

Materiál Ministerstva vnitra



Export z Národní architektury eGovernmentu ČR

Obsah

Popis Národní identitní autority 3

Seznam poskytovatelů identity (Identity Provider; IdP) 3

Seznam poskytovatelů služeb (Service Provider; SeP) 6

Atributy vydávané poskytovatelům služeb (Service Providerům; SeP) 7

Pseudonym - bezvýznamový směrový identifikátor 8

Nevizuální přihlašování z mobilních aplikací 8

Popis Národní identitní autority

Národní identitní autorita vytváří federativní systém zajišťující orgánům veřejné správy státem garantované služby **identifikace a autentizace**, který se skládá z následujících komponent:

- **Národní bod pro identifikaci a autentizaci** jako centrální bod federativního systému, který zajišťuje komunikaci a registraci účastníků federace. Tato komponenta zajišťuje současně vždy jednoznačné ztotožnění osoby, která prokazuje svoji totožnost s využitím autentizačních prostředků (prostředků pro elektronickou identifikaci). Je definován v zákoně č. 250/2017 Sb. jakožto informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace. Zajišťuje orgánům veřejné správy státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principy Single Sign-On.
- **Kvalifikovaný správce**, který vydává jednoznačně identifikovaným fyzickým osobám prostředky pro vzdálenou autentizaci (prokázání totožnosti) a provádí veškeré činnosti spojené se správou těchto prostředků a prokazováním totožnosti fyzické osoby, tj. spravuje kvalifikovaný systém elektronické identifikace.
- **Kvalifikovaný poskytovatel online služeb**, který připojuje k Národnímu bodu online služby, ke kterým je vyžadováno přihlášení prostředky vydanými kvalifikovanými správci.
- **Základní registry**, které poskytují jednoznačnou identifikaci osoby a zajištění vazeb této osoby vůči referenčním údajům o osobě.
- **Národní uzel eIDAS**, který je samostatnou součástí Národního bodu a zajišťuje přijímání vzdáleného prokázání totožnosti z ohlášených systémů dle nařízení eIDAS a předávání vzdálené identifikace a autentizace z České republiky ostatním státům EU. Ostatní státy EU musí akceptovat české identity od 13.9.2020, kdy vypršela roční lhůta pro zavedení akceptace ohlášeného prostředku **elektronického občanského průkazu**.

Pro osoby uvedené v **ROB** přihlašující se prostředky pro elektronickou identifikaci vydanými v ČR nebo přihlašující se identitou v rámci eIDAS z členských států EU nemusí OVS řešit přihlašovací identity pro své klienty samo.

- V současném stavu **ROB** (stav As-Is) tedy pouze pro občany ČR a cizince s trvalým/přechodným pobytem (cizinec musí být evidován v ROB).
- V budoucím stavu (stav To-Be) pro občany ČR, cizince s trvalým/přechodným pobytem a **jiné fyzické osoby (EJFO)**, které mají k ČR právní či majetkový vztah (zahraniční vlastník nemovitosti, zahraniční lékař, zahraniční student, apod.).

Ačkoliv nyní poskytuje NIA své služby pouze jako "Front-end" řešení za pomoci SAML tokenů, je plánováno i poskytování služeb jako "Back-end" pro využití překladů identity a identifikátorů za pomoci **eGON služeb**.

Seznam poskytovatelů identity (Identity Provider; IdP)

