DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Příručka k využití služeb národní identitní autority pro kvalifikované poskytovatele služeb veřejné správy

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA

OBSAH

1. Historie dokumentu

Verze	Datum	Autor	Stav dokumentu / Popis změn
0.1	30. 11. 2016	NAKIT	Vytvoření dokumentu
0.2	2. 12. 2016	Petr Loskot	Formalizace dokumentu
0.3	8. 12. 2016	Lukáš Cimler	Doplnění popisu LoA, Pseudonym a pojmu Portál
0.4	7. 2. 2017	Lukáš Cimler	Úprava vzhledu dokumentu
0.5	23. 2. 2017	Lukáš Cimler	Doplněny odkazy na dokumenty eIDAS, upraven seznam atributů, aktualizace obrazovek
0.6	13. 3. 2017	NAKIT	Úprava členění kapitoly 4 a kapitoly 6 (nyní 6 a 7), doplněny kapitoly 8 a 9, zapracovány připomínky
0.7	27. 3. 2017	NAKIT	Aktualizována Tabulka 1
0.8	31. 3. 2017	NAKIT	Aktualizace vybraných termínů v Seznamu zkratek a pojmů
0.9	24. 7. 2017	NAKIT	Doplnění atributů Typ dokladu a Číslo dokladu do příslušných tabulek
0.10	11. 9. 2017	NAKIT	Upraven namespace v kapitole 9.3.1. Příklad AuthRequest
0.11	6. 2. 2018	NAKIT	Aktualizovány odkazy v kapitole 3.3 Technické specifikace eIDAS
0.12	26. 3. 2018	NAKIT	Aktualizovány příklady v podkapitolách 9.3.1. a 9.3.3., doplněn Typ u 9.4. Příklad atributů NIA a doplněna XSD schémata adres
1.0	25. 6. 2018	NAKIT	Aktualizován název portálu na „Portál národního bodu“. Aktualizovány obrazovky portálu na základě jeho redesignu. Úprava podmínek pro registraci SeP. Doplněna konfigurace SeP o položky s popisem, logem a úvodní URL adresou. Doplněna kapitola „Legislativní rámec“. Použita nová šablona pro dokument.
1.1	20. 8. 2018	NAKIT	Rozšíření popisu podkapitoly 4.2. Portál národního bodu, úprava CurrentAddress dle specifikace eIDAS, doplněny nové podkapitoly 9.3.4. Příklad LogoutRequest a 9.3.5. Příklad LogoutResponse.

Verze	Datum	Autor	Stav dokumentu / Popis změn
1.2	9. 10. 2018	NAKIT	Aktualizována kapitola 4.2. Portál národního bodu.
1.3	19. 10. 2018	NAKIT	Doplněna kapitola 3.4. Bezpečnostní doporučení.
1.4	16. 10. 2018	NAKIT	Aktualizována kapitola 4.2. Portál národního bodu a vybrané obrazovky.
1.5	27. 11. 2018	NAKIT	Doplněna kapitola 9.5. Testovací profily.
1.6	11. 4. 2019	SZR	Doplněna povinnost vložení certifikátu pro šifrování, povinnost LogOut a principů SSO
1.7	21. 08. 2019	NAKIT	Zrušena původní kapitola 7. Vybrané obrazovky portálu národního bodu, Aktualizovány kapitoly 4.2. Portál národního bodu, 6.1. Popis procesu registrace a konfigurace SeP, 7.1. Registrace organizace a 7.2. Konfigurace poskytovatele a vybrané obrazovky. Doplněna nová kapitola 7.3.Správa skupin kvalifikovaných poskytovatelů.
1.8	12. 11. 2019	NAKIT	Nové kapitoly 10. Individuální výdej a 11. Poskytovatel údajů. Aktualizovány kapitoly 4.2. Portál národního bodu, 7.2. Konfigurace poskytovatele služeb a 7.3. Správa skupin kvalifikovaných poskytovatelů.
1.9	20. 02. 2020	NAKIT	Rozšíření popisu načtení certifikátu z metadat v podkapitole 7.2. Konfigurace poskytovatele služeb.
1.10	24. 08. 2020	NAKIT	Zpřístupnění autentizace prostřednictvím brány eIDAS defaultně zapnuto, SeP nemůže vypnout.
1.11	25. 03. 2021	SZR	Nová vložená kapitola 8.1. Přihlášení pomocí mezinárodního eIDAS uzlu, aktualizována kapitola 4.2. Portál národního bodu.
1.12	2. 11. 2021	NAKIT	Aktualizace dokumentu ve vazbě na přechod z eidentita.cz na identitaobcana.cz.
1.13	10. 11. 2021	NAKIT	Rozšíření kapitoly 6, nová kapitola 11 popisující aktivní federaci (přihlašování mobilních aplikací).

