DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

National Identity Authority

Description of the National Identity Authority

The NIA provides state-guaranteed services to public administrations identification and authentication, including federation of data on the subject of law from the basic registers and the possibility of transmitting login identities according to the Single Sign-On principle. For persons listed in the ROB or logging in with an eIDAS identity from EU Member States, the OVS does not need to handle login identities for its clients itself. In the current state of the ROB (As-Is state), therefore, only for citizens of the Czech Republic and foreigners with permanent residence. In the future state (To-Be state) for Czech citizens, foreigners with permanent residence and other natural persons (EjFO) who have a legal or property relationship to the Czech Republic (foreign property owner, foreign doctor, foreign student, etc.).

The National Identity Authority creates a federated system consisting of the following components:

- **National Point** as the central point of the federative system, which ensures communication and registration of the federation participants. This component also ensures that the person who proves his identity by presenting authentication means is always **uniquely identified**.
- **Qualified administrator,** which issues remote authentication (proof of identity) devices to uniquely identified individuals and performs all activities related to the management of these devices and proof of identity of the individual
- **Basic registries,** which provide unambiguous identification of an individual and ensure the linkage of that individual to reference data about the individual
- **The eIDAS National Node,** which provides for the acceptance of remote proof of identity from the notified systems under the eIDAS Regulation and the transmission of remote identification and authentication from the Czech Republic to other EU states. Other EU states will have to accept Czech identities from 13 September 2020, when the notified Electronic Identity Card means expires.

Although the NIA currently provides its services only as a "front-end" solution using SAML tokens, it is planned to also provide services as a "back-end" for the use of identity translations and identifiers using eGON services.

Identity Provider (IdP) list

Identity Resource Name	Resource Type	Resource Level	Description	URL	Use for international identity verification in eIDAS
eCitizen	Electronic ID card with activated electronic identification part	High (highest possible according to eIDAS)	Login via a new ID card issued after 1 July 2018 that contains a chip and its electronic functionality has been activated. To log in with this ID card, a document reader and the relevant software must be installed.	https://info.eidentita.cz/eop/	YES - eObčanka is so far the only means declared under eIDAS for international identification and authentication purposes. Its use is mandatory for other countries under eIDAS for use from September 2020.
Mobile eGovernment Key	Mobile application with QR code verification function	Substantia	The eGovernment Mobile Key represents the use of login without the need to enter additional authentication codes. Once installed and activated, you will be able to log in to services using electronic identification through the National Point. In order for everything to work, you must have the mobile key app installed on your mobile device. The mobile key app is identical to the existing ISDS mobile key app. If you already have this app for logging in to data boxes, updating this app will also give you the option to use it to log in to services through the National Point.	https://info.eidentita.cz/mep/	NO
NIA ID	Name + password + sms. Classic second factor login.	Substantia	Login with the username and password you entered when you created your ID on the National Point portal. You complete the login by entering the verification code that will be sent to your phone number as an SMS.	https://info.eidentita.cz/ups/	NO
První certifikační autorita, a.s.	Starcos chip card with identification certificate	High (highest possible according to eIDAS)	Sign in with Starcos chip card of První certifikační autorita, a.s., which was used to generate and store the private key of the identity commercial certificate. To log in, you will need a smart card reader (if not integrated into the PC/NTB) and the SecureStore control software installed (downloadable from www.ica.cz).	https://www.ica.cz/ica-identity-provider	NO
MojeID	Login credentials to your MojeID account paired with a FIDO resource	Substantia	Log in with your MojeID account. To log in, you need to secure the account with a security key (token) certified by the FIDO Alliance to at least L1 level, either physical (USB, NFC, Bluetooth) or system (Windows Hello, Android v. 7 and higher). It is also necessary to have the mojeID account activated to access public administration services and to verify your identity once (with an existing device or by visiting Czech POINT). The mojeID service is operated by CZ.NIC, the administrator of the .CZ domain.	https://www.mojeid.cz/	NO