Název identitního prostředku	Typ prostředku	úroveň záruky prostředku (LoA)	Popis	URL	Použití pro mezinárodní ověření identity v eIDAS
eObčanka	Elektronický občanský průkaz s aktivovanou částí elektronické identifikace	Vysoká (nejvyšší možná dle eIDAS)	Přihlášení prostřednictvím nového občanského průkazu vydaného po 1. 7. 2018, který obsahuje čip a jeho elektronická funkcionality byla aktivována. Pro přihlášení tímto občanským průkazem je zapotřebí čtečka dokladů a nainstalovaný příslušný software.	https://info.identitaobcana.cz	ANO - eObčanka je zatím jako jediný prostředek ohlášen dle eIDAS pro potřeby mezinárodní identifikace a autentizace. Její použití je pro ostatní státy v rámci eIDAS povinné k použití od září 2020.
Mobilní klíč eGovernment	Mobilní aplikace s funkcí ověřování QR kódů	Značná	Mobilní klíč eGovernmentu představuje využití přihlašování bez potřeby zadávání dalších ověřovacích kódů. Po jeho instalaci a aktivaci Vám bude umožněno přihlašování ke službám využívajícím elektronickou identifikaci prostřednictvím Národního bodu. Aby vše fungovalo, je nutné mít nainstalovanou aplikaci mobilního klíče na svém mobilním zařízení. Aplikace mobilního klíče je shodná se stávající aplikací mobilního klíče ISDS. Pokud již vlastnitě tuto aplikaci pro přihlašování k datovým schránkám, aktualizací této aplikace získáte i možnost využít ji i pro přihlašování ke službám prostřednictvím Národního bodu. Tento prostředek nevyžaduje od uživatele zadávat při jeho použití žádné hodnoty, stačí pouze vyfotit QR kód mobilním zařízením, anebo jej nechat přečíst z obrazovky téhož mobilního zařízení. Mobilní klíč má dále jednu mimořádnou vlastnost, kterou ostatní prostředky nemohou nabídnout. Díky svému propojení s jádrem systému Národního bodu (NIA) dovoluje zapnout notifikaci přihlášení i jakýmkoliv jiným prostředkem téhož uživatele. To je výrazný bezpečnostní prvek, který dovoluje uživateli být v reálném čase informován o tom, že případně někdo jiný nějaký jeho prostředek zneužil a přihlásil se jím.	https://info.identitaobcana.cz/mep/	NE

Název identitního prostředku	Typ prostředku	úroveň záruky prostředku (LoA)	Popis	URL	Použití pro mezinárodní ověření identity v eIDAS
NIA ID	Jméno + heslo + sms. Klasické přihlašování pomocí druhého faktoru.	Značná	Přihlášení prostřednictvím uživatelského jména a hesla, které jste zadali při založení Vašeho identitního prostředku na portálu národního bodu. Přihlášení dokončíte zadáním ověřovacího kódu, který Vám bude zaslán ve formě SMS na Vaše telefonní číslo.	https://info.identitaobcana.cz/ups/	NE
První certifikační autorita, a.s.	Čipová karta Starcos s identitním certifikátem	Vysoká (nejvyšší možná dle eIDAS)	Přihlášení prostřednictvím čipové karty Starcos společnosti První certifikační autorita, a.s., která byla použita pro generování a uložení privátního klíče identitního komerčního certifikátu. Pro přihlášení budete potřebovat českou čipovou kareť (pokud není integrována do PC/NTB) a nainstalovaný ovládací software SecureStore (ke stažení z www.ica.cz).	https://www.ica.cz/ica-identity-provider	NE
MojID - úroveň "značná"	Přihlašovací údaje do účtu MojID spárovaný s prostředkem FIDO	Značná	Přihlášení prostřednictvím účtu mojID. Pro přihlášení je potřeba zabezpečit účet bezpečnostním klíčem (tokenem) certifikovaným od FIDO Alliance alespoň na úrovni L1, a to buď fyzickým (USB, NFC, Bluetooth), anebo systémovým (Windows Hello, Android v. 7 a vyšší). Dále je nutné mít účet mojID aktivován pro přístup ke službám veřejné správy a jednorázové ověření svou totožnost (již existujícím prostředkem nebo návštěvou Czech POINTu). Službu mojID provozuje CZ.NIC, správce domény .CZ.	https://www.mojid.cz/	NE
MojID - úroveň "vysoká"	Přihlašovací údaje do účtu MojID spárovaný s prostředkem FIDO	Vysoká	Přihlášení prostřednictvím účtu mojID. Pro přihlášení je potřeba zabezpečit účet bezpečnostním klíčem (tokenem) certifikovaným od FIDO Alliance alespoň na úrovni L1, a to fyzickým USB, NFC. Dále je nutné mít účet mojID aktivován pro přístup ke službám veřejné správy a jednorázové ověření svou totožnost (již existujícím prostředkem nebo návštěvou Czech POINTu). Službu mojID provozuje CZ.NIC, správce domény .CZ.	https://www.mojid.cz/	NE
IIG - International ID Gateway	Výběr z možných identitních prostředků, které jsou ohlášeny jinými členskými státy EU v rámci eIDAS uzlů	nízká až vysoká dle daného prostředku	Aktuálně je možné v rámci eIDAS uzlů vybrat z prostředků, které jsou zveřejněny na stránkách eIDAS https://ec.europa.eu/cedigita/wiki/display/EDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS		NE
Bankovní identita	Identita poskytovaná Československou obchodní bankou, a.s.	Značná		https://www.csob.cz/portal/csob/csob-identita	Ne
	Identita poskytovaná Českou spořitelnou, a.s.	Značná		https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita	Ne
	Identita poskytovaná Bankou CREDITAS a.s.	Značná		https://www.creditas.cz/	Ne
	Identita poskytovaná Komerční bankou, a.s.	Značná		https://www.kb.cz/cs/podpora/bankovnictvi-a-nastroje/kb-bankovni-identita	Ne
	Identita poskytovaná Air Bankou, a.s.	Značná		https://www.airbank.cz/produkty/bankovni-identita/	Ne
	Identita poskytovaná Fio Bankou, a.s.	Značná		https://www.fio.cz/bankovni-sluzby/bankovni-identita	Ne
	Identita poskytovaná MONETA Money Bank, a.s.	Značná		https://www.moneta.cz/otevrene-bankovnictvi/bankovni-identita	Ne
	Identita poskytovaná Raiffeisenbank, a.s.	Značná		https://www.rb.cz/informacni-servis/pro-media/tiskove-zpravy/tiskove-zpravy-2021/tiskove-zpravy-202109/01092021-bankovni-identita	Ne
	Identita poskytovaná UniCredit Bank Czech Republic and Slovakia, a.s.	Značná		https://www.unicreditbank.cz/cs/obcane/bankID.html	Ne