Verze	Datum	Autor	Stav dokumentu / Popis změn
1.14	10.3.2022	NAKIT	Nová kapitola 12 Autorizace digitálního úkonu. Aktualizace odkazů na vývojářskou dokumentaci.
1.15	18. 11. 2022	NAKIT	Rozšíření kapitol 6.2. a 8.5 o informace vztahující se k novému claimu „Doklady“ (FullIds). Doplněna kapitola 8.5.3 Schéma a kódování FullIds.
1.16	1. 4. 2023	DIA	Formální změny souvisejí s transformací SZR do Digitální a informační agentury.
1.17	5.5.2023	NAKIT	Aktualizace odkazů v podkapitole 3.3. Technické specifikace eIDAS.
1.18	10.10.2023	NAKIT	Rozšíření informací o atributu LoA. Doplněna kapitola 6.2.1, 8.4 a 8.5.6. Drobná úprava v kapitole 8.5.
1.19	19.10.2023	NAKIT	Aktualizace obrazovek a textací na základě redesignu Portálu Identity občana (Portálu Národního bodu).
1.20	26.10.2023	NAKIT	Rozšíření kapitoly 7 o kapitoly 7.2 a 7.3 pro připojení soukromoprávních subjektů k NIA
1.21	5.1.2024	NAKIT	Rozšíření informace o přihlašování přes informační systém datových schránek v kapitole 7.1
1.22	2.4.2024	NAKIT	Doplnění kapitoly 8 o možné delší přihlašování z důvodu frontování.

2. Seznam zkratek a pojmů

Agenda	Souhrn úředních činností, většinou vázaný na konkrétní správní činnost, např. Agenda registru občanských průkazů, Agenda procesu územních řízení.
ACS	Access Control Service – Služba zpracovávající autentizační tokeny na straně poskytovatele služby. Služba je také zodpovědná za session management na straně poskytovatele služby.
AIS	Agendový informační systém. Informační systém veřejné správy, který slouží k výkonu Agendy.
BSI	Bezvýznamový směrový identifikátor.
DIA	Digitální a informační agentura
eGSB	eGON Service BUS – Poskytuje údaje o fyzické osobě, které jsou publikovány jednotlivými agendami veřejné správy prostřednictvím napojených Agendových informačních systémů.
eIDAS	Zkratka pro nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.
identitaobcana.cz	Portál zpřístupňující funkcionalitu pro občany a funkcionalitu pro poskytovatele služeb (portál národního bodu).
ETSI	The European Telecommunications Standards Institute je nezávislá, nezisková organizace pro standardizaci v telekomunikačním průmyslu v Evropě. Vytváří globálně aplikovatelné standardy pro ICT včetně internetových technologií.
FCM	Firebase Cloud Messaging slouží k odesílání push notifikací na mobilní zařízení.
Hash	Výstup hashovací funkce, což je algoritmus převádějící vstupní hodnotu na jeho otisk v podobě čísla.
IdP	Identity Provider. Kvalifikovaný správce dle zákona č. 250/2017 Sb. o elektronické identifikaci. Kvalifikovaný správce poskytuje důvěryhodnou službu identifikace a autentizace fyzické osoby pomocí vydaných prostředků identifikace a autentizace. Tyto prostředky a procesy identifikace a autentizace jsou poskytovány na úrovních důvěry v souladu s nařízením eIDAS a návazné národní legislativy.
ISDS	Informační systém datových schránek.
ISZR	Informační systém základních registrů.
LoA	Level of Assurance, úroveň ověření dle eIDAS.

