

PROTOCOL ON INTERCONNECTION OF SCHEMES FOR ELECTRONIC IDENTIFICATION OF THE CITIZENS OF THE WESTERN BALKANS

We the Western Balkan participants referred to collectively as “the Contracting Parties” and individually as “the Contracting Party”

In keeping with Article 8 of the Agreement on Interconnection of Schemes for Electronic Identification of the Citizens of the Western Balkans, signed on 21 December 2021 in Tirana (hereinafter: the Agreement)

have agreed as follows:

Article 1

This Protocol regulates more detailed conditions for the implementation of the Agreement on Interconnection of Schemes for Electronic Identification of the Citizens of the Western Balkans, especially the technical description of the Open Balkan Identification Number and processes of connecting national software solutions that enable federation of electronic identities according to the principle of interconnection of schemes with eGovernment services of other Contracting Parties.

Article 2

The conditions referred to in Article 1 of this Protocol are described in detail in the document Open Balkan Identification Number: The Technical Reference Architecture for the Implementation of the Agreement “Interconnection of Schemes for Electronic Identification of the Citizens of the Western Balkans”, which is attached to this Protocol and forms an integral part thereof.

Article 3

The Contracting parties shall establish Joint Working Group to discuss and resolve all legal and technical issues arising from the implementation of the Agreement and this Protocol.

The Contracting parties shall each appoint one person with a duty to lead and co-chair Joint Working Group meetings and to represent main contact point for coordination of the implementation of this Protocol.

The Contracting parties may designate as many people as necessary as members of the Joint Working Group in order to fulfil the obligations of the cooperation areas stipulated in the Agreement and this Protocol.

The Contracting Parties shall notify each other through appropriate channels of the appointed persons referred to in paragraph 2 of this Article and shall exchange information on contact points, no later than 7 days from the date of the signing of this Protocol.

Article 4

For each Contracting Party, this Protocol shall enter into force on the date of the receipt of the last written notification by which the Parties notify each other, through the Depository, of the completion of the procedures as required by their domestic legislation for the entry into force of this Protocol.


The Parties may amend this Protocol in writing.

This Protocol is concluded for an indefinite period of time and shall remain in force as long as the Agreement remains in force.

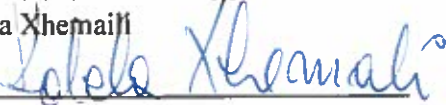
The original of this Protocol in a single copy in the English language shall be deposited with the Government of the Republic of Albania, as the Depository of the Agreement, which shall transmit a certified copy to each Contracting Party.

Done in Skopje, on 22nd of January, two thousand twenty-four

On behalf of the Government of North Macedonia
Azir Aliu




On behalf of the Government of Albania
Adela Xhemali



On behalf of the Government of Serbia

Gojko Stanivukovic



Open Balkan ID

The Technical Reference Architecture for the Implementation of the Agreement “Interconnection of Schemes for Electronic Identification of the Citizens of the Western Balkans”

Final version 2.0

April 2023

Contents

Foreword	6
Introduction	7
Revision history	7
Architecture	9
Authentication flow use case	10
Protocol	10
OIDC Authorization server endpoints	11
OAuth 2.0 (OIDC) authorization flows	11
Citizen data exchange	12
Supported Scopes	12
Claims – Scope mapping	14
Open Balkan ID number	15
Levels of assurance	16
Republic of Albania levels of assurance	17
Regulation references	17
North Macedonia levels of assurance	18
Regulation references	20
Republic of Serbia levels of assurance	21
Regulation references	21
Changes to the SSO systems	22
Obtain OAuth 2.0 access	22
Environments	22
SSO configuration endpoints	22
Testing of integration	22
Request for access	23
Appendix 1 – Certificate of issued Open Balkan ID number	25
Appendix 2	27
QR code on the Open Balkan ID number certificate	27
QR code content	27
Reading QR code process	27
One-step displaying user's data	27
Two-steps displaying user's data	28

Application Programming Interface Specification	30
verify-validity	30
get-user-data	30
Authentication	32
Detailed technical specification	32

Foreword

This document is prepared with the aim to define an interoperability technical architecture and protocol between the national electronic identification systems of the member countries participating as a subordinate document to the trilateral contract “Interconnection of Schemes for Electronic Identification of the citizens of the Western Balkans” (hereafter Agreement). It is a product of the information, documents, and consensus made during the technical meetings of the technical workgroup members. It summarizes the conclusions and the scope of implementation project which will support, but is not limited to the implementation of the “Open Balkan ID number” initiative. The technical principles and interconnection protocols should support a wide variety of citizen services will there be political and/or legal grounds by the respective representatives.

Introduction

The purpose of this document is to define interoperability architecture and technical protocols to enable cross-border online user authentication utilizing the existing national electronic identification systems or schemes.

The workgroup members nominated from each country exchanged technical information and documents in an attempt to get familiar with electronic identification systems and try to define possible interoperability architecture and underlying protocols with aim of connecting corresponding national electronic identification systems to allow the identification of cross border citizens identification to support Open Balkan ID initiative and lay the ground for future extension of different services available through the national eGovernment service Portals. These architecture and protocols should allow eGovernment service Portals to receive, request, and process personal identification (hereafter: Services) data of citizens of other Parties of the Contract aligned by the national laws and in line with the Agreement.