Statistiky využití identitních prostředků



Data jsou informativní a platná v konkrétním čase
30.3.2023

Celkem státních ID prostředků		1 518 591
Celkem nestátních ID prostředků		10 565 485
Celkem ID prostředků		12 084 076
Počet profilů alespoň s jedním aktivním prostředkem		6 087 908
Celkový počet unikátních přihlášení		2 432 241
Konverze - procentuální zastoupení těch, kdo se skutečně přihlásili z těch, kdo se přihlásit mohli		39.95% %
Identitní prostředek	Popis počtu	Počet
eObčanka (od 1.7.2018):	Počet aktivovaných prostředků	669 250
	Počet aktivních prostředků	553 811
	Počet aktivních unikátních identit	553 778
	Počet přihlášení	1 960 980
	Unikátních přihlášení	62 446
NIA ID (dříve „Jméno, Heslo, SMS“) (od 1.7.2018):	Počet aktivovaných prostředků	357 741
	Počet aktivních prostředků	347 966
	Počet aktivních unikátních identit	347 965
	Počet přihlášení	8 176 219
	Unikátních přihlášení	333 713
Mobilní klíč eGovernmentu (od 16.11.2020):	Počet aktivovaných prostředků	506 208
	Počet aktivních prostředků	468 963
	Počet aktivních unikátních identit	372 402
	Počet přihlášení	10 011 957
	Unikátních přihlášení	381 271