Metadata	Data, která poskytují informaci o jiných datech.
NIA	Národní bod dle zákona č. 250/2017 Sb. o elektronické identifikaci. Informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému. Vykonává agendu dle nařízení EU 910/2014 a návazné legislativy ČR. Vytváří národní část uzlu eIDAS, udržuje vazbu mezi základní elektronickou identitou fyzické osoby (záznam v Registru obyvatel) a instancemi elektronické identity této osoby u kvalifikovaného systému elektronické identifikace. Součástí národního bodu je mezinárodní uzel eIDAS zprostředkující komunikaci mezi národními identitními systémy členských zemí EU.
ORG	Převodník identifikátorů ORG fyzických osob. ISVS jehož hlavním účelem je převod Agendových identifikátorů fyzických osob ze Zdrojových identifikátorů fyzických osob.
OTP	One-time password. Jednorázové heslo.
OVM	Orgán veřejné moci.
Referenční údaj	Údaj vedený v Základním registru, který ZZR jako Referenční údaj označuje, údaj v některém ze základních registrů považovaný za správný a právně závazný, pokud není prokázán opak nebo pokud nevznikne pochybnost o jeho správnosti.
REST	Representational State Transfer. Architektura rozhraní navržená pro distribuované prostředí.
ROB	Registr obyvatel, základní registr obyvatel.
ROS	Registr osob, základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci.
RPP	Registr práv a povinností, základní registr agend orgánů veřejné moci a některých práv a povinností.
RÚIAN	Základní Registr územní identifikace, adres a nemovitostí.
SAML	Security Assertion Markup Language – standard založený na XML určený pro výměnu autentizačních a autorizačních dat mezi poskytovatelem služeb a poskytovatelem identity.
SeP	Service Provider. Kvalifikovaný poskytovatel dle zákona č. 250/2017 Sb. o elektronické identifikaci. Kvalifikovaný poskytovatel online služeb, při nichž je vyžadováno prokázání totožnosti s využitím elektronické identifikace.
SePP	Service Provider Pseudonym. Bezvýznamový směrový identifikátor pro komunikaci mezi národním bodem a kvalifikovaným poskytovatelem.

SSO	Single Sign-On – umožňuje uživatelům jediné přihlášení, které jim zpřístupní informační zdroje z více různých systémů bez opětovného požadavku na přihlašování.
SZR	Správa základních registrů.
URI	Uniform Resource Identifier (jednotný identifikátor zdroje) je textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací.
URL	Uniform Resource Locator (jednotná adresa zdroje) je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací.
ZR	Základní registr.
ZZR	V tomto dokumentu je pod pojmem ZZR míněn zákon č.111/2009 Sb., o základních registrech.

3. Úvod dokumentu

Účelem tohoto dokumentu je předat kvalifikovaným poskytovatelům služeb (SeP – Service Provider) základní předpoklady a návod pro registraci a konfiguraci kvalifikovaného poskytovatele a jeho fungování v rámci procesu ověření uživatele.

