një profili bazë përdoruesi do të thotë se identiteti fizik i përdoruesit nuk konfirmohet dhe verifikohet gjatë procesit të regjistrimit. Procesi i regjistrimit verifikon vetëm që një përdorues ka akses në adresën e dhënë të postës elektronike.* *Me profilin bazë të përdoruesit, përdoruesi mund të aplikojë për shërbime elektronike për të cilat nuk kërkohet identiteti i aplikantit.* *Hyrja me profilin bazë të përdoruesit kërkon vërtetim me emrin e përdoruesit dhe fjalëkalimin.*

Niveli	Përshkrimi i politikave
I ULËT	*Pajisja me emrin e përdoruesit ekzistues nga PRO* *Tatimpagues i regjistruar, i verifikuar dhe i vërtetuar* *Nëse një person fizik ka një llogari përdoruesi aktiv në regjistrin e tatimpaguesve të zyrës së të ardhurave publike, ai person mund të regjistrohet në Portalin e Shërbimeve me nivel të ulët sigurie me atë llogari. Në formularin e regjistrimit, përdoruesi shënon të njëjtin emër përdoruesi dhe fjalëkalim që është përdorur për regjistrim në regjistrin e tatimpaguesve PRO. Nëse të dhënat e regjistrit PRO janë të sakta dhe nëse SIN-i i përdoruesve nga PRO ekziston në Regjistrin Qendror të Popullsisë (CPR), ai profil përdoruesi në ZSHS krijohet automatikisht dhe regjistrohet në Portalin e Shërbimeve Elektronike. Duke u regjistruar me sukses në llogarinë e përdoruesit PRO, eID krijohet me nivel të ulët sigurie. Me këtë Lloj të Eid-së, përdoruesi mund të aplikojë për shërbime elektronike të nivelit të ulët.* *Nëse përdoruesi ka një certifikatë të kualifikuar për nënshkrimin elektronik të lëshuar nga një ofrues i regjistruar i kualifikuar i shërbimit të besimit, përdoruesi mund të përmirësojë certifikatën e tij eID të nivelit të ulët në eID të nivelit të lartë.* *Pasja e një Eid-je të nivelit të ulët do të thotë që identiteti fizik i përdoruesit është konfirmuar dhe verifikuar gjatë procesit të regjistrimit, ku ai/ajo ka qenë personalisht i pranishëm gjatë procesit të regjistrimit, ka treguar një dokument të vlefshëm identifikimi personal dhe të dhënat e tij/saj të disponueshme në Popullsinë Qendrore. Regjistri (CPR) është konfirmuar dhe regjistruar shtesë. eID në nivel të lartë sigurie krijohet bazuar në identitetin fizik të konfirmuar.* *Hyrja me Eid (elektronik)të nivelit të ulët kërkon vërtetim me emrin e përdoruesve dhe fjalëkalimin. Niveli i besueshmërisë së një identifikimi të tillë është i ulët, sepse ekziston një nivel i caktuar i mundësisë për të zbuluar emrin e përdoruesit dhe fjalëkalimin.*
SUBSTANCIAL	*E pazbatushme*
I LARTË	*Pajisja me certifikatë të kualifikuar për nënshkrim elektronik të lëshuar nga një ofrues i regjistruar i kualifikuar i shërbimit të besimit.* *Nëse një person fizik ka një certifikatë të vlefshme të kualifikuar për nënshkrimin elektronik të lëshuar nga një ofrues i kualifikuar i shërbimit të besimit, i regjistruar në Regjistrin e ofruesve të shërbimeve të besimit dhe skemave të identifikimit elektronik, përdoruesi mund të regjistrohet në distancë për eID në nivel të lartë sigurie. Në formularin e regjistrimit, përdoruesi shënon SIN-in e tij për të cilin lëshohet certifikata, adresën e postës elektronike që do të përdoret më tej si emër përdoruesi i hyrjes në SSO dhe fjalëkalimin. ZSHS verifikon lëshuesin e certifikatës së përzgjedhur të kualifikuar për nënshkrim elektronik, për të verifikuar lidhjen ndërmjet certifikatës dhe SIN-it të regjistruar. Nëse lëshuesi i certifikatës konfirmon se certifikata dhe SIN janë të lidhura, SSO verifikon nëse SIN-i i dhënë ekziston në Regjistrin Qendror të Popullsisë (CPR). Pas përfundimit të suksesshëm të të dy proceseve të verifikimit, krijohet profili i përdoruesit të ZSHS-së, ku një e-mail verifikimi në adresën e-mail jepet gjatë procesit të regjistrimit.* *Llogaria e përdoruesit të SSO-së aktivizohet me një klikim të vetëm në lidhjen e dhënë në e-mail. Duke u regjistruar me sukses me certifikatë të kualifikuar për nënshkrim elektronik, krijohet eID me nivel të lartë sigurie që mund të përdoret për të aplikuar online për të gjitha shërbimet elektronike të disponueshme në Portal.* Pasja një eID -je të nivelit të lartë do të thotë që të gjitha kërkesat për krijimin e ID-së së nivelit të ulët janë plotësuar gjatë procesit të regjistrimit dhe se një certifikatë dixhitale e vlefshme është siguruar gjatë procesit të regjistrimit, e lëshuar nga lëshuesi i certifikatës, i regjistruar në Regjistrin e Lëshuesve të Certifikatave në Republikën e Maqedonisë së Veriut (Regjistri i lëshuesve të certifikatave). Hyrja me eID të nivelit të lartë kërkon vërtetim me anë të certifikatës së nënshkrimit dixhital. Niveli i besueshmërisë së një identifikimi të tillë konsiderohet i lartë, sepse kërkon zotërimin e mesatares së eID-së dhe kodit PIN, ku mundësia që dikush tjetër të regjistrohet me atë eID është dukshëm më e ulët. Nëse ai/ajo është regjistruar me eID të nivelit të lartë, përdoruesi mund të identifikohet edhe me eID të nivelit të ulët, pa certifikatë dixhitale.