After having concluded the analysis phase, the participants of the analysis phase project have concluded the common technical architecture and protocols to support the Services as specified in this document.

The technical feasibility of two different architectures has been assessed during the technical meetings.

This document does not define project implementation activities, resources and schedule but focuses only on the technical architecture and protocols to establish a base for the exchange of electronic identity data and additional attributes (for example, Open Balkan ID number as defined in the Agreement).

Revision history

Version	Date	Version Change Details
1.0.0.1-Draft	16.12.2021	Initial documentation drafted by North Macedonia
1.0.0.2-Draft	27.12.2021	Updated version after harmonization technical meeting held on 23.12.2021
1.0.0.3-Draft	02.02.2022	Updated version with LOA information, updated diagrams and styles
1.0.0.4-Draft	22.02.2022	Update version with OB ID number format, OB ID certificate and appendix I
1.0.0.5-Draft	20.04.2022	Update with additional claims in the ID token

1.0.0.6-Draft	05.05.2022	Updated version with added mandatory supported Scopes and Claims – Scope mapping
1.0.0.7-Draft	10.05.2022	Updated version with added new claim (Gender) and Appendix 2
1.0.0.8- Draft	23.05.2022	Updated version with adding bar code to Open Balkan ID certificate
2.0 – Final	04.04.2023	Updated version with updated visual representation of the Certificate of issued Open Balkan ID number and API Return parameter description masking rules

Architecture

Citizen access to the eGovernment services Portal in each Contracting Party will be enabled through configuring federation on Single Sign-On (hereafter: SSO) systems level.

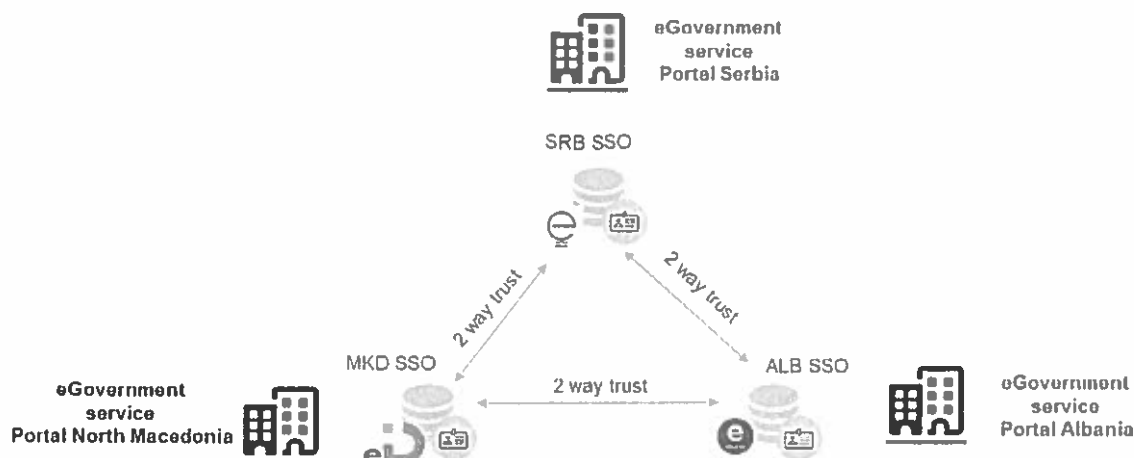


Figure 1: Architecture

SSO is a service through which the users are authenticated and allowed access to the eGovernment Portals and other service providers.

Each country at the moment has established a single online identity provider (IDP) for the national eGovernment Portal and it is recommended that federated login architecture is configured to support the cross-border citizen authentication scenarios.

The federated login allows that user authentication and authorization are managed by each member country for its citizens while allowing the secure exchange of required information for user identification in other Contracting Parties' eGovernment systems.

A federation can be expressed as an agreement between Contracting Parties that trust each other. In bilateral federations, you can have direct trust between the parties. Therefore, 3 bilateral federations will be established.

An entity in the federation must be able to trust that other entities it is interacting with belong to the same federation. It must also be able to trust that the information the other entities publish about themselves has not been tampered with during transport and that it adheres to the federation's policies.

Authentication flow use case

The diagram below shows a typical authentication flow of foreign citizens in a domestic eGovernment Portal.