Identity Resource Name	Resource Type	Resource Level	Description	URL	Use for international identity verification in eIDAS
IIG - International ID Gateway	Choice of possible identity resources that are reported by other EU Member States within eIDAS nodes	low to high depending on the resource	Currently, it is possible to choose from the resources of eIDAS nodes https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS		NO
Banking Identity	Identity provided by Československá obchodní banka, a. s.	Substantia		https://www.csob.cz/portal/csob/csob-identita	NO
	Identity provided by Česká spořitelna, a. s.	Substantial		https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita	No
	Identity provided by Komerční banka, a. s.	Substantial		https://www.kb.cz/cs/podpora/bankovnictvi-a-nastroje/kb-bankovni-identita	No
	Identity provided by Air Bank, a. s.	Substantial		https://www.airbank.cz/produkty/bankovni-identita/	No
	Identity provided by MONETA Money Bank, a. s.	Substantial		https://www.moneta.cz/otevrene-bankovnictvi/bankovni-identita	No

Identity usage statistics

Data is informative and valid at a specific time 24.05.2021

Number of profiles with at least one active resource	3704483
Total state resource IDs	481717
Total non-state resource IDs	4838451

Identity Resource	Number Description	Number
eCitizen (as of July 1, 2018):	Number of activated resources	386535
	Number of active resources	342326
	Number of logins	722248
NIA ID (formerly "Name, Password, SMS") (since 1.7.2018):	Number of activated resources	119864
	Number of active resources	117966
	Number of logins	2985801
Mobile eGovernment Key (from 16.11.2020):	Number of activated resources	22617
::::	Number of activated resources	21425
	Number of logins	196790
Air Bank:	Number of activated resources	1083972
	Number of active resources	894705
::::	Number of logins	83696
Czech Savings Bank:	Number of activated funds	1896981
	Number of active funds	1752676
::::	Number of logins	391753
ČSOB Identity - fully authenticated access	Number of activated resources	304642
	Number of active resources	219860
	Number of logins	120153
ČSOB Identity - Fast Access	Number of activated resources	157042
	Number of active resources	152844
	Number of logins	8300
První certifikační autorita, a.s.:	Number of activated resources	597
	Number of active resources	557
	Number of logins	57844
Commercial Bank:	Number of activated resources	946009
	Number of active resources	927895
	Number of logins	119803

Identity Resource	Number Description	Number
myID:	Number of activated resources	19886
	Number of active resources	17806
	Number of logins	151050
MONETA Money Bank:	Number of activated funds	878064
	Number of active funds	872108
	Number of logins	28834

List of Service Providers (Service Provider; SeP)

There are already more than 50 service providers and more are in the pipeline. The final number is in the hundreds. The current list is available here https://info.eidentita.cz/sep/.

Just as other states are obliged under eIDAS to accept Czech declared means of identity (eObčanka), Czech service providers are obliged to accentuate the identity declared by another state under eIDAS. The obligation to allow login using the IIG - International Identity Gateway is enabled for all service providers as of 30.6.2020.

Attributes issued to Service Providers (SePs)

The following attributes are issued by the NIA to so-called Qualified Service Providers. The issue is also described in Portals of public administration and private data users. The bolded attributes correspond to the eIDAS standard, while the other attributes do not correspond to the standard, but the qualified service provider has the possibility to request their release when communicating within the Czech Republic.