Tabela 6. Niveli i politikës së sigurimit të Maqedonisë së Veriut

Niveli i sigurisë së skemës së identifikimit elektronik përcaktohet në varësi, të:

- nivelit të sigurimit të hyrjes dhe regjistrimit të subjektit të identifikimit elektronik;
- nivelit të sigurimit të vërtetimit të identitetit dhe verifikimit të personave fizikë.

Referencat e rregullores

1. https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/pravilnik_identitet.pdf
2. https://uslugi.gov.mk/register.nspx
3. https://uslugi.gov.mk/e-id.nspx
4. https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/pravilnik_tom_shemi.pdf
5. https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronski_dokumenti_eid_i_doverlivi_uslugi.pdf
6. https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_elektronsko_upravuvanje_i_elektronski_uslugi_0.pdf

Nivelet e sigurisë së Republikës së Serbisë

Niveli	**Përshkrimi i politikave**
ANONIM	*E pazbatueshme*
I ULËT	*Përdoruesit identifikohen me emrin e përdoruesit dhe fjalëkalimin.* *Në procesin e regjistrimit, pas plotësimit të formularit të regjistrimit në internet, përdoruesi merr një email verifikimi për të konfirmuar hyrjen në adresën e emailit të dhenë. Nëse regjistrimi bëhet online pas konfirmimit të adresës së emailit, regjistrimi shqyrtohet nga personeli i autorizuar në Zyrën për IT dhe eGovernment dhe të dhënat kontrollohen në regjistrat zyrtarë brenda 48 orëve. Nëse regjistrimi bëhet në sportel (më shumë se 1000+ lokacione), personi i autorizuar regjistron llogarinë e përdoruesit në kontakt të drejtpërdrejtë, konfirmon identitetin e personit duke rishikuar kartën e identitetit ose pasaportën e tij/saj dhe kontrollon të dhënat në regjistrat zyrtarë.*
SUBSTANCIAL	*E pazbatueshme*
I LARTË	*Përdoruesit identifikohen me vërtetim me dy faktorë.* *Përdoruesit mund të përditësojnë aksesin në llogarinë e tyre nga emri i përdoruesit dhe fjalëkalimi në vërtetimin me dy faktorë, duke përdorur pajisjen e tyre celulare (telefon inteligjent ose tablet). Aplikacioni celular emërtohet ConsentID dhe parametrat e aktivizimit i jepen përdoruesit në kontakt të drejtpërdrejtë nga personi i autorizuar në një nga 1000+ vendndodhjet, me kusht që përdoruesi të ketë kartë identiteti ose pasaportë të vlefshme për qëllime identifikimi. Përdoruesi duhet të nënshkruajë një letër për të konfirmuar se ka marrë parametrat e aktivizimit.* *Përdoruesit identifikohen me certifikatë dixhitale të kualifikuar.*