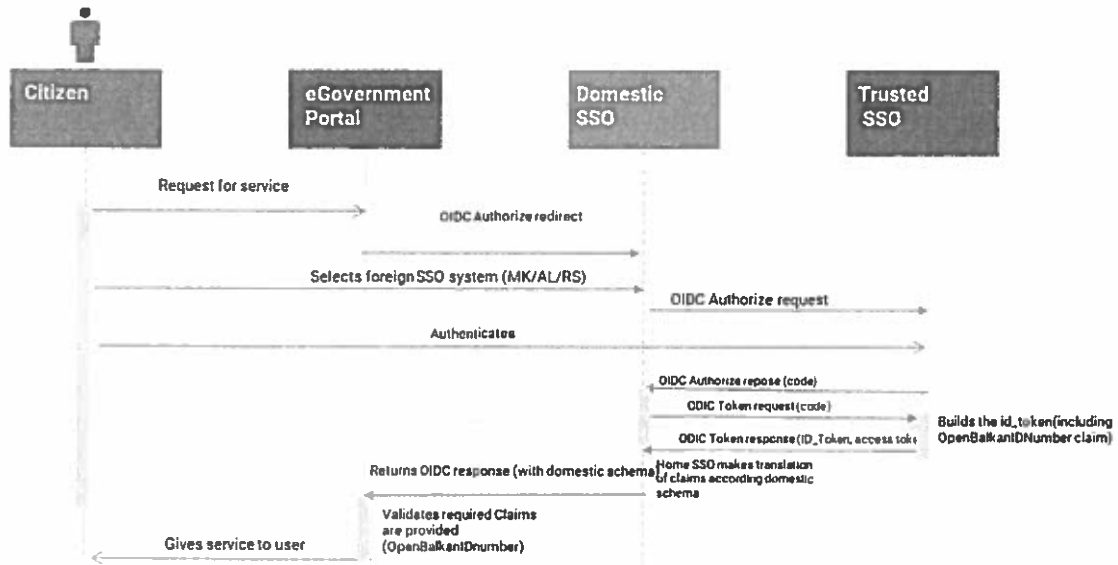


Figure 2: Use case flow

Protocol

All SSO systems must support user authentication based on OpenID Connect 1.0 (OIDC) specification built on top of the OAuth 2.0 (IETF RFC 6749) specification.

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It enables Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

OpenID Connect 1.0 federation OpenID Connect Federation trust chains rely on cryptographically signed JSON Web Token (JWT) documents.

OIDC Authorization server endpoints

All SSO systems must support minimum the following endpoints as defined by the OIDC standard.

Endpoint	Use
<i>authorization_endpoint</i>	Interact with the resource owner and obtain an authorization grant.
<i>token_endpoint</i>	Obtain an access and/or ID token by presenting an authorization grant or refresh token.
<i>userinfo_endpoint</i>	Return Claims about the authenticated end user.
<i>end_session_endpoint</i>	End the session associated with the given ID token.
<i> JWKS_URI</i>	JWT token Signing Key retrieval endpoint

Table 1 – Authorization server endpoints

All of the endpoints on this page start with an authorization server, however the URL for that server varies depending on the endpoint and the type of authorization server. You have two types of authorization servers to choose: stage and production.

OAuth 2.0 (OIDC) authorization flows

All SSO systems must support the following **Authorization Code Flow** with multiple response types as defined in the OAuth 2.0 protocol.

The authorization request will support the following response types

Identifier	Description
Code	Authorization Code Flow as specified in the OpenID Connect 1.0 specification
id_token, token	This is mandatory as the Token Endpoint will not be used for the exchange of additional Claims defined in this document.

Table 2 – Authorization flows supported response types

Each SSO shall support combined response types a typical request is given in example bellow:

```
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=af0ijfslkdj HTTP/1.1  
Host: server.example.com
```

Citizen data exchange

All citizen data requirements for the interconnection will be shared through the Claims included in the *id_token* and authorized through the use of the corresponding Scope.

Translation of Claims on domestic SSO systems may be required as each country's SSO systems have different Claim specifications and Claim schemas.

Each country's SSO system will need to implement translation for each Claim provider to avoid changes in existing systems integrated with their SSO system and ensure transparency towards domestic eGovernment service portals.

New Claims for the users could be additionally specified so translation can be implemented in the domestic SSO systems.

Supported Scopes

OpenID Connect Clients use Scope values as defined in 3.3 of OAuth 2.0 [RFC6749] to specify what access privileges are being requested for Access Tokens. The Scopes associated with Access Tokens determine specific sets of information that will be made available as Claim/Values.

The three systems should at minimum support and grant access to each other to the following Scopes:

Scope	Description
<i>openid</i>	Mandatory Scope for retrieving ID token.
<i>profile</i>	The Claims/values covered by this Scope as part of the <i>id_token</i> are The Claims/values are defined in the Claims-Scope mapping section.
<i>email</i>	The Claim/value covered by this Scope as part of the <i>id_token</i> is voluntary but each SSO system should support providing <i>email</i> and/or <i>email_verified</i> Claims. Each country should specify the availability and policy associated with this data.
<i>openbalkanid</i>	The Claims/values covered by this Scope as part of the <i>id_token</i>
<i>pidn</i>	Scope used to manage the Unique citizen number exchange as part of the ID token
<i>dateofbirth</i>	Scope used to manage the Birth date claim as part of the ID token

Table 3 –Mandatory supported Scopes

It is agreed that data Claimed data should be included in the *id_token* as specified in the OIDC 1.0 specification. The ID Token is represented as a JSON Web Token (JWT). It is not mandatory that standard *userinfo_endpoint* endpoint will contain additional Claims defined by the extended Scope (*openbalkanid* Scope).

Claims – Scope mapping

Each country should provide minimum information on the following Claims exchanged as part of the *id_token*.