Attribute/Element	Attribute Name	Description
Surname	**CurrentFamilyName**	Reference - Surname of the natural person. See eIDAS reference.
Name	**CurrentGivenName**	Reference - The name or names of the natural person. See eIDAS reference.
BirthDate	**DateOfBirth**	Reference - The date of birth of the natural person. See eIDAS reference.
Place of Birth	**PlaceOfBirth**	Reference - Place of birth of the natural person. See eIDAS reference.
Country of Birth	CountryCodeOfBirth	Reference - Country of birth of the natural person, transmitted in ISO 3166-3 code.
Residence address	**CurrentAddress**	Reference - Residence address of the natural person, transmitted in BASE64 encoding. It contains (if specified in the ROB) the street name (Thoroughfare), the post name (PostName), the postcode (PostCode), the name of the municipality, possibly supplemented by the municipality subdivision (CvaddressArea) and the house number/orientation number (LocatorDesignator). The attribute is based on the ISA Core Vocabulary and a more detailed description of the attribute is also given there.
Email	Email	Email address listed on eidentita.cz in the "Your details" section.
Is older than X	IsAgeOver	The calculation is older than X according to the reference Date of Birth.
Age	Age	Calculation of age according to the reference Date of Birth.
Phone	PhoneNumber	Phone number listed on eidentita.cz in the "Your details" section.

Attribute/Element	Attribute Name	Description
Residence address (transmitted in the form of RUIAN codes)	TRaddressID	Reference data - The residence address of a natural person is transmitted in the RUIAN codes. It contains (if specified in ROB) codes for district, municipality, part of municipality, street, postcode, building, address place, house number and landmark number.
Level of Assurance (LoA)	LoA	Level of assurance or reassurance. See eIDAS reference.
Pseudonym	PersonIdentifier	Identifier of a natural person.
IdType	Type of electronically readable document.	
Document Number	IdNumber	Electronically Readable Document Number.

Pseudonym - meaningless directional identifier

The pseudonym, or natural person identifier, transmitted from the NIA is unique and immutable for each qualified service provider. It does not serve as a public identifier, but as a technical identifier. Should a situation arise where the pseudonym for a natural person changes, the authority will be informed of this fact through the basic registers information system, as its agenda identifier of the natural person will also change. The private data user will not be notified of this change as he cannot be connected to the basic registers indirectly, but this service can be provided by his superior authority.

However, if the qualified service provider wants to be sure that the pseudonym is up-to-date, it has to follow the rules of linked data pool, i.e. to have its data trunk identified and to receive notifications from basic registers information system.

Rules for the National Identity Authority

A fundamental requirement of security and transparency for public administration information systems is the requirement for uniform electronic identification of external users. For each operation, knowledge of the person performing the operation is required, especially in terms of the undeniable responsibility of the person. External users (clients) of public administration information systems must be uniquely identified, in particular for reasons of personal data protection and from a procedural point of view, as provided for in the Administrative Procedure Code (unambiguous proof of the identity of the parties to the proceedings).

The access management task for each public administration information system consists of the following steps:

- **Identification -** unambiguous and undeniable identification of the natural person accessing the public administration information system
- **Authentication** - proving that the accessing person is the person he/she claims to be. Authentication takes place by presenting **authentication means** (e.g. username and password, authentication certificate) assigned to the person by the administrator of the information system
- **Authorisation** - on the basis of the data about the identified and authenticated person and other data about this person (for example, job classification), assignment of the person to the appropriate role and the resulting evaluation of the authorisation for actions and data within the information system.

The NAP requires the following principles to be implemented for all public administration information systems in this area:

1. Any authority that provides its services electronically and needs an authenticated client for them must use the services of a qualified electronic identification system (currently only NIA) where identity verification is required by law or by the exercise of competence
2. In order to use a qualified electronic identification system, an organisation must become a Qualified Service Provider (SeP), following the process described below

3. Each authority must accept not only the identity of a Czech citizen, but of any citizen of the European Union according to eIDAS.
4. When creating the identity space, first make an analysis whether one of the federated identities within the qualified electronic identification system (currently only NIA) is not already sufficient.
5. Any new identity space must be built to be federated within a qualified electronic identification system (currently only NIA)
6. Means of identification and authentication shall always be issued in a secure and unambiguous manner to the identified person so as to ensure a minimum level of trust that is substantial. There shall be a permanent record of this issuance of the means, together with details of how the identity of the person was verified
7. The person to whom the funds have been issued is inherently responsible for protecting the funds from theft and misuse
8. The person to whom the means have been issued shall be solely responsible for all operations performed on the information system using those means
9. The substantive administrator of the agendas that are carried out within the information system is responsible for the assignment of persons to roles (technically carried out by the technical administrator of the information system, but always on the basis of input from the substantive administrators). He may delegate this responsibility to more than one responsible person within the organisational structure.