Národní identitní autorita (NIA) zprostředkovává služby důvěryhodných poskytovatelů identit (Identity Provider – IdP) jednotlivým důvěryhodným poskytovatelům služeb (Service Provider – SeP) vyžadujícím důvěryhodnost autentizací přistupujících subjektů (uživatelů). NIA dále zprostředkovává poskytnutí důvěryhodných údajů o těchto subjektech (tj. jejich atributů prostřednictvím tzv. assertions/claims) z připojených zdrojů těchto údajů a pro zajištění důsledného oddělení jednotlivých kmenů zajišťuje vydávání unikátních identifikátorů pro každého registrovaného SeP. Součástí NIA je podpora administrativních procesů nutných k registraci IdP a SeP a navázání jejich důvěry. Dále NIA zahrnuje persistentní úložiště a uživatelské rozhraní pro správu subjektem definovaných údajů. Rozhraní pro veřejnost (subjekty údajů) a pro správce připojených systémů (SeP, IdP) je poskytováno prostřednictvím webového portálu na identitaobcana.cz.

3.1. Vymezení základních pojmů

NIA – informační systém veřejné správy vykonávající agendu dle zákona 250/2017 Sb. o elektronické identifikaci a další návazné legislativy ČR. Udržuje vazbu mezi základní elektronickou identitou fyzické osoby (záznam v Registru obyvatel) a instancemi elektronické identity této osoby u poskytovatelů důvěryhodných služeb.

Service Provider (SeP) – kvalifikovaný poskytovatel dle zákona č. 250/2017 Sb. o elektronické identifikaci.

Identity Provider (IdP) – kvalifikovaný správce dle zákona č. 250/2017 Sb. o elektronické identifikaci. Subjekt poskytující důvěryhodnou službu identifikace a autentizace fyzické osoby pomocí jím vydaných prostředků identifikace

LoA – úroveň záruky (Level of Assurance, LoA) vyjadřuje míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti dané osoby. Míra spolehlivosti, kterou úroveň záruky představuje, je definována na základě použitých postupů, řídících činností a prováděných technických kontrol.

Pseudonym – bezvýznamový směrový identifikátor. Pseudonym, který slouží k jednoznačné identifikaci dané osoby u konkrétního poskytovatele služeb, je označován jako SePP (Service Provider Pseudonym), dle zákona č. 250/2017 Sb. se jedná o identifikátor držitele v rámci online služby. Pseudonym vydaný pro

konkrétního Identity Providera je označován jako IdPP (Identity Provider Pseudonym), dle zákona č. 250/2017 Sb. se jedná o identifikátor držitele v rámci kvalifikovaného systému.

ISZR – Informační systém základních registrů zajišťuje sdílení dat mezi jednotlivými základními registry navzájem, a mezi Základními registry a Agendovými informačními systémy. Mezi další úkoly ISZR patří správa oprávnění přístupu k datům, přístup AIS k základním registrům, zajištění integrity a dostupnosti referenčních dat a poskytování služeb pro jejich pořizování, aktualizaci a zajištění požadovaných rozhraní.

Základní registry – Poskytují primární elektronickou identitu fyzické osoby (záznam v ROB) a dále poskytují referenční údaje o této fyzické osobě

identitaobcana.cz – portál jako rozcestník ke službám pro občany a službám pro poskytovatele služeb (Service Provider, SeP).

3.2. Legislativní rámec

Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů

Tento zákon vymezuje obsah základních registrů, informačního systému základních registrů a stanoví práva a povinnosti, které souvisí s jejich vytvářením, užíváním a provozem. Prostřednictvím tohoto zákona byla rovněž zřízena Správa základních registrů (SZR) včetně vymezení základních kompetencí. Působnost SZR převzala od 1. dubna 2023 Digitální a informační agentura na základě zákona č. 471/2022 Sb.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů

Zákon o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. V návaznosti na to upravuje působnost Digitální a informační agentury jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy.

Vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do IS

Obsahuje základní informace o dostupnosti a obsahu zpřístupněných IS VS. Tato vyhláška je klíčovým dokumentem, který upravuje formu a technické náležitosti

předávání údajů do veřejného informačního systému. Pokud OVM předpokládá využití vlastních IS (kterých je správcem) pro komunikaci se základními registry, je podmínkou pro získání příslušného certifikátu registrace v IS o ISVS.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

Tento zákon upravuje zřízení datových schránek, včetně zřízení datových schránek OVM, definuje a vymezuje ISDS, včetně vazby ISDS na evidenci obyvatel (§ 15 zákona).