Claim	Description	URI	Scope
<i>First Name</i>	First name of the citizen	To be specified by each country	<i>profile, openbalkanid</i>
<i>Last Name</i>	Last name of the citizen	To be specified by each country	<i>profile, openbalkanid</i>
<i>Gender</i>	Gender of the citizen	To be specified by each country	<i>profile, openbalkanid</i>
<i>E-mail</i>	Confirmed E-mail address	To be specified by each country	<i>profile, openbalkanid</i>
<i>Country</i>	2 letter country code “MK”, “AL”, “RS”	To be specified by each country	<i>openbalkanid</i>
<i>loa</i>	Level of assurance as defined in the national electronic identification laws. Possible values “ANONYMOUS”, “LOW”, “SUBSTANTIAL”, “HIGH”	To be specified by each country	<i>openbalkanid</i>
<i>obid</i>	As defined in the OpenBalkanID Number section.	To be specified by each country	<i>openbalkanid</i>
<i>Unique Citizen Number</i>	Domestic citizen unique number	<i>To be specified by each country</i>	<i>pidn</i>
<i>Date of birth</i>	Date of birth	<i>To be specified by each country</i>	<i>dateofbirth</i>

Table 4: Claims/Scope mapping

In case first and last name are in domestic alphabet, each Party will use ICAO Doc 9303 standard in claims exchanged:

https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

Open Balkan ID number

Each member state shall implement its process for issuing Open Balkan ID number on the eGovernment portal in order to support its exchange over the agreed protocol.

The authorities responsible for issuing the Open Balkans ID in Contracting Parties are:

- Office for Information Technology and Electronic Government in the Republic of Serbia;
- Ministry of Information Society and Administration in the Republic of North Macedonia;
- General Directorate of the Civil Registry in the Republic of Albania.

A citizen who obtains Open Balkan ID number on his/her national eGovernment portal receives an Open Balkan ID electronic certificate containing personal data. Data within Open Balkan ID certificate and format is specified in the Appendix 1 of this document. The agreed Claim name is “*obid*” and should be provided within the *id_token* when authorization request is made containing the *openbalkanid* Scope.

Format of the prefix country code 2 numbers + 11 numbers:

Republic of Serbia – 81 XXXXXXXXXXXXX

North Macedonia – 89 XXXXXXXXXXXXX

Republic of Albania – 55 XXXXXXXXXXXXX

The algorithm to be used for generating and verifying the OBID numbers is Luhn algorithm: https://en.wikipedia.org/wiki/Luhn_algorithm excluding the country code (first 2 digits are not part of the check).

Each Party must provide interface for other two Parties for validation of Open Balkan ID certificates issued. Interface specification shall be additionally agreed during implementation.

Protocol for checking *obid* and obtaining additional information required by the service providers (example: Ministry of interior for issuing unique citizen number for foreigner) will be additionally specified.

Levels of assurance

Level of assurance is an important factor in the system and there are discrepancies in the interpretation, implementation and availability of systems supporting it among the participating countries.

The definition of acceptable level of assurance is not subject to the definition in this Document. The level of assurance will be represented as single value with following values.

- ANONYMOUS
- LOW
- SUBSTANTIAL
- HIGH

The information on a technical level will be exchanged as part of the *id_token* when a request has been made with the *openbalkanid* Scope. The Claim name is agreed to be "*loa*".

As the level of assurance is guaranteed (therefore trusted) by the national SSO systems, additional information on the policy for each level shall be exchanged and agreed between the countries. There is no technical possibility for automated, technical validation of actual meaning of these levels therefore the technical protocol for interconnection will only have technical means to exchange this information.

Republic of Albania levels of assurance

Level	Policy description
ANONYMOUS	<i>N/A</i>
LOW	<i>N/A</i>
SUBSTANTIAL	<i>Users login by username and password. In the registration process, the data provided are cross checked in real time with the national civil registry for citizens and the commercial register for businesses. Users have to fill specific data known only by them and also they get equipped with a 4 digit code through sms and activation link provided through mail.</i>
HIGH	<i>Users login with digital certificate</i>

Table 5 – Albania level of assurance policy

Regulation references

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

Level	Policy description
ANONYMOUS	<p><i>Online with Valid E-Mail Address</i></p> <p><i>Users log-in with valid e-mail address</i></p> <p><i>For creation of basic user profile ie. registration and authentication of the user of eID on anonymous level of assurance, the user only needs a valid e-mail address. In the registration form, the user enters valid e-mail and password, and confirmation of the password. After this process an e-mail is sent to the claimed e-mail address for the purpose of verification and registration on anonymous level of assurance.</i></p> <p><i>By successfully registering only by e-mail address, basic user profile is created and can be used for application for electronic services that do not require verification and authentication of user identity.</i></p> <p><i>Having a basic user profile means that user's physical identity is not confirmed and verified during the registration process. The registration process only verifies that a user has access to the provided e-mail address.</i></p> <p><i>With the basic user profile, the user may apply for e-services for which the applicant's identity is not required.</i></p> <p><i>Login with basic user profile requires authentication with username and password.</i></p>
LOW	<p><i>Remote with Existing Username from PRO</i></p> <p><i>Registered, verified and authenticated taxpayer</i></p> <p><i>If a natural person has an active user account in Public revenue office taxpayer registry, that person may register on the E-Services Portal on low level of assurance with that account. In the registration form, the user enters the same username and password that was used for registration in PRO taxpayer registry. If PRO register data are correct and if users SIN from PRO exists in the Central Population Registry (CPR), that user profile in SSO is automatically created and registered on the E-Services Portal. By successfully registering with PRO user account, eID is created on low level of assurance. With this type of eID, the user may apply for low-level e-services.</i></p> <p><i>If the user has a qualified certificate for electronic signature issued from registered qualified trust service provider, the user may upgrade its low level eID certificate to high level eID.</i></p>

