

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Identifikace klientů veřejné správy	3
<i>Popis identifikace klientů veřejné správy</i>	3
<i>Pravidla pro identifikace klientů veřejné správy</i>	5

Identifikace klientů veřejné správy

Popis identifikace klientů veřejné správy

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografie držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nespĺňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Aby mohla fyzická identifikace fungovat jak při aktuální potřebě (člověk se v daný čas dostaví na místo), tak i při historické potřebě (ověření platnosti identifikačního dokladu z historické smlouvy), budou služby eGovernmentu poskytované přes [Referenční rozhraní](#) rozšířeny o službu, která na jakékoliv historické číslo a typ identifikačního dokladu vrátí, zda byl v požadované době platný a aktuální údaje držitele tohoto historického identifikačního dokladu.

Fyzická identifikace pro osoby bez identifikačního dokladu

Ačkoliv předcházející text předpokládá identifikaci pouze prostřednictvím identifikačních dokladů, existují situace, kdy osoba nemá možnost se tímto identifikačním dokladem prokázat. Typicky jde o děti pod 15 let či cizince. Základním předpokladem, aby mohla proběhnout identifikace i těchto osob je jejich evidence v informačním systému veřejné správy, napojený na [propojený datový fond](#) a následné vydávání potvrzení či úřední/veřejnou listinu, které může zastat roli identifikačního dokladu. Pro osoby do 15 let to může být rodný list vedený v jednom z [editorských agendových informačních systémů](#) nebo povolení o přechodném pobytu pro cizince.

Některé z těchto listin - například povolení k trvalému pobytu, azylový štítek či vízový štítek jsou již dnes vedeny v [základním registru obyvatel](#), avšak jejich použití pro identifikaci není plně dořešeno.

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s [Informační koncepcí ČR](#) a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní zátěže.

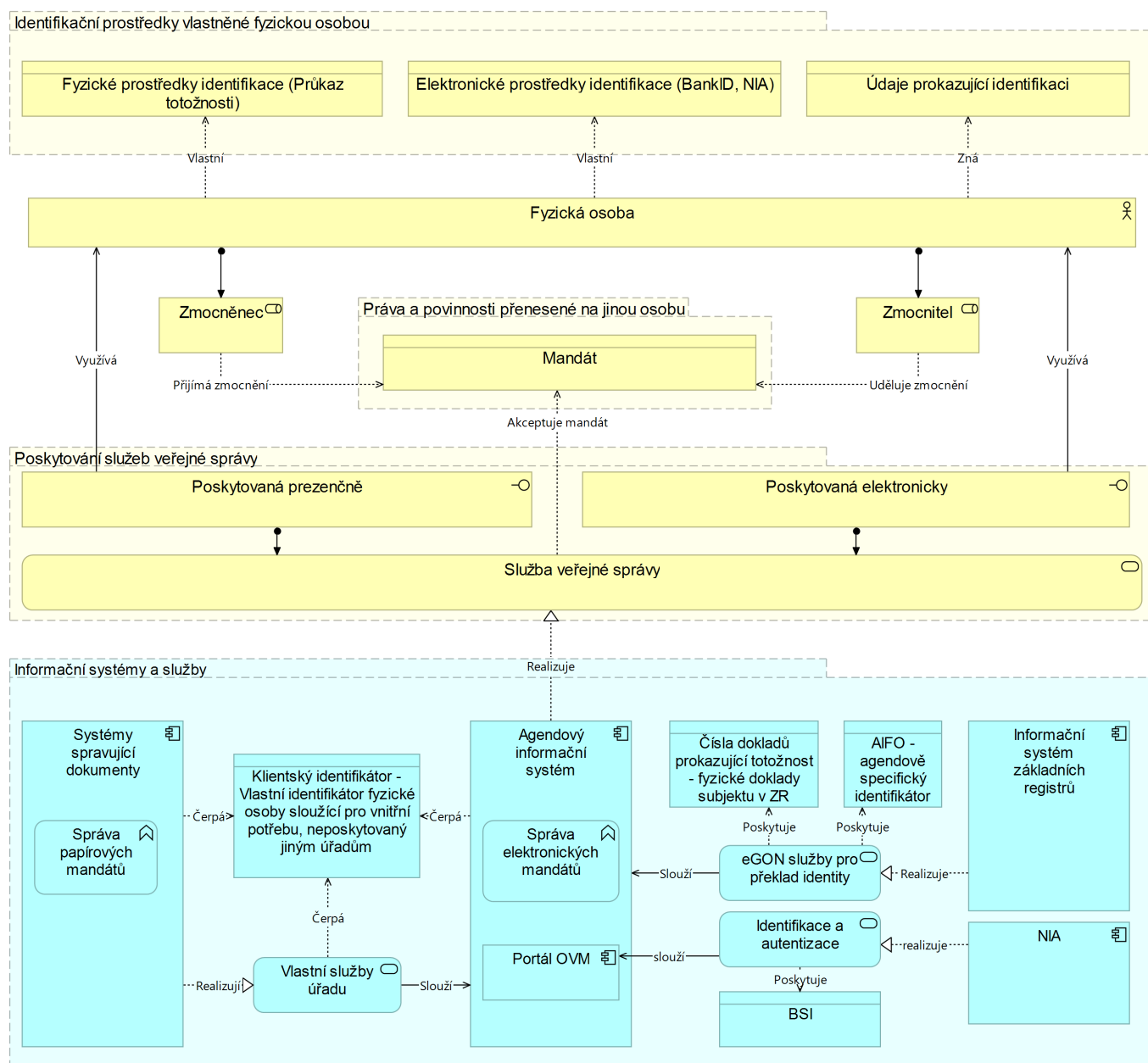
[Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2](#) povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace. Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožňuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma Národní identitní autority (také jako NIA), která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Mandáty, práva a role v elektronické identifikaci pro klienty veřejné správy