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

Správní řád upravuje postup orgánů, které vykonávají působnost v oblasti veřejné správy. Zákon o základních registrech tyto definované postupy rozšiřuje o povinnost OVM využívat při své činnosti referenční údaje obsažené v příslušném základním registru, viz § 5 odst. 1 zákona č. 111/2009 Sb.

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Základním účelem tohoto zákona je definice povinností při zpracování osobních údajů a stanovení podmínek nakládání s nimi. Z pohledu implementace dopadů zákona o základních registrech je z obsahu zákona o ochraně osobních údajů podstatný zejména § 5, odst. 1, který definuje povinnosti správce osobních údajů a § 13 stanovující požadavky na zabezpečení osobních údajů. OVM jsou tedy povinni zabránit sdružování osobních údajů, které může nastat při nevhodném způsobu zajištění výkonu agend lokálními IS/AIS a přijmout taková opatření, aby nemohlo dojít k neoprávněnému či nahodilému přístupu k osobním údajům (tato opatření musí být řádně zdokumentována).

Zákon č. 250/2017 Sb., o elektronické identifikaci

Tento zákon upravuje působnost Digitální a informační agentury na úseku elektronické identifikace.

Nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Toto nařízení platné a účinné pro všechny členské státy EU reaguje na rychlý technologický rozvoj prostředků pro zpracování osobních údajů a probíhající proces globalizace a dává pevnější a soudržnější rámec pro ochranu osobních údajů v rámci Unie. Vytváří základ pro důsledné vymáhání práva, jenž je nezbytný pro nastolení

důvěry tak, aby se mohla rozvíjet digitální ekonomika na celém vnitřním trhu EU. Fyzickým osobám dává právo a možnost kontrolovat své vlastní osobní údaje. Tam, kde je Nařízení v rozporu se zákonem č. 101/2000 Sb., platí Nařízení.

Nařízení EU 910/2014 o elektronické identifikaci a službách vytvářejících důvěru (eIDAS) včetně návazných prováděcích aktů

Zákon o občanských průkazech č. 269/2021 Sb., ve znění pozdějších předpisů

Na základě tohoto zákona Digitální a informační agentura zajišťuje elektronickou identifikaci a autentizaci držitele občanského průkazu pomocí státních dat pro elektronické využití občanského průkazu, která jsou potřebná pro elektronickou identifikaci a autentizaci. Zároveň provádí zablokování státních dat pro elektronické využití občanského průkazu, která jsou potřebná pro elektronickou identifikaci a autentizaci.

3.3. Technické specifikace eIDAS

Technické specifikace pro eIDAS interoperability framework byly vytvořeny na základě spolupráce členských států v technickém podvýboru expertní skupiny eIDAS. Tyto specifikace mohou členské státy využít při své vlastní implementaci eIDAS. Technické specifikace eIDAS se skládají z níže uvedených čtyř samostatných dokumentů. Každý z dokumentů, na které je odkazováno, popisuje specifickou oblast dané problematiky.

eIDAS SAML Message Format ve verzi 1.2 z 27. 9. 2019
eIDAS SAML Attribute Profile ve verzi 1.2 z 27. 9. 2019
eIDAS – Interoperability Architecture ve verzi 1.2 z 27. 9. 2019
eIDAS – Cryptographic requirements for the Interoperability ve verzi 1.2 z 27. 9. 2019