Identitní prostředek	Popis počtu	Počet
Technicky IdP pro mobilní aplikace	Počet aktivovaných prostředků	149 314
	Počet aktivních prostředků	147 851
	Počet aktivních unikátních identit	66 006
	Počet přihlášení	501 624
	Unikátních přihlášení	66 354
Bankovní identita Air Bank:	Počet aktivovaných prostředků	1 513 739
	Počet aktivních prostředků	1 274 839
	Počet aktivních unikátních identit	729 574
	Počet přihlášení	2 201 696
	Unikátních přihlášení	214 223
Bankovní identita Banka CREDITAS - Pilot:	Počet aktivovaných prostředků	56
	Počet aktivních prostředků	47
	Počet aktivních unikátních identit	47
	Počet přihlášení	145
	Unikátních přihlášení	26
Bankovní identita Česká spořitelna:	Počet aktivovaných prostředků	3 096 849
	Počet aktivních prostředků	2 322 191
	Počet aktivních unikátních identit	2 320 468
	Počet přihlášení	6 670 709
	Unikátních přihlášení	634 986
Bankovní identita ČSOB Identita - plně ověřený přístup	Počet aktivovaných prostředků	2 788 564
	Počet aktivních prostředků	1 650 161
	Počet aktivních unikátních identit	1 556 137
	Počet přihlášení	4 337 035
	Unikátních přihlášení	426 822
Bankovní identita ČSOB Identita - rychlý přístup	Počet aktivovaných prostředků	1 716 823
	Počet aktivních prostředků	1 600 447
	Počet aktivních unikátních identit	1 514 433
	Počet přihlášení	91 618
	Unikátních přihlášení	36 979
Bankovní identita Fio banka:	Počet aktivovaných prostředků	618 021
	Počet aktivních prostředků	612 232
	Počet aktivních unikátních identit	612 221
	Počet přihlášení	393 833
	Unikátních přihlášení	63 247
První certifikační autorita, karta Starcos:	Počet aktivovaných prostředků	2 173
	Počet aktivních prostředků	932
	Počet aktivních unikátních identit	902
	Počet přihlášení	170 349
	Unikátních přihlášení	818
Bankovní identita Komerční banka:	Počet aktivovaných prostředků	1 042 678
	Počet aktivních prostředků	977 404
	Počet aktivních unikátních identit	922 854
	Počet přihlášení	3 681 846
	Unikátních přihlášení	313 741

Identitní prostředek	Popis počtu	Počet
MojID - úroveň "značná":	Počet aktivovaných prostředků	111 848
	Počet aktivních prostředků	86 851
	Počet aktivních unikátních identit	72 631
	Počet přihlášení	1 655 765
	Unikátních přihlášení	73 290
MojID - úroveň "vysoká":	Počet aktivovaných prostředků	4 736
	Počet aktivních prostředků	4 484
	Počet aktivních unikátních identit	4 255
	Počet přihlášení	43 335
	Unikátních přihlášení	3 561
Bankovní identita MONETA Money Bank:	Počet aktivovaných prostředků	1 107 892
	Počet aktivních prostředků	979 848
	Počet aktivních unikátních identit	650 671
	Počet přihlášení	1 400 315
	Unikátních přihlášení	159 679
Bankovní identita Raiffeisenbank:	Počet aktivovaných prostředků	1 319 659
	Počet aktivních prostředků	810 944
	Počet aktivních unikátních identit	807 448
	Počet přihlášení	1 201 408
	Unikátních přihlášení	144 640
Bankovní identita UniCredit Bank:	Počet aktivovaných prostředků	252 423
	Počet aktivních prostředků	245 105
	Počet aktivních unikátních identit	243 916
	Počet přihlášení	40 078
	Unikátních přihlášení	10 450

Seznam poskytovatelů služeb (Service Provider; SeP)

Poskytovatelů služeb je již více než 50 a v přípravě jsou další. Konečný počet je v řádu stovek. Aktuální seznam je dostupný zde <https://info.identitaobcana.cz/sep/>.

Podobně jako jsou jiné státy v rámci eIDAS povinny přijímat české ohlášené prostředky identity (eObčanka), jsou čeští poskytovatelé služeb povinni akceptovat identitu ohlášenou jiným státem v rámci eIDAS. Povinnost umožnit přihlášení pomocí IIG - International Identity Gateway je všem poskytovatelům služeb zapnuta od 30.6.2020. Současné znění nařízení eIDAS, povazuje členské státy, které oznámily systém elektronické identifikace, aby zajistily jedinečnou identifikaci osoby.