Kvalifikovaný poskytovatel elektronických služeb **bude nadále zodpovědný** za řízení oprávnění (autorizaci) fyzické osoby, která prokázala takto svoji totožnost. Nadále tedy musí provádět správu oprávnění na základě údajů o osobě, které získá z **Propojeného datového fondu** a vlastních údajů vedených v agendě.

Pohled na identifikaci a identifikátory klientů VS



Pravidla pro identifikace klientů veřejné správy

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografii držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nespĺňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Samotný občanský průkaz, který může sloužit i k elektronické identifikaci, lze použít k fyzické identifikaci na různé úrovni:

- Střední úroveň
 - Zjištění, zda nejde o padělaný občanský průkaz
 - [Strojově čitelné občanské průkazy](#)
 - [Ostatní občanské průkazy](#)
 - Zjištění, zda je předložený občanský průkaz platný
 - [Seznam platných občanských průkazů](#)
 - [Seznam neplatných občanských průkazů](#)
 - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
- Vysoká úroveň
 - Zjištění, zda nejde o padělaný občanský průkaz
 - [Strojově čitelné občanské průkazy](#)
 - [Ostatní občanské průkazy](#)
 - Zjištění, zda je předložený občanský průkaz platný
 - [Seznam platných občanských průkazů](#)
 - [Seznam neplatných občanských průkazů](#)
 - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
 - Vyžádání si aktuálních údajů, včetně fotografie, o klientovi, který jej předložil a jejich kontrola

Fyzická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (buď i nepřímo, např. je-li právnická osoba statutárním orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Pro použití ve fyzickém prostředí se identifikační prostředky právnických osob v České republice nevydávají. Je tomu tak proto, že právnická osoba není ve fyzickém prostoru přítomna a vždy za ni jedná fyzická osoba, která prokazuje svou vlastní totožnost.

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s [Informační koncepcí ČR](#) a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní

zátěže.

[Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2](#) povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím [kvalifikovaného systému elektronické identifikace](#). Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožňuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma [Národní identitní autority \(také jako NIA\)](#), která vykonává činnosti Národního bodu dle [§ 20](#) a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Elektronická identifikace právnických osob

Pokud jde o právnické osoby v pojetí českého právního řádu, tyto nemohou z jejich povahy nikdy právně jednat samy, musí za ně vždy jednat zástupce, kterým je (byť i nepřímo, např. je-li právnická osoba statutárním orgánem jiné právnické osoby) finálně vždy fyzická osoba (příp. fyzické osoby). Z toho plyne, že ustanovení [§ 2](#) zákona o elektronické identifikaci, které dopadá na případy fyzických osob, se tak vztahuje i na jednání právnických osob, neboť jsou to vždy fyzické osoby, které fakticky jednají, ať již za sebe, či za jinou fyzickou osobu nebo právnickou osobu.

V elektronickém prostředí, zejména jde-li o automatizovanou komunikaci, jsou nicméně používány mechanismy, které mají charakter identifikačního prostředku právnické osoby. Jde např. o certifikát pro evidenci tržeb podle zákona č. 112/2016 Sb., o evidenci tržeb, nebo certifikáty vydané Českou národní bankou pro automatizovanou komunikaci mezi ČNB a subjekty podléhající jejímu doзору, typicky bankami. Platí nicméně, že identifikační prostředky právnických osob s použitím bez ohledu na agendy, ekvivalentní např. občanským průkazům, se v České republice nevydávají.

Zatímco samotná autentizace fyzické osoby není problematická, problematická se jeví otázka určení, zda fyzická osoba jedná v dané situaci za sebe (popř. v jaké roli za sebe) anebo zda jedná za jinou fyzickou osobu nebo za právnickou osobu. Problematika mandátů a oprávnění je řešena [níže](#).

Skutečnost, že daná fyzická osoba, má právo se identifikovat a autentizovat za určitou právnickou osobu (tj. „přihlásit se ke službě jménem právnické osoby“), ještě nezakládá bez dalšího právo na to, že tato fyzická osoba má právo za danou právnickou osobu činit úkony prostřednictvím digitální služby. Autorizaci dané fyzické osoby k poskytnutí digitální služby musí posoudit ten, ke komu se fyzická osoba hlásí na základě jím dostupných údajů (informace z obchodního rejstříku, plná moc opravňující konkrétní osobu jednat jménem právnické osoby,...) ve spojení s příslušnými právními předpisy.

Jako příklad takového přístupu můžeme uvést datové schránky, do nichž se fyzická osoba přihlásí například novým občanským průkazem s aktivovaným čipem. Po úspěšné autentizaci s pomocí prostředku pro elektronickou identifikaci (tj. např. s pomocí „eObčanky“) a souhlasu s předáním osobních údajů na portálu [Národního bodu pro identifikaci a autentizaci](#), je fyzická osoba pro účely [informačního systému datových schránek \(ISDS\)](#) ztotožněna. Po ztotožnění tak nabídne ISDS fyzické osobě seznam datových schránek, ve vztahu k nimž je přihlášená fyzická osoba oprávněná jednat.

Autentizovaná fyzická osoba si tedy vybírá, za koho a v jaké roli bude prostřednictvím [datových schránek](#) jednat. Informaci o tomto oprávnění si ISDS obstarává např. z [ROS](#), z jiných zdrojů (např. údaj o tom, že určitá osoba je advokátem nebo insolvenčním správcem) anebo jej vede na základě sdělení samotného držitele datové schránky (např. údaj o tzv. pověřené osobě). Bez ohledu na zdroj informace o oprávnění k zastupování jiné osoby, resp. na zdroj informace o roli je však na samotném ISDS jakožto poskytovateli služeb, aby oprávnění k zastupování jiné osoby ve svém prostředí řádně implementoval tak, aby osoby mohly toto oprávnění realizovat.