3.4. Bezpečnostní doporučení

ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

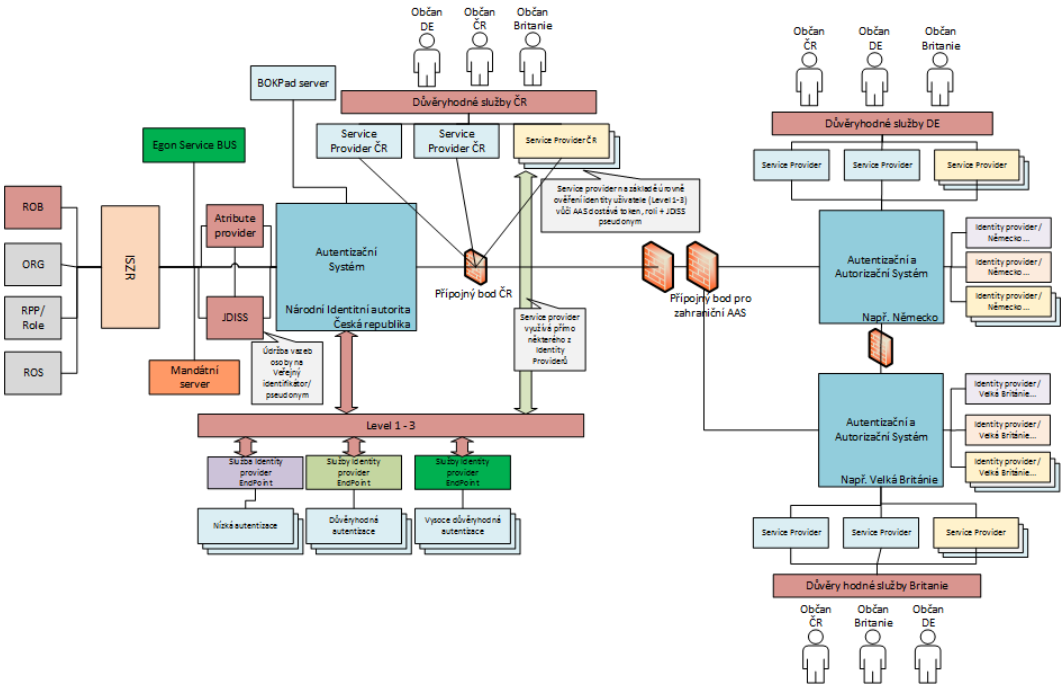
Tento evropský standard ETSI ustanovuje soubor postupů, procesů a bezpečnostních opatření, jejichž cílem je minimalizace možných provozních a finančních hrozeb a s nimi spjatých rizik na straně důvěryhodných poskytovatelů služeb. Tato obecná politika klade základní požadavky na postupy při provozu a managementu důvěryhodného poskytovatele služeb bez zřetele k tomu, jaké služby poskytuje. Dokument odkazuje na další předpisy ETSI zaměřené na důvěryhodné poskytovatele služeb určitých zaměření.

Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0

Tento OASIS (Organization for the Advancement of Structured Information Standards) standard obsahuje doporučené bezpečnostní techniky pro práci se SAML.

Aktuální dokument ve verzi 2.0 je dostupný zde:
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

4. Národní identitní autorita a Service Provider



Obrázek 1 - Schéma NIA a SeP

4.1. Přínosy NIA pro SeP

Jaké výhody přináší NIA pro SeP:

- volba nejvyšší úrovně LoA s využitím NIA a eOP,
- vazba na základní registry, tedy referenční údaje o uživateli,
- další údaje poskytnuté uživatelem,
- správa souhlasů poskytnutí údajů uživatelem,

- sada údajů o uživateli pro ověření a předvyplnění ve formulářích.

V zaslaném requestu může SeP definovat požadované LoA (Level of Assurance). Pokud neuvede konkrétní úroveň LoA, jsou mu nabídnuti IdP pro všechna LoA. Jeden SeP může požadovat více úrovní LoA prostřednictvím minimálního požadovaného LoA obsaženého v requestu nebo požadovat konkrétního IdP.

LoA definovaná dle eIDAS má následující tři úrovně:

- Low,
- Substantial,
- High.