Level	Policy description
	<p><i>Having a low level eID means that user's physical identity has been confirmed and verified during the registration process, whereby he/she have been personally present during the registration process, have shown a valid personal identification document and his/hers data available in the Central Population Registry (CPR) have been additionally confirmed and registered. eID on high level of assurance is created based on confirmed physical identity.</i></p> <p><i>Login with low level eID requires authentication with username and password. The level of reliability of such login is considered low, because there is certain level of possibility to discover the username and password.</i></p>
SUBSTANTIAL	N/A
HIGH	<p><i>Remote with qualified certificate for electronic signature issued from registered qualified trust service provider</i></p> <p><i>If a natural person has a valid qualified certificate for electronic signature issued by qualified trust service provider registered under the Register of trust service providers and electronic identification schemes the user may remotely register for eID on high level of assurance. In the registration form, the user enters its SIN for which the certificate is issued, e-mail address that would be further used as SSO login username, and password. SSO verifies issuer of the selected qualified certificate for electronic signature, to verify link between the certificate and entered SIN. If the certificate issuer confirms the certificate and the SIN are linked, SSO verifies whether the provided SIN exists in the Central Population Registry (CPR). After successful completion of both verification processes, the SSO user profile is created, whereby a verification e-mail on the e-mail address provided during the registration process. The SSO user account is activated with a single click on the link provided in the e-mail. By successfully registering with qualified certificate for electronic signature, eID on high level of assurance is created that can be used to apply online for all e-Services available on the Portal.</i></p> <p>Having a high level eID means that all requirements for creating low level eID are met during the registration process, and that a valid digital certificate has been provided during the registration process, issued by</p>

Level	Policy description
	<p>certificate issuer registered in the Register of Certificate Issuers in the Republic of North Macedonia (Register of Certificate Issuers).</p> <p>Login with high level eID requires authentication by means of digital signature certificate. The level of reliability of such login is considered high, because it requires possession of the eID mean and PIN code, whereby the possibility of someone else registering with that eID is significantly decreased.</p> <p>If he/she has registered with high level eID, the user may also login with low level eID, without digital certificate.</p>

Table 6 – North Macedonia level of assurance policy

Level of assurance of the electronic identification scheme is determined depending on:

- Level of assurance of the sign in and sign up of the subject of electronic identification;
- Level of assurance of authentication of the identity and verification of natural persons.

Regulation references

- [1] https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/pravilnik_identitet.pdf
- [2] <https://uslugi.gov.mk/register.nspix>
- [3] <https://uslugi.gov.mk/e-id.nspix>
- [4] https://mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/pravilnik_tom_s_hemi.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

Level	Policy description
ANONYMOUS	N/A
LOW	<p><i>Users login by username and password.</i></p> <p><i>In the registration process, after filling in registration form online, user receives a verification email to confirm access to email address provided. If the registration is done online after confirming email address, registration is then reviewed by authorized personnel in the Office for IT and eGovernment and data is check in official registries within 48 hours. If the registration is done on the counter (more then 1000+ locations), authorized person registers user account in direct contact, confirms identity of a person by reviewing his/her ID card or passport and checks data in official registries.</i></p>
SUBSTANTIAL	N/A
HIGH	<p><i>Users login with two-factor authentication.</i></p> <p><i>Users can upgrade access to their account from username and password to two factor authentication using their mobile device (smart phone or tablet). Mobile application is called ConsentID and activation parameters are provided to the user in direct contact by authorized person at one of 1000+ locations provided that user has valid ID card or passport for identification purposes. User must sign a paper to confirm they have received activation parameters.</i></p> <p><i>Users login with qualified digital certificate.</i></p>

Table 7 – Serbia level of assurance policy

Regulation references

- [1] <https://www.pravno-informacioni-sistem.rs/SIGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2017/94/4/reg>
- [2] <http://www.pravno-informacioni-sistem.rs/SIGlasnikPortal/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>

Changes to the SSO systems

Each country as part of the establishment of federated trust will implement an explicit selection of the user of identity provider on the authenticate/authorize user page by adding redirection links (Example: on MK SSO authorization page redirect links to Albanian SSO and Serbian SSO will be added) so users can complete the authentication process.

Each country as part of the establishment of federated trust will implement Claim translation of foreign SSO Claim types into the domestic established Claims.

Obtain OAuth 2.0 access

Environments

Each member should provide access and information for use for one stage where integration testing can be performed. Access to this environment should be available at all times during the implementation of Services as well as long there is a valid Agreement for providing the Services.

Additionally, access to the production endpoints shall be provided once a successful test is conducted and signed by participating members.

Access to any endpoints is granted by sharing valid OAuth2 *Client ID* and *Client Secret* and URL to the respective environment that complies with the specification in this Document.

SSO configuration endpoints

The configuration for the eID OIDC production environment is available at:

Country	OIDC configuration endpoint	Type
Albania	https://e-albania.gov.al/.well-known/openid-configuration	Production
Republic of North Macedonia	https://eid.mk/.well-known/openid-configuration	Production
Republic of Serbia	https://prijava.eid.gov.rs/oauth2/oidcdiscovery/.well-known/openid-configuration	Production

Table 8 – Production configuration endpoint

Each country shall provide stage endpoints details during the process of system development.