Nabídka jednotlivých oprávnění, resp. rolí, tedy spadá do kompetence daného poskytovatele služeb a odvíjí se od údajů a oprávnění, které vede v rámci svého informačního systému nebo od údajů, ke kterým má přístup.

Mandáty, role a práva v elektronické komunikaci

Zajištění správné obsazení do role neboli autorizace, klienta využívajícího elektronické služby je jedním ze základních předpokladů jejího správného fungování. Různé role mají v rámci služby různá oprávnění a povinnosti a poskytovatel služby je povinen nabídnout klientovi veškeré role, do kterých se v rámci služby může pasovat, včetně rolí jako zástupce právnické osoby, zástupce nezletilého, registrující lékař pacienta a další. Tyto role s oprávněními vůči jiným klientům veřejné správy jsou mandáty. Aby proběhlo správné obsazení do role a zjištění mandátu, je pro poskytování elektronických služeb klientům veřejné správy nutné mít zajištěno několik základních náležitostí:

1. Znalost typů mandátů při jednání s veřejnou správou
2. Jednoznačnou identifikaci a autentizaci klienta veřejné správy
3. Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu
4. Vlastní zajištění autorizace klienta veřejné správy

Mandáty pro jednání s veřejnou správou

Při výkonu veřejné správy a to zejména při jakékoliv interakci a komunikaci s klientem veřejné správy je nutné, aby veřejná správa respektovala mandáty k zastupování jedné osoby druhou na základě různých titulů. Zjednodušeně se dá rozdělit forma mandátu zastupování dle následující tabulky.

Typ subjektu	Mandát
Fyzická osoba	Jednající sama svým jménem
	Jednající jménem jiné fyzické osoby ze zákona: <ul style="list-style-type: none"> - rodič dítěte, - manžel/manželka, - registrovaný partner/partnerka, - opatrovník, osvojitel, poručík, pěstoun - dědic, exekutor, - zastupující osoba pro osoby neschopné jednat nebo nemající zákonného zástupce
	Jednající jménem jiné fyzické osoby ze zmocnění: <ul style="list-style-type: none"> - plná moc, - advokát, - zastupující FO, - jiný druh zmocnění, - na žádost bez zmocnění
	Plná moc opravňující konkrétní osobu jednat jménem právnické osoby

Typ subjektu	Mandát
Fyzická osoba jednající za právnickou osobu	Jednatel právnické osoby
	statutární zástupce právnické osoby (jedna FO)
	Statutární orgán právnické osoby (více FO)
	Insolvenční správce
	Likvidátor
	Jednající jménem zřizovatele právnické osoby
	Pověřen k jednání za právnickou osobu: - Veřejnoprávním titulem, - Soukromoprávním titulem (smlouva, plná moc, společenská smlouva, apod.)
	Pokud agendový předpis povoluje využívání přístupových údajů k systému datových schránek jako identifikačních prostředků je to dále: a) Pro fyzické osoby - statutární zástupce oprávněné k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). b) Pro fyzické osoby - oprávněné statutárním zástupcem k přístupu do datové schránky právnické osoby ověřením oprávnění k datové schránce právnické osoby prostřednictvím Informačního systému datových schránek (ověření přístupových údajů a oprávnění). c) Ověřením speciálního agendového oprávnění podle agendového předpisu, na jehož základě jsou poskytovány agendové digitální služby.

Příklady mandátů pro fyzické osoby vyplývající z některých vyhlášek a nařízení měst a obcí:

- Pro přihlášení k platbě poplatku za odvoz komunálního odpadu
- Pro přihlášení k platbě poplatku:
 - ubytovacího,
 - ze psa,
 - za zábor a užívání veřejného prostranství.
- Pro převody, koupě, prodej, nabytí městského majetku, (provozovny v budovách v majetku města)
- Pro užívání, podnájem, zrušení užívání bytového fondu města
- Mandát pro jednání s knihovnou - výpůjčky registrovaného čtenáře

Jak je zdůrazněno níže, při výkonu veřejné správy je nutné, aby příslušný orgán konající nějakou činnost v rámci dané agendy věděl, pro jakou formu zastupování je mandát umožněný nebo dokonce nutný. Zcela jiným způsobem se orgán veřejné moci bude chovat k mandátu plynoucímu z veřejnoprávního titulu rodičovství a jinak k mandátu plynoucímu ze soukromoprávního titulu plné moci.