4.2. Portál národního bodu

Úvodní stránka portálu národního bodu, který je umístěn na webových stránkách identitaobcana.cz, představuje pro uživatele rozcestník mezi službami pro občany a službami pro kvalifikované poskytovatele služeb (Service Provider, SeP). Uživatel přistupující v roli občana může po úspěšném ověření spravovat svůj profil v národním bodu. Pod tuto správu patří správa vlastních údajů, správa souhlasů s poskytováním údajů kvalifikovaným poskytovatelům služeb a dále zobrazení seznamu svých aktivních identifikačních prostředků, které jsou připojeny k národnímu bodu nebo zobrazení historie své činnosti vůči národnímu bodu. Uživatel může v prostředí portálu národního bodu také spravovat svůj uživatelský profil (identifikační prostředek NIA ID, dříve také znám jako Jméno, heslo a SMS). Správa uživatelského profilu obsahuje změnu hesla, změnu bezpečnostní otázky a odpovědi pro obnovu hesla, správu telefonního čísla a e-mailové adresy pro NIA ID a dále možnost si tento identifikační prostředek plně aktivovat pro použití k přihlašování i mimo portál národního bodu nebo naopak provést jeho zrušení.

Uživatel přistupující jako zástupce organizace může po úspěšném ověření provést registraci organizace nebo v rámci již registrované organizace konfigurovat či rušit jednotlivé poskytovatele služeb, případně zařazovat jednotlivé konfigurace do společných skupin pro výdej BSI (SePP). NIA tak umožní nastavit vztah důvěry se Service Providerem. Uživatel zastupující organizaci může nastavit vybraného poskytovatele za účelem využívání služeb individuálního výdeje a získat tak možnost požádat o doplnění údajů o občanovi, který je autentizován skrze národní bod. Dalším rozšířením je možnost nastavit vybraného kvalifikovaného poskytovatele do role poskytovatele údajů a nabízet tak jeden či více údajů o občanovi skrze národní bod.

5. Pozice Service Providera v rámci ověření uživatele

Následující kroky popisují jednotlivé části procesu, který je naznačen níže.

1. Uživatel požaduje po Service Providerovi (poskytovateli služeb) určitou službu, kterou Service Provider nabízí.

2. Aby mohl Service Provider danou službu uživateli nabídnout, požaduje uživatelovu identifikaci. Service Provider připraví SAML žádost o přihlášení, ve kterém definuje požadované údaje a zejména LoA, tedy minimální úroveň záruky, kterou se musí uživatel prokázat národnímu bodu. Následně přesměruje uživatele na vstupní bod národního bodu.

3. Národní bod nabídne ověřovanému uživateli seznam těch Identity Providerů (poskytovatelů identit), kteří jsou ve vztahu důvěry s Národním bodem a splňují minimálně LoA definované poskytovatelem služby.

4. Uživatel zvolí Identity Providera z nabízeného seznamu a provede ověření vlastní osoby vůči tomuto poskytovateli. Pokud zvolenému LoA vyhovuje pouze jeden poskytovatel identity, je uživatel přesměrován na příslušného poskytovatele bez potřeby výběru. Ověření je realizováno na základě splnění pravidel, která si definuje zvolený Identity Provider.