Nicméně je vhodné na tomto místě upozornit, že pomocí údajů obdržených na základě využití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému elektronické identifikace, nemusí být vždy možné udělat jednoznačný „identity matching“ – tj. jednoznačné ztotožnění osoby, která se přihlašuje pomocí „zahraničního“ prostředku pro elektronickou identifikaci s údaji, které vede poskytovatel online služeb. Pro účely „identity matchingu“ by pak mohl posloužit také údaj (či údaje), který by musel zadat sám uživatel. Nejlépe samozřejmě údaj, který by měl být znám ze své podstaty pouze samotnému uživateli. Výše uvedené vychází z předpokladu spolehnout se na základní osobní údaje obdržené na základě využití prostředku pro elektronickou identifikaci a na údaj (či údaje), které doplní sám uživatel. Seznam dostupných atributů u jednotlivých ohlášených systémů elektronické identifikace je k dispozici na:

<https://ec.europa.eu/cedigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes>.

Atributy vydávané poskytovatelům služeb (Service Providerům; SeP)

Následující atributy jsou NIA vydávány tzv. kvalifikovaným poskytovatelům služby. Problematika je popsána také v části [Portály veřejné správy a soukromoprávních uživatelů údajů](#). Tučně označené atributy odpovídají standardu eIDAS, ostatní atributy sice standardu neodpovídají, kvalifikovaný poskytovatel služby má ale možnost při komunikaci v rámci ČR o jejich vydání požádat.

Atribut/Element	Název atributu	Popis
Příjmení	CurrentFamilyName	Referenční údaj – Příjmení fyzické osoby. Viz eIDAS reference.
Jméno	CurrentGivenName	Referenční údaj – Jméno, případně jména fyzické osoby. Viz eIDAS reference.
Datum narození	DateOfBirth	Referenční údaj – Datum narození fyzické osoby. Viz eIDAS reference.
Místo narození	PlaceOfBirth	Referenční údaj – Místo narození fyzické osoby. Viz eIDAS reference.
Země narození	CountryCodeOfBirth	Referenční údaj – Země narození fyzické osoby, předávána v kódu podle standardu ISO 3166-3.
Adresa pobytu	CurrentAddress	Referenční údaj – Adresa pobytu fyzické osoby, je předávána zakódovaná pomocí BASE64. Obsahuje (pokud je uvedeno v ROB) název ulice (Thoroughfare), název pošty (PostName), PSČ (PostCode), název obce, případně doplněnou o část obce (CvaddressArea) a číslo domovní/číslo orientační (LocatorDesignator). Atribut vychází z ISA Core Vocabulary a tam je také uveden podrobnější popis atributu.
Email	Email	Emailová adresa uvedená na Portálu NIA (přihlášení na identitaobcana.cz) v sekci „Vaše údaje“.
Je starší než X	IsAgeOver	Výpočet je starší než X podle referenčního údaje Datum narození.
Věk	Age	Výpočet věku podle referenčního údaje Datum narození.
Telefon	PhoneNumber	Telefonní číslo uvedeno na identitaobcana.cz v sekci „Vaše údaje“.
Adresa pobytu (předávaná v podobě RÚIAN kódů)	TRadresaID	Referenční údaj – Adresa pobytu fyzické osoby je předávána v kódech podle RÚIAN. Obsahuje (pokud je uvedeno v ROB) kódy pro okres, obec, část obce, ulici, PSČ, stavební objekt, adresní místo, číslo domovní a orientační.
Level of Assurance (LoA)	LoA	Stupeň (úroveň) jistoty nebo zajištění. Viz eIDAS reference.
Pseudonym	PersonIdentifier	Identifikátor fyzické osoby.
Typ dokladu	IdType	Druh elektronicky čitelného dokladu.
Číslo dokladu	IdNumber	Číslo elektronicky čitelného dokladu.

Při použití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému elektronické identifikace se množina osobních údajů (v případě fyzických osob) skládá minimálně z následujících údajů:

- příjmení,
- jméno,
- datum narození a
- unikátního identifikátoru (pseudonymu).

Seznam dostupných atributů u jednotlivých ohlášených systému elektronické identifikace je k dispozici na: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes>.

Při použití prostředku pro elektronickou identifikaci vydaného v rámci „zahraničního“ oznámeného systému

elektronické identifikace nicméně není možné využít [služby základních registrů E226 eidentitaCtiAifo](#) pro překlad pseudonymu na AIFO dané agendy.