Qualified Service Provider (SeP) notification procedure

The following steps describe each part of the process outlined below, based on verification through ISDS. Currently, registration of an organisation through the National Point Portal is only available to public authorities, other entities must register directly with the Basic Registry Administration (see step 8). The complete guide is available here.

1. The user, as a representative of an organisation, shall request the service enabling the registration of the organisation from the National Point Portal, which is a Service Provider. This registration allows the organisation to function in NIA and to create individual Service Providers.
2. The National Point Portal contacts the National Identity Authority, which provides the authentication, with a request for authentication of the person (user).
3. For user authentication for organisation registration or individual Service Provider configurations, the Identity Provider is the designated Information System for Data Mailboxes (ISDS). The National Identity Authority will redirect to the data mailbox login.
4. The user authenticates himself by logging in to the data mailboxes. In order to register an organisation on the National Point Portal, the user must be logged in via ISDS (in the defined role and mailbox type of the OVM). If the organisation is not an OVM, registration with the Basic Registry Administration is required.
5. In the case where the user is successfully authenticated, the Data Mailbox Information System will pass an authentication token containing the entity ID and name, the role of the logged-in user and other attributes to the National Identity Authority as a result of the authentication.
6. The National Identity Authority collects the attributes in the Information System of Basic Registers (ISZR) and then checks the existence of the ID.
7. The National Identity Authority transmits to the National Point Portal the necessary attributes from the Basic Registers Information System and the attributes received in the authentication token from the Data Box Information System, which are necessary to process the registration form.
8. Upon successful completion of the previous steps, the National Point Portal shall enable the registration service of the organisation (SeP) and display the completed registration form to the user. This applies only to organisations that are OVMs. If the organisation is not an OVM, detailed information on how to register directly with the Basic Registry Administration is displayed instead of the registration form.
9. The user confirms the correctness of the data and the registration of the organisation (SeP).
10. The National Point Portal processes the received registration request and after successful registration allows the user to configure the individual Service Providers falling under the organisation (list of qualified provider configurations).
11. The user shall perform the Service Provider configuration including the following data:
    - Entity ID

- Qualified Provider Name.
- Description of the qualified provider.
- URL linking to the qualified provider's homepage.
- URL address for submitting requests
- Address for receiving the issued token
- URL to which the user will be redirected when logging out of your website
- Retrieving the certificate
- Address to retrieve the public portion of the encryption certificate from the metadata
- Accessing authentication through the eIDAS gateway
- Qualified provider logo

Example for health service providers

The health service provider is not a public authority and therefore the following steps need to be ensured in addition to the above procedure:

1. Apply to the Ministry of Health to be entered into the register of rights and obligations as an SPMU according to the obligations arising from Acts 250/2017 Coll. and 372/2011 Coll., ideally under the agenda A1086
2. At https://www.eidentita.cz/Home/Ovm log in as an authorised user with the data mailbox of the health service provider
   - A new manual data entry should be offered with a further procedure
   - If it does not appear, follow the general points above - send a data message containing the necessary data (URL, logo....)
3. Edit your profile on https://www.eidentita.cz/Home/Ovm for access by others (IT department e.g.) and manage your profile, configure for the Health Service Provider Patient Portal.

NIA, National Identity Space, National Point, Identity provider, Service provider, IdP, Qualified administrator, Qualified provider, Functional unit