Tabela 7. Niveli i politikës së sigurimit të Serbisë

Referencat e rregullores

1. https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2017/94/4/reg
2. http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/uredba/2018/60/1/reg
3. https://epotpis.mtt.gov.rs/registar-pruzalaca-usluga-elektronske-identifikacije-i-sema-elektronske-identifikacije/
4. https://epotpis.mtt.gov.rs/wp-content/uploads/2021/07/kanc.pdf

Ndryshimet në sistemet SSO

Secili vend si pjesë e federimit të besuar të implementuar do të zbatojë një përzgjedhje të qartë të përdoruesit të ofruesit të identitetit në faqen e autentifikimit/autorizimit të përdoruesit, duke shtuar lidhje ridrejtimi (Shembull: në faqen e autorizimit të MK ZSHS, lidhjet e ridrejtimit në ZSHS-në shqiptare dhe SSO-në serbe do të jenë shtuar) në mënyrë që përdoruesit të mund të përfundojnë procesin e autentifikimit.

Çdo vend si pjesë e federimit të besuar të implementuar do të zbatojë Përkthimin e kërkesës së SSO-së së huaj, llojet e kërkesave në kërkesat e vendosura vendase.

Marrja e aksesit në OAuth 2.0

Mjediset

Çdo anëtar duhet të sigurojë akses dhe informacion për përdorim për një fazë ku mund të kryhet testimi i integrimit. Aksesi në këtë mjedis duhet të jetë i disponueshme gjatë gjithë kohës së zbatimit të shërbimeve, si dhe për sa kohë ka një Marrëveshje të vlefshme për ofrimin e shërbimeve.

Gjithashtu, aksesi në nyjat fundore të ambientit të prodhimit (live) do të sigurohet pasi të kryhet një test i suksesshëm dhe të nënshkruhet nga anëtarët pjesëmarrës.

Qasja në çdo pikë përfundimtare jepet duke ndarë ID-në e klientit OAuth2 dhe sekretin e klientit dhe URL-në në mjedisin përkatës që përputhet me specifikimet në këtë Dokument.

Nyjat fundore të konfigurimit të SSO-së

Konfigurimi për mjedisin e ambientit të prodhimit (live) të ID OIDC ofrohet në:

Vendi	**Ndërfaqet e konfiguruara OIDC**	**Lloji**
Shqipëria	https://e-albania.gov.al/.well-known/openid-configuration	Ambienti i prodhimit (Live)
Republika e Maqedonisë së Veriut	https://eid.mk/.well-known/openid-configuration	Ambienti i prodhimit (Live)
Republika e Serbisë	https://prijava.eid.gov.rs/oauth2/oidcdiscovery/.well-known/openid-configuration	Ambienti i prodhimit (Live)

Tabela 8. Ndërfaqet e konfiguruara

Çdo vend do të japë detaje të nyjave fundore të fazës gjatë procesit të zhvillimit të sistemit

Testimi i integrimit

Lidhja e integrimit e bazuar në federimin e besuar të krijuar në protokollin OIDC mund të testohet në nivel dypalësh dhe nuk ka nevojë për një proces të përbashkët testimi shumëpalësh. Pasi vendet të nënshkruajnë protokollin dypalësh të pranimit, mund të sigurohet qasja në pikat përfundimtare të prodhimit. Megjithatë, data e saktë për aktivizimin e shërbimeve do të përcaktohet nga Palët e Marrëveshjes.

Pasi ekipi i mbështetjes ID të marrë këtë informacion, një konfigurim në serverët e ID-së do të ekzekutohet dhe kredencialet e OAuth 2.0 (ID-ja e klientit, sekreti i klientit) do të shkëmbehen me personin e kontaktit.