Testing of integration

Integration connection based on the federated trust established on OIDC protocol can be tested bilaterally and there is no need for a joint multilateral testing process. Once the countries sign-off bilateral acceptance protocol access to the production endpoints could be provided.

However, the exact date for enabling the Services shall be defined by the Parties of the Agreement.

Once the eID support team receives this information a configuration on the eID servers will be executed and OAuth 2.0 credentials (ClientID, Client secret) will be exchanged with the Contact person.

Request for access

In order to configure the federated trust Parties shall exchange at minimum the following information and update this information if changed so processes of support and maintenance can be maintained.

Information	Description
Organization Name	Name of the Government Agency to be presented during user authorization process on the SSO system. (Republic of North Macedonia, Republic of Serbia, Albania)
Contact Person Name	First Name, Last Name of the primary contact related to SSO federation maintenance and support.
Contact e-mail address	E-mail address of the primary contact responsible for SSO federation maintenance and support.
Application Name	3 rd party application name. Example (“euprava.gov.rs”, “e-Albania.al”, “uslugi.gov.mk”...) this depending on the SSO authentication capabilities could be presented during user authorization flow.
OAuth 2.0 Call Back URL	Return OAuth 2.0 metadata related to the specified authorization server.
Application Privacy Policy link	This link is mandatory due to compliance with the Data protection regulation (GDPR and other where applicable). It must be hosted on HTTPS public reachable link and protected by SSL certificate issued to the organization.
Application Icon	Application Icon in jpg, png format with minimum resolution of 200x200 pixels in 1:1 ratio. Needed to be shown to the user during end-user authentication/authorization web scenarios.

Table 9 – Required configuration information

References

1. OpenID Connect 1.0 Final: [OpenID Connect Core 1.0 incorporating errata set 1](#)
2. The OAuth 2.0 Authorization Framework <https://datatracker.ietf.org/doc/html/rfc6749>

3. Electronic Identities – a brief introduction, https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf, downloaded on August 25, 2021
4. OpenID Libraries, Products, and Tools, <https://openid.net/developers/libraries/>, visited on August 25, 2021
5. Authorization Code Flow with Proof Key for Code Exchange (PKCE), <https://auth0.com/docs/flows/authorization-code-flow-with-proof-key-for-code-exchange-pkce>, visited on August 25, 2021

Appendix 1 – Certificate of issued Open Balkan ID number

Personal and other data to be presented on the **Certificate of issued Open Balkan ID number** is as follows (in 4 languages):





Information	Description
Last Name and First Name	First Name and Last Name in international ICAO format as present on personal identification document.
Date of birth	Date of Birth (dd.mm.yyyy)
Country of citizenship	Issued by Country (Albania, Republic of Serbia, Republic of North Macedonia)
Unique domestic ID number	Unique domestic number (13 digits)
Open Balkan ID number	Open Balkan ID number in the agreed format
Date and time of obtaining Open Balkan ID number	Date and time of issuing the certificate in dd.mm.yyyy h24:min format.
Email	Email address equal to username received in the <i>ID_token</i> .
Issuing authority and electronic seal	Authority responsible for issuing the Open Balkans ID in Contracting Party as defined in section Open Balkan ID number
QR code	QR code containing permanent link to the web page where the validity of Open Balkan ID number certificate can be confirmed
Bar code	Bar code (code 128 auto) containing Open Balkan ID number

Certificate itself contains two disclaimers represented at the bottom of the page:

1st disclaimer – Approval is issued as electronic document and printed version represents a copy of this document

2nd disclaimer - Approval is valid with appropriate personal document which proves the identity of the person

Below is the visual representation of the Certificate (A4 size):

	Идентификациони број Отвореног Балкана Потврда о издатом Идентификацијом броју Отвореног Балкана	
Numër ID për Ballkanin e Hapur Vërtetimi i lëshimit të numrit të ID për Ballkanin e Hapur	Отворен Балкан идентификационен број Потврда за издаден идентификациски број за Отворенот Балкана	Open Balkan ID number Certificate of issued Open Balkan ID number
Prezime e eme / Surname and name / Emri dhe Mbiemri / Презиме и име	Идентификациони број Отвореног Балкана Open Balkan ID number Numër ID për Ballkanin e Hapur Идентификациски број Отвореног Балкана	
Data e lindjes / Date of birth / Dittëlindja / Датум на раѓање		
Drashjanstvo / Citizenship / Shtetësi / Државјанство		
JMFI / Unique personal ID number / Numër ID personal unik / Единствен личен број на граѓанинот		
Data e lëshimit të numrit të ID për Ballkanin e Hapur / Датум и време на добивање на идентификациски број за Отворенот Балкана		
Imeja e adresës / E-mail address / Adresa e emailit / Адреса на електронска пошта		
Poterdha e izdara / Certificate issued by / Vërtetimi i lëshimit nga / Потврдата ја издава	Дигитални потпис / Electronic seal / Vu e elektronike / Дигитален потпис	
		
Poterdha se изда е као електронски документ и ододелно одвојен потпис представља копија. Архива се издава во електронски документ и одвојена копија од документот. Архивата е одвојена копија од документот. Потврдата се издава као електронски документ и ододелно одвојен потпис од потврдата представља копија.		
Poterdha je važna uz odgovarajuća lična dokumentacija koja dokazuje identitet. Approval is valid with appropriate personal document which proves the identity of the person. Архива е валидна влијателни документ персонал ре-катоs qe vërteton identitetin e personit. Потврдата е важечка само со соодветен личен документ со кој се докажува идентитетот.		