Pseudonym - bezvýznamový směrový identifikátor

Pseudonym při použití prostředku pro elektronickou identifikaci vydaného v ČR, neboli bezvýznamový identifikátor fyzické osoby, který se od NIA předává je pro každého kvalifikovaného poskytovatele služby, je jedinečný a neměnný. Neslouží jako veřejný identifikátor, ale jako [identifikátor technický](#). Pokud by došlo na situaci, kdy se pseudonym pro fyzickou osobu změní, bude úřad o této skutečnosti informován prostřednictvím informačního systému základních registrů, protože se mu změní i [agendový identifikátor fyzické osoby](#). Soukromoprávní uživatel údajů o této změně nebude notifikován, protože nemůže být napojen na [základní registry](#) nepřímo, avšak tuto službu mu může zprostředkovat jeho nadřízený úřad.

Pokud však chce mít kvalifikovaný poskytovatel služby jistotu o aktuálnosti pseudonymu, musí postupovat dle pravidel [propojeného datového fondu](#), tzn. mít ztotožněn svůj datový kmen a odebírat [notifikace z informačního systému základních registrů](#).

Nevizuální přihlašování z mobilních aplikací

Principem tzv. nevizuálního přihlašování je uspořádání, kdy konkrétní instance aplikace daného uživatele byla jednorázově zaregistrována v Národním bodu (NIA), prostřednictvím klasického vizuálního přihlášení. Pro běžné použití této aplikace pak stačí ověření uživatele při vstupu do této mobilní aplikace (typicky otisk prstu, fotografie obličeje, nebo PIN). Jakmile se uživatel dostane do mobilní aplikace a ta zjistí, že od posledního přihlášení k NIA uběhla více než určitá doba (vývojářům aplikace je doporučeno dodržovat hodnotu 24 hodin), provede aplikace automatické přihlášení daného uživatele k NIA a to způsobem, který nevyžaduje žádnou jeho interakci. Tímto způsobem se mobilní aplikace dozví o možné změně údajů daného uživatele, ke které mezitím v [ROB](#) mohlo dojít, například změna příjmení atp. Uživatel má dále možnost vyhledat si v konfiguraci NIA seznam, zobrazující které mobilní aplikace má připojené v režimu nevizuálního přihlašování a z jakého zařízení. V případě potřeby (například ztráty svého mobilního telefonu) je pak možno v tomto seznamu konkrétní aplikaci odpojit. Aby se tento fakt mobilní aplikace dozvěděla a uvedla sama sebe do nezaregistrovaného stavu, je mobilní aplikace povinná v pravidelných intervalech volat příslušnou službu. Doporučená hodnota periodicity tohoto volání je vývojářům mobilní aplikace doporučena v úrovni 60 minut.

NIA poskytuje soubor rozhraní, které mají za cíl umožnit poskytovatelům služeb (SeP) vytvoření takových vlastních mobilních aplikací a vlastních backendových API, které dohromady budou umět ověřit identitu občana prostřednictvím volání webových služeb, tedy nevizuálně bez interakce občana.

Původně generická Mobilní aplikace bude muset být uživatelem nejprve registrována k užívání a následně bude umožňovat opakované přihlašování k NIA nevizuálním způsobem. Mobilní aplikace bude předávat informaci o provedeném přihlášení do API poskytovatele služeb, které následně z NIA získá JSON Web Token s detaily o přihlášeném uživateli. Fakt registrace bude opakovaně kontrolován na NIA prostřednictvím procesů mobilní aplikace a API, aby uživatel mohl např. při ztrátě zařízení možnosti nevizuálního přihlašování zabránit.

Cílem funkcionality není, aby mobilní aplikace poskytovatele služeb byla na úrovni poskytovatele identity (není to Identity provider). Není ji tedy možné používat pro přihlašování k portálům a jiným službám ostatních poskytovatelů služeb.

Více viz popis [na stránkách SZR ČR](#).

From:

<https://archi.gov.cz/> - **Architektura eGovernmentu ČR**

Permanent link:

https://archi.gov.cz/nap:popisy:popis_nia

Last update: **2021/04/30 10:14**