Kërkesa për akses

Për të konfiguruar federimin e besuar, Palët do të shkëmbejnë të paktën informacionin e mëposhtëm dhe do ta përditësojnë këtë informacion nëse ndryshohet, në mënyrë që proceset e mbështetjes dhe mirëmbajtjes të mund të mbahen.

Informacioni	**Përshkrimi**
Emri i organizatës	Emri i Agjencisë Qeveritare që do të prezantohet gjatë procesit të autorizimit të përdoruesit në sistemin e SSO-së. (Republika e Maqedonisë së Veriut, Republika e Serbisë, Shqipëria)
Emri i personit të kontaktit	Emri, Mbiemri i personit kryesor të kontaktit në lidhje me mirëmbajtjen dhe mbështetjen e federatës SSO.
Adresa e-mailit e personit të kontaktit	Adresa e postës elektronike e personit kryesor të kontaktit, përgjegjës për mirëmbajtjen dhe mbështetjen e federatës SSO.
Emri i aplikimit	Emri i aplikacionit të palës së tretë, shembull ("euprava.gov.rs", "e-Albania.al","uslugi.gov.mk"…) në varësi të aftësive të verifikimit të SSO, mund të paraqitet gjatë rrjedhës së autorizimit të përdoruesit.
URL-ja e kthimit të thirrjes OAuth 2.0	Ktheni të dhënat meta të OAuth 2.0 në lidhje me serverin e autorizimit të specifikuar.
Lidhja e politikës së privatësisë së aplikacionit	Kjo lidhje është e detyrueshme për shkak të pajtueshmërisë me rregulloren e mbrojtjes së të dhënave (GDPR dhe të tjera kur është e zbatueshme). Duhet të hapet në lidhjen e arritshme publike HTTPS dhe të mbrohet nga certifikata SSL e lëshuar për organizatën.
Ikona e aplikacionit	Ikona e aplikacionit në formatin jpg, png me rezolucion minimal 200x200 piksele në raport 1:1. Duhet t'i tregohet përdoruesit gjatë skenarëve të uebit të autentifikimit/autorizimit të përdoruesit fundor.

Tabela 9. Informacioni i kërkuar i konfigurimit

Referencat

1. OpenID Connect 1.0 Final: OpenID Connect Core 1.0 që përfshin grupin e gabimeve 1
2. Korniza e autorizimit OAuth 2.0 https://datatracker.ietf.org/doc/html/rfc6749

3. Identitetet elektronike – një hyrje e shkurtër, https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf,

4. Bibliotekat, Produktet dhe Mjetet e OpenID, https://openid.net/developers/libraries/,

5. Rrjedha e kodit të autorizimit me çelësin e provës për shkëmbimin e kodit (PKCE), https://auth0.com/docs/flows/authorization-code-flow-with-proof-key-for-code-exchange-pkce.

SHTOJCA 1
CERTIFIKATA E LËSHUAR ME NUMËR ID TË BALLKANIT TË HAPUR

Të dhënat personale dhe të dhëna të tjera që do të paraqiten në certifikatën e lëshuar me numër ID të Ballkanit të Hapur, janë si më poshtë (në 4 gjuhë):

Informacioni	**Përshkrimi**
Mbiemri dhe emri	Emri dhe Mbiemri në formatin ndërkombëtar ICAO siç janë të pranishëm në dokumentin personal të identifikimit.
Data e lindjes	Data e lindjes (dd.mm.vvvv)
Vendi i shtetësisë	Lëshuar nga shteti (Shqipëria, Republika e Serbisë, Republika e Maqedonisë së Veriut)
Numri unik i ID-së së brendshme	Numri unik i brendshëm (13 shifra)
Numri i ID-së të Ballkanit të Hapur	Numri i ID-së së Ballkanit të Hapur në formatin e rënë dakord
Data dhe ora e marrjes së numrit të ID të të Ballkanit të Hapur	Data dhe ora e lëshimit të certifikatës në formatin dd.mm.vvvv h24:min.
Email	Adresa e emailit e barabartë me emrin e përdoruesit të marrë në ID_token.
Autoriteti lëshues dhe vula elektronike	Autoriteti përgjegjës për lëshimin e ID-së së Ballkanit të Hapur në Palën Kontraktuese, siç përcaktohet në rubrikën Numri i ID-së së Ballkanit të Hapur
Kodi QR	Kodi QR që përmban lidhjen e përhershme në faqen e internetit ku mund të konfirmohet vlefshmëria e certifikatës së numrit të ID-së së Hapur të Ballkanit
Barkodi	Barkodi (kodi 128 auto) që përmban numrin ID të Ballkanit të Hapur

Certifikata në vetvete përmban dy shënime ligjore në fund të faqes:

Shënimi i parë: miratimi lëshohet si dokument elektronik dhe versioni i printuar përfaqëson një kopje të këtij dokumenti.