Appendix 2

Each Contracting Party is responsible for issuing Open Balkan ID number (OBID) for their own citizens and to provide web service for verification of issued Open Balkan ID number. Part of the verification process is reading QR code which is contained on the Certificate of issued Open Balkan ID number (see Appendix 1).

Appendix 2 describes the contents and procedures for reading QR code and the verify OBID web service specification.

QR code on the Open Balkan ID number certificate

QR code content

Content of the QR code (the information it holds) should be permanent link to the web page where the validity of QR code and Open Balkan ID number certificate can be confirmed. Permanent link should consist of web page address which has the same value for all users and unique code related to the user:

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

Example: <https://eid.gov.xy/ob/qr/S8KSCWMDEJTUXKWIEK>
where **S8KSCWMDEJTUXKWIEK** is the user code.

User code represents ASCII characters string of arbitrary length from which none of the user's data could be determined. Method for creating user code is determined by each Party.

Reading QR code process

When QR code is scanned, the following information should be provided:

- information whether QR code is valid or not valid
- user's data (complete or masked) so the viewer can compare data from the document and from the system.

Each Party shall provide the service to validate QR code and retrieve user's data. There are two variants of the procedure to validate QR code and display user's data among which each Contracting Party shall choose one to use.

One-step displaying user's data

One step procedure consists of displaying user's data at the first web page after scanning QR code. The procedure is shown in the diagram below:

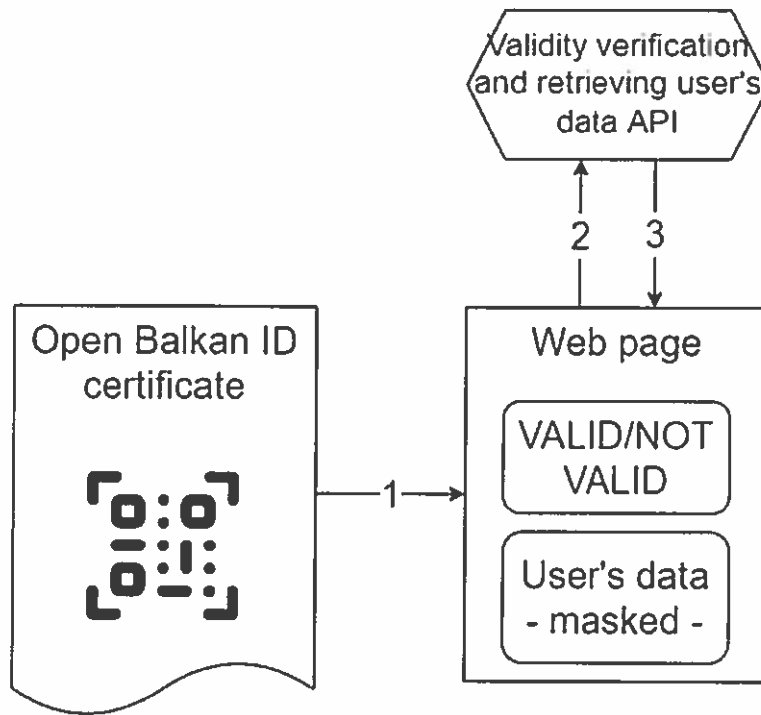


Diagram 1 One-step displaying user's data

When QR code is scanned and its link is clicked, the invoked web application (1) should call “Validity verification and user’s retrieving user’s data API” (2) to get information whether Open Balkan ID is valid and get user’s data which can be displayed on the web page. User’s data shown on the web page could be masked or in the original format. Masked data means that sensitive data is partially displayed, for example first few letters are shown and asterisk characters instead of other letters. Whether user’s data should be masked or not will be decided by the fact whether it is the authenticated user who is scanning QR or not. Authenticated users like official institutions are the ones which are authorized to view sensitive data.

Two-steps displaying user’s data

The two-step procedure consists of displaying information whether QR code is valid or not at the first web page after scanning QR code and showing user’s data at the second web page invoked after clicking on a temporary link on the first page.

Process of reading QR code is shown in the diagram below:

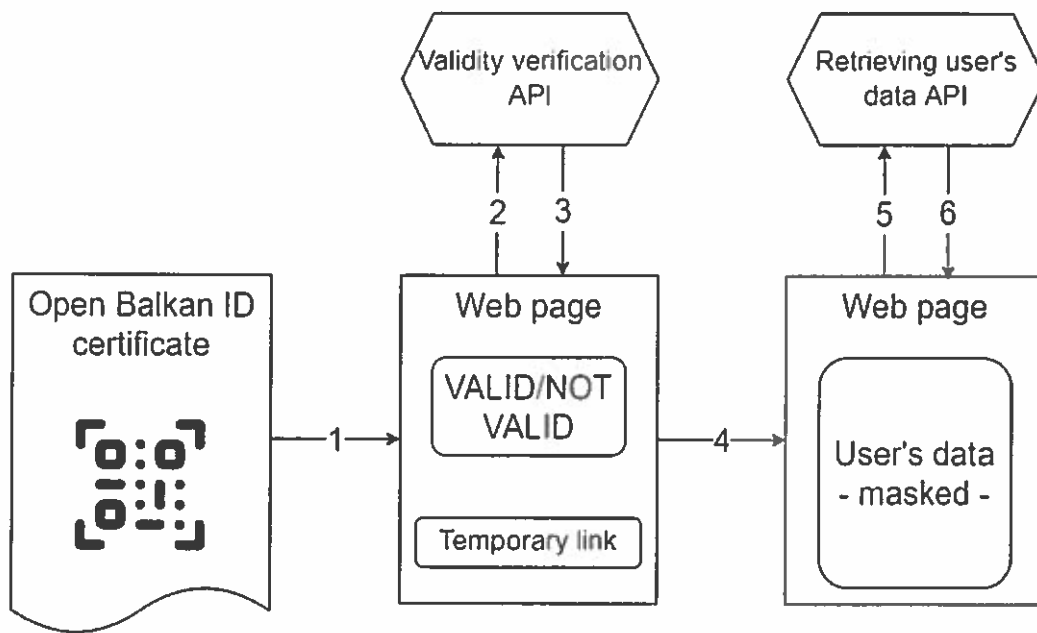


Diagram 2 Two-step displaying user's data

When QR code is scanned and its link is clicked, the invoked web application (1) should call “Validity verification API” (2) to get information whether Open Balkan ID is valid. API determines Open Balkan ID by the user code which is sent as parameter.

In the API response (3), the web application will get information whether QR code and its Open Balkan ID number is valid or not. If valid, API will also return unique code for temporary access to user’s data. Web page should display information about validity and a temporary link for viewing user’s data. Temporary link should be valid for 5 minutes. This link should consist of web page address which will show user’s data and temporary code got from API:

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

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

The reason for having temporary code and accordingly temporary link is to prevent to open user’s data web page from saved and indexed data by search engines. Link for viewing user’s data will be valid for just a few minutes and cannot be used later. Each time a user’s QR code is scanned, a new link for viewing data should be presented. Generation of new temporary code does not cancel validity of previously generated and still active temporary codes for the same user. This means that each code is active for 5 minutes and there can be multiple active temporary links for one user.

When temporary link is clicked, invoked web page (4) should call “Retrieving user’s data API” (5) to get user’s data. API verifies temporary code which is sent as parameter. If it is valid, API returns user’s data which may be masked or not (6).

Upon receiving response from the API, web page will display masked user’s data to be checked by a human whether data on the certificate match with data displayed on the web page.

Application Programming Interface Specification

Each party should define the following Application Programming Interface (API) endpoints:

1. verify validity – returns whether provided code is valid or not
2. get user data – retrieves user data

verify-validity

Input parameter	Description	Type	Possible values
code	Unique user code	string	
code_type	Type of the user code	string	qr_code obid pidn (unique citizen number)

Return parameter	Description	Type	Possible values
valid	Information whether user code is valid or not	bool	true false
temp_code	Temporary code which may be used to retrieve user's data for a limited time	string	

get-user-data

Input parameter	Description	Type	Possible values
code	Unique user code	string	
code_type	Type of the user code	string	qr_code temp_code obid pidn
masked	Whether returned user data should be masked or not	bool	true false

Return parameter	Description	Type	Possible values
------------------	-------------	------	-----------------

name	(Masked*) User's name formatted according to ICAO 9303 standard Mask rule: only the first and last character shown, asterisk symbols for each other character (example: Jasminka shown as J*****A)	string	
last_name	(Masked*) User's last name formatted according to ICAO 9303 standard Mask rule: only the first and last character shown, asterisk symbols for each other character (example: Jakimovska show as J*****A)	string	
obid	Open Balkan ID number	string	
obid_issued	(Masked*) Date when the OBID was issued formatted according to ISO 8601 in format YYYY-MM-DD shown as (visible format) DD.MM.YYYY (example: 2023-12-30 shown as 30.12.2023)	string	
date_of_birth	(Masked*) Date of birth formatted according to ISO 8601 in format YYYY-MM-DD shown as (visible format) DD.MM.YYYY Mask rule in format YYYY-MM-DD: first two characters in year and characters of day shown, asterisk symbols for each other character (example: 2023-12-30 show as 20**-**-30) Mask rule in (visible) format DD.MM.YYYY characters of day and first two characters in year shown, asterisk symbols for each other character (example: 30.12.2023 show as 30.**.20**)	string	
country	User's citizenship country code	string	ALB MKD SRB
pidn	(Masked*) National ID number Mask rule: first two characters and last two characters shown, asterisk symbols for each other character (example: 1811979410079 show as 18*****79)	string	

* Masked data only for non-authenticated client requests.

Authentication

All API endpoints calls have to be authenticated since they will be called by referent Party's application. The application itself will implement logic whether data are served to the authenticated user and return original data or to the non-authenticated user and return masked data.

Detailed technical specification

Each Contracting Party is obliged to provide and share with other Contracting Parties technical manuals for interconnection of schemes for electronic identification and integration of Open Balkan ID verification methods.