Je také vhodné rozlišovat účel mandátu, tedy typ úkonů, které prostřednictvím zastupované osoby klient veřejné správy dělá. Ty je možno rozdělit do následujících skupin:

- Nahlížení na údaje subjektů práva bez jakéhokoliv interaktivního využívání či zapisování údajů (informační účel).
- Přístup k údajům subjektů a jejich reklamace, nebo pokud je přímo umožněna editace klientům veřejné správy (transakční účel).
- Zmocnění k přístupu či využívání údajů subjektu práva pro třetí strany, nebo poskytnutí údajů z ISVS třetím stranám (zmocňovací účel).
- Činění podání a úkonů vůči orgánům veřejné správy (účel úkonu).
- Využívání elektronických klientských služeb jako je objednání se k úředníkovi.
- Zápis, úprava a zrušení mandátu.

Jednoznačná identifikace a autentizace klienta veřejné správy

Všechny subjekty povinné dle [zákona č. 250/2017 Sb., o elektronické identifikaci](#) mají povinnost dle §2 využívat k prokázání totožnosti při elektronickém kontaktu pouze kvalifikovaný systém, konkrétně:

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s

využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.“

Kvalifikovaný systém spravuje kvalifikovaný správce (státní orgán nebo akreditovaná osoba) a splňuje technické normy i specifikace Evropské unie a především je propojen s národním bodem pro identifikaci a autentizaci – tzv. Národní identitní autorita (NIA).

Identifikace a autentizace prostřednictvím NIA zajistí jen a pouze službu ověřené identity fyzické osoby, neboli každý systém čerpající služby NIA, se může spolehnout na to, že přihlášená fyzická osoba je skutečná ta, za kterou se vzdáleně a elektronicky vydává. Již se dále nezajišťují další služby typu autorizace.

Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu

Systém poskytující elektronické služby veřejné správy musí být schopen komunikovat a získávat údaje z [propojeného datového fondu](#). K tomu musí systém odpovídat předpisům:

- [Zákon 365/2000 Sb.](#), o informačních systémech veřejné správy. Systém klasifikovaný jako Informační systém veřejné správy (ISVS) využívající referenční rozhraní veřejné správy.
- [Zákon 111/2009 Sb.](#), o základních registrech. Systém klasifikovaný jako agendový informační systém (AIS) využívající údaje základních registrů a editorů základních registrů dle svého agendového zákona.
- [Zákon 250/2014 Sb.](#), o elektronické identifikaci. Systém, který vyžaduje ověření totožnosti
- Nařízení eIDAS

Více o využívání údajů propojeného datového fondu a infrastruktury referenčního rozhraní je napsáno v kapitolách:

- [eGON Service Bus/Informační systém sdílené služby](#)
- [Centrální místo služeb](#)
- [Propojenný datový fond](#)

Centrální sdílené služby eGovernmentu dokáží zajistit následující mandáty pro fyzické osoby, které se prokázaly u poskytovatele služeb svou zaručenou elektronickou identitou:

- eGON služba [rosCtiPodleUdaju](#), [rosCtilco](#), [rosCtiAifo](#) (základní registr osob)
 - pro zajištění ověření, zda je fyzická osoba statutárním zástupcem
- eGON služba [aiseoCtiPodleUdaju](#), [aiseoCtiAifo](#) (agendový informační systém evidence obyvatel)
 - pro zajištění ověření, zda je fyzická osoba rodič nezletilého, který není svéprávný
 - pro zajištění ověření, zda je fyzická osoba zákonným zástupcem jiné fyzické osoby
 - pro zajištění ověření, zda je fyzická osoba opatrovníkem jiné fyzické osoby
 - pro zajištění ověření, zda je fyzická osoba manžel/manželka
- eGON služba [isknCtiVlastniky](#) (informační systém katastru nemovitostí)
 - pro zajištění ověření, zda je fyzická osoba vlastníkem nemovitosti
- Služba ISDS
 - Pro zajištění, zda je fyzická osoba pověřená k činění úkonů v ISDS vlastníkem datové schránky

Žádné další centrální služby ověření oprávnění/mandátů se v současné, ani dohledné době, neplánují. Proto je důležité, aby si každý poskytovatel elektronických služeb zajistil jiné typy mandátů sám.

Vlastní zajištění autorizace klienta veřejné správy

Každá vykonávaná agenda (výkon veřejné správy) může pro svoji potřebu vyžadovat jiné mandáty. Například mandát podání daňového přiznání za jinou fyzickou osobu, mandát nahlížení na zdravotnickou dokumentaci jiné fyzické osoby, nakládání s majetkem právnické osoby, u které nejsem statutární zástupce, či například mandát k zastupování při dědickém řízení.

Všechny tyto mandáty se musí řešit v rámci dané agendy a jako ideální řešení navrhuje:

- Zřídít buď v jednotlivých agendových informačních systémech, nebo v rámci centralizované správy subjektů mandátní registr.
- V rámci mandátního registru určit předem definované typy mandátů přípustné v dané agendě a způsob zápisu mandátů pro nahlížení a pro transakce ze strany klienta
- Povolit zapisovat všem klientům mandáty dle definovaných typů pod svou zaručenou elektronickou identitou.
- Umožnit klientům přidat mandát i offline, například na přepážce úřadu.
- Při každém přihlášení klienta kontrolovat kromě mandátů z centrálních sdílených služeb eGovernmentu i vlastní mandátní registr a dát vždy při přihlášení vybrat klientovi, v jaké roli a s jakým mandátem chce pracovat.

Je důležité zdůraznit, že veřejná správa nemá rozlišovat formu komunikace a jednání s klientem. Tedy mandát obecně platící pro osobní jednání s úředníkem, nebo pro fyzické provádění úkonů na přepážce, musí mít klient umožněn využívat i při elektronické komunikaci a naopak. Také proto je nutné vést mandáty standardizovanou formou na jednom místě a využívat jich i při elektronické komunikaci klienta.

Mandát plynoucí z veřejnoprávního nebo soukromoprávního titulu a to včetně plných mocí a dohod o zastupování při správním jednání s úřady patří mezi společné rozhodné skutečnosti, tak jak jsou zakotveny v souvisejících ustanoveních Správního řádu (zejména § 6 a § 50 a související). Proto je nanejvýš vhodné, aby příslušný orgán veřejné moci, pokud

- využívá a buduje centrální evidenci subjektů,
- centrální evidenci rozhodných skutečností,
- skutečnosti o zapsaném anebo z něčeho plynoucím mandátu k zastupování,
- je zahrnul do rozhodných skutečností.

Klient se totiž může odvolat na příslušná ustanovení správního řádu a neposkytovat zejména plné moci a další dokumenty, z nichž mandát plyne, úřadu opakovaně.

[NIA](#), [Národní identitní prostor](#), [Identity provider](#), [Service provider](#), [IdP](#), [Tematická oblast](#), [eop](#), [občanský průkaz](#), [identifikační doklad](#), [cestovní pas](#), [mandáty](#), [mandáty v elektronické komunikaci](#), [zastupování](#), [oprávnění](#), [mandát](#)

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

Permanent link:
https://archi.gov.cz/nap:elektronicka_identifikace_pro_klienty_veřejne_spravy

Last update: **2021/04/29 15:20**