Shënimi i dytë: miratimi është i vlefshëm bashkëshoqëruar me dokument personal përkatës që vërteton identitetin e personit.

Më poshtë jepet paraqitja vizuale e certifikatës (formati A4):

SHTOJCA 2

Secila palë kontraktuese është përgjegjëse për lëshimin e numrit të ID-së të Ballkanit të Hapur (OBID) për qytetarët e vet dhe për të ofruar shërbimin online për verifikimin e numrit të ID-së të Ballkanit të Hapur. Pjesë e procesit të verifikimit është leximi i kodit QR i cili gjendet në Certifikatën e lëshuar me numrin e ID-së të Ballkanit të Hapur (shihni shtojcën 1).

Shtojca 2 përshkruan përmbajtjen dhe procedurat për leximin e kodit QR dhe verifikimin e specifikimit të shërbimit OBID.

Kodi QR në certifikatën e numrit ID të Ballkanit të Hapur

Përmbajtja e kodit QR

Përmbajtja e kodit QR (informacioni që ai mban) duhet të jetë një lidhje e përhershme në ndërfaqen ku mund të konfirmohet vlefshmëria e kodit QR dhe certifikatës së numrit të ID-së të Ballkanit të Hapur. Lidhja e përhershme duhet të përbëhet nga adresa e faqes së internetit e cila ka të njëjtën vlerë për të gjithë përdoruesit dhe kodin unik që lidhet me përdoruesin:

https://<web page URL>/<user code>

Shembull: https://eid.gov.xy/ob/qr/S8KSCWMDEJTUXKWIEK,
ku **S8KSCWMDEJTUXKWIEK** është kodi i përdoruesit.

Kodi i përdoruesit përfaqëson vargun e karaktereve ASCII me gjatësi arbitrare nga i cili nuk mund të përcaktohet asnjë nga të dhënat e përdoruesit. Metoda për krijimin e kodit të përdoruesit përcaktohet nga secila palë.

Procesi i leximit të Kodit QR

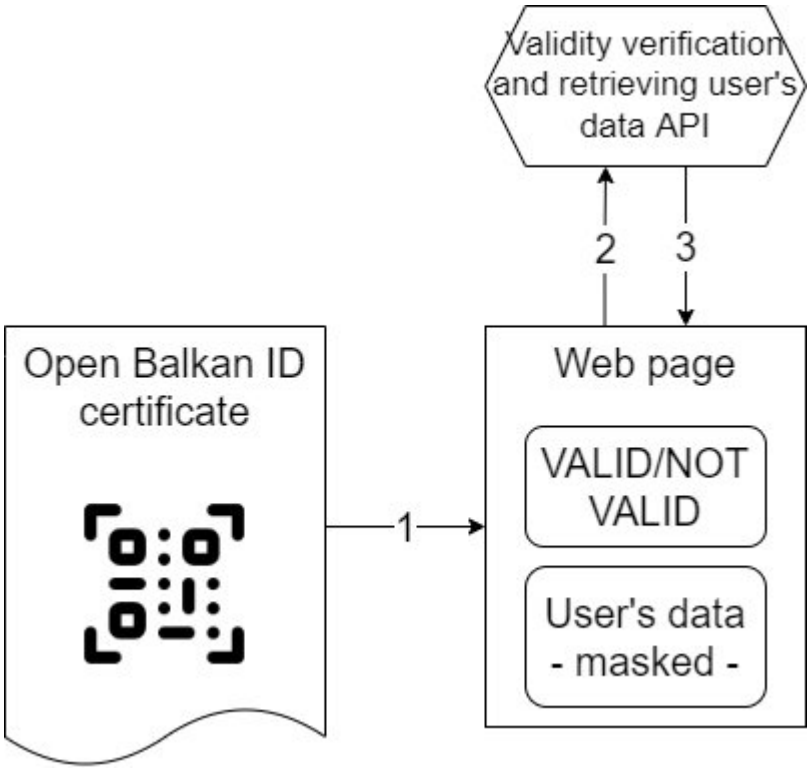
Kur skanohet kodi QR, duhet të jepet informacioni i mëposhtëm:

- informacion nëse kodi QR është i vlefshëm apo jo;
- të dhënat e përdoruesit (të plota ose të maskuara), në mënyrë që shikuesi të mund të krahasojë të dhënat nga dokumenti dhe nga sistemi.

Secila palë do të ofrojë shërbimin për të vërtetuar kodin QR dhe për të marrë të dhënat e përdoruesit. Ekzistojnë dy variante të procedurës për të vërtetuar kodin QR dhe për të shfaqur të dhënat e përdoruesit, midis të cilave secila Palë Kontraktuese do të zgjedhë një për të përdorur.

Shfaqja me një hap e të dhënave të përdoruesit

Procedura me një hap konsiston në shfaqjen e të dhënave të përdoruesit në faqen e parë të internetit pas skanimit të kodit QR. Procedura është paraqitur në diagramin më poshtë:



Diagrami 1. Shfaqja e të dhënave të përdoruesit me një hap

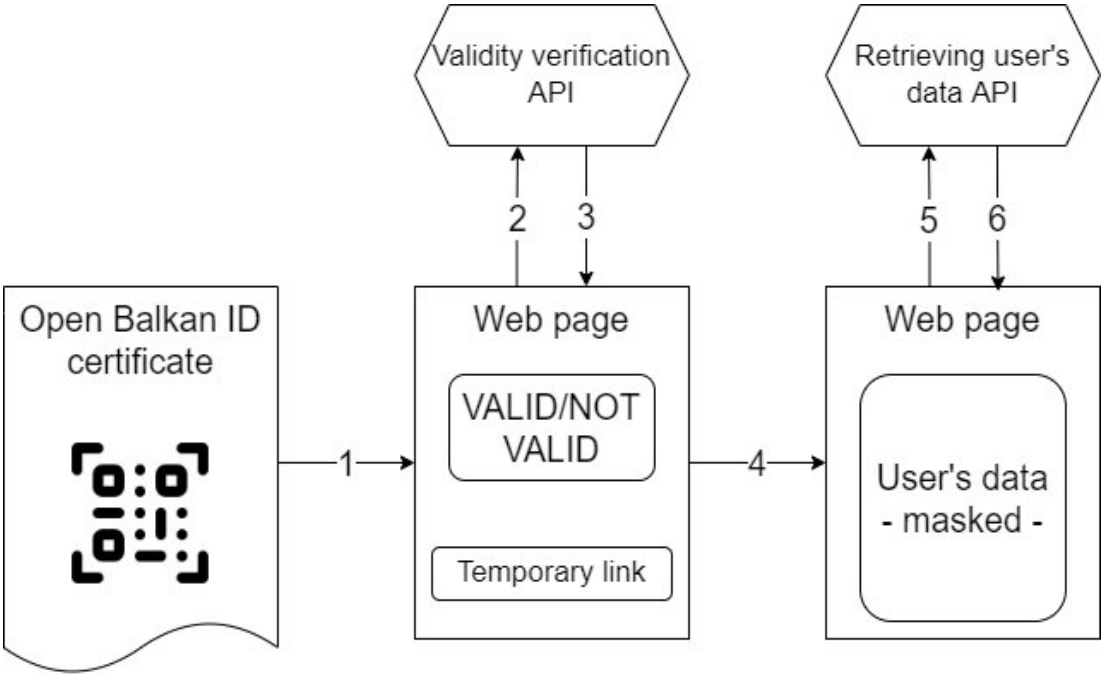
Kur kodi QR skanohet dhe klikohet lidhja e tij, aplikacioni web i hapur: (1) duhet të kërkojë "Verifikimin e vlefshmërisë dhe rikthimin e të dhënave të përdoruesit API"; (2) për të marrë informacion nëse ID e Ballkanit të Hapur është e vlefshme dhe për të marrë të dhënat e përdoruesit që mund të shfaqen në ndërfaqe. Të dhënat e përdoruesit të shfaqura në ndërfaqe mund të jenë të maskuara ose në formatin origjinal. Të dhënat e maskuara do të thotë që të dhënat sensitive shfaqen pjesërisht, për shembull shfaqen shkronjat e para dhe karakteret me yll* në vend të shkronjave të tjera. Nëse të dhënat e përdoruesit duhet të maskohen apo jo, do të vendoset nga fakti nëse është përdoruesi i vërtetuar që po skanon QR apo jo. Përdoruesit e verifikuar si institucionet zyrtare, janë të autorizuar që të shikojnë të dhëna sensitive.

Dy hapa që shfaqin të dhënat e përdoruesit

Procedura me dy hapa konsiston në shfaqjen e informacionit nëse kodi QR është i vlefshëm ose jo në faqen e parë të internetit pas skanimit të kodit QR dhe shfaqjes së të dhënave të

përdoruesit në ndërfaqen e dytë të thirrur pasi klikoni në një lidhje të përkohshme në faqen e parë.

Procesi i leximit të kodit QR tregohet në diagramin më poshtë:



Diagrami 2. Të dhënat e përdoruesit që shfaqin dy hapa

Kur kodi QR skanohet dhe klikohet lidhja e tij, aplikacioni ueb i kërkuar: (1) duhet të kërkojë "API-në e verifikimit të vlefshmërisë"; (2) për të marrë informacion nëse ID-ja e Ballkanit të Hapur është e vlefshme. API-ja përcakton ID-në e Ballkanit të Hapur nga kodi i përdoruesit i cili dërgohet si parametër.

Në përgjigjen e API-t (3), aplikacioni në internet do të marrë informacion nëse kodi QR dhe numri i tij ID i Ballkanit të Hapur është i vlefshëm apo jo. Nëse është e vlefshme, API do të kthejë gjithashtu kodin unik për qasje të përkohshme në të dhënat e përdoruesit. Faqja e internetit duhet të shfaqë informacione rreth vlefshmërisë dhe një lidhje të përkohshme për shikimin e të dhënave të përdoruesit. Lidhja e përkohshme duhet të jetë e vlefshme për 5 minuta. Kjo lidhje duhet të përbëhet nga adresa e faqes së internetit e cila do të tregojë të dhënat e përdoruesit dhe kodin e përkohshëm të marrë nga API:

https://<web page URL>/<temporary code>

Shembull: https://eid.gov.xy/ob/qr-data/D8F30FKE83S2

Arsyeja për të pasur kod të përkohshëm dhe rrjedhimisht lidhje të përkohshme është për të parandaluar hapjen e faqes së internetit të të dhënave të përdoruesit nga të dhënat e ruajtura dhe të indeksuara nga motorët e kërkimit. Lidhja për shikimin e të dhënave të përdoruesit do të jetë e vlefshme për vetëm disa minuta dhe nuk mund të përdoret më vonë. Sa herë që skanohet kodi QR i një përdoruesi, duhet të paraqitet një lidhje e re për shikimin e të dhënave. Gjenerimi i kodit të ri të përkohshëm nuk anulon vlefshmërinë e kodeve të përkohshme të krijuara më parë dhe ende aktive për të njëjtin përdorues. Kjo do të thotë që çdo kod është aktiv për 5 minuta dhe mund të ketë shumë lidhje të përkohshme aktive për një përdorues.

Kur klikohet lidhja e përkohshme, faqja e kërkuar në internet (4) duhet të shfaqë "Rikuperimi i të dhënave të përdoruesit API" (5) për të marrë të dhënat e përdoruesit. API verifikon kodin e përkohshëm i cili dërgohet si parametër. Nëse është e vlefshme, API kthen të dhënat e përdoruesit të cilat mund të maskohen ose jo (6).

Pas marrjes së përgjigjes nga API, faqja e internetit do të shfaqë të dhënat e maskuara të përdoruesit për t'u kontrolluar nga një person nëse të dhënat në certifikatë përputhen me të dhënat e shfaqura në faqen e internetit.

Specifikimi i ndërfaqes së programimit të aplikacionit

Secila palë duhet të përcaktojë pikat përfundimtare të ndërfaqes së Programimit të Aplikimit (API) në vijim:

1. verifikoni vlefshmërinë – kthen nëse kodi i dhënë është i vlefshëm apo jo
2. merrni të dhënat e përdoruesit – nxjerr të dhënat e përdoruesit

verifikon-vlefshmërinë

Parametri hyrës	**Përshkrimi**	**Lloji**	**Vlerat e mundshme**
code	Kodi unik i përdoruesit	string (varg)	
code_type	Lloji i kodit të përdoruesit	string	Kodi_qr obid pidn (numri unik i qytetarit)

Parametri i kthimit	**Përshkrimi**	**Lloji**	**Vlerat e mundshme**
valid	Informacion nëse kodi i përdoruesit është i vlefshëm apo jo	bolean	E vërtetë E gabuar
temp_code	Kodi i përkohshëm që mund të përdoret për të marrë të dhënat e përdoruesit për një kohë të kufizuar	string	

marr-të dhëna-përdoruesi

Parametri hyrës	Përshkrimi	Lloji	Vlerat e mundshme
code	Kodi unik i përdoruesit	string	
code_type	Lloji i kodit të përdoruesit	string	Kodi_qr Kodi_temp obid pidn
masked	Nëse të dhënat e kthyera të përdoruesit duhet të maskohen apo jo	bolean	E vërtetë E gabuar

Parametri i kthimit	**Përshkrimi**	**Lloji**	**Vlerat e mundshme**
name	(I maskuar*) Emri i përdoruesit i formatuar sipas standardit ICAO 9303 Rregulli i maskës: vetëm karakteri i parë dhe i fundit i shfaqur, simbolet me yje për secilin karakter tjetër (shembull: Jasminka treguar si J*******A)	string	
last_name	(I maskuar*) Mbiemri i përdoruesit i formatuar sipas standardit ICAO 9303 Rregulli i maskës: vetëm karakteri i parë dhe i fundit i shfaqur, simbolet e yjeve për secilin karakter tjetër (shembull: Jakimovska shfaq si J********A)	string	
obid	Numri ID në Ballkanin e Hapur	string	
obid_issued	(I maskuar*) Data dhe ora kur është lëshuar OBID i formatuar sipas ISO 8601. në formatin V.-M-D i shfaqur si (format i dukshëm) D-M-V. (për shembull 2023-12-30) treguar si 30.12.2023	string	
Date_of_birth	(I maskuar*) Data e lindjes e formatuar sipas ISO 8601 në formatin V-M-D i shfaqur si (format i dukshëm) D-M-V Rregulli i maskës në formatin V-M-D: shfaqen dy karakteret e para të vitit dhe karakteret e ditës, simbolet e yjeve për secilin karakter tjetër (shembull: 2023-12-30 shfaqen si 20**-**-30) Rregulli i maskës në formatin (të dukshëm) D-M-V karakteret e ditës dhe dy karakteret e para të vitit të treguar, simbolet e yjeve për njëri	string	

	karakter tjetër (shembull: 30.12.2023 shfaqen si 30.**.20**)		
country	Kodi i shtetit të shtetësisë së përdoruesit.	string	ALB MKD SRB
pidn	(I maskuar*) Numri i identitetit kombëtar Rregulli i maskës: dy karakteret e para dhe dy karakteret e fundit të shfaqura, simbolet e yjeve për secilin karakter tjetër (shembull: 1811979410079 trego si 18**********79)	string	

* Të dhënat e fshehura vetëm për kërkesat e klientit jo të autentifikuar.

Autentifikimi

Të gjitha thirrjet e nyjave fundore të API-t duhet të vërtetohen pasi të thirren nga aplikacioni i palës referente. Vetë aplikacioni do të zbatojë logjikën nëse të dhënat i dërgohen përdoruesit të autentifikuar dhe do të kthejë të dhënat origjinale ose përdoruesit jo të autentifikuar dhe të dhëna të fshehura.

Specifikimi teknik i detajuar

Secila Palë Kontraktuese është e detyruar të sigurojë dhe të ndajë me Palët e tjera Kontraktuese manuale teknike për ndërlidhjen e skemave për identifikimin elektronik dhe integrimin e metodave të verifikimit të ID-së së Ballkanit të Hapur.