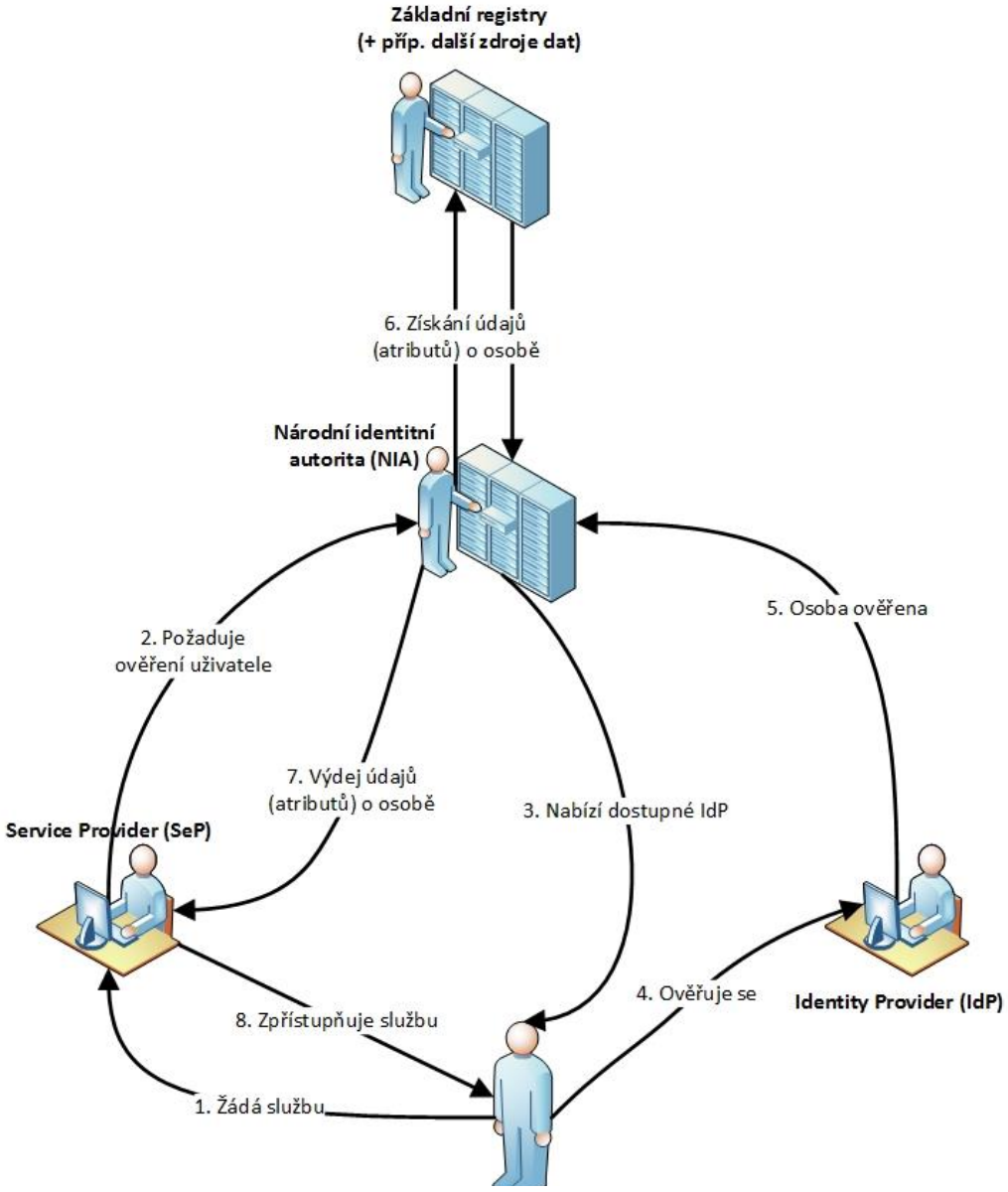
5. V případě, kdy je uživatel úspěšně ověřen, Identity Provider předá Národnímu bodu jako výsledek ověření autentizační token obsahující tzv. IdP pseudonym a případně další informace, které o daném uživateli udržuje. Předávaný pseudonym jednoznačně identifikuje danou osobu ve vztahu Identity Provider – Národní bod.

6. Národní bod provede sběr atributů z Informačního systému základních registrů (ISZR) a dalších napojených datových zdrojů. Atributy, které jsou o uživateli vyzvednuty z příslušných datových zdrojů, jsou definovány v úvodní žádosti o identifikaci uživatele. Bez ohledu na požadované atributy je vždy z ISZR vyzvednut údaj kontrolující úmrtí osoby. Je-li osoba v ROB označena jako zemřelá, je celá transakce identifikace ukončena jako neplatná.

7. Národní bod předává Service Providerovi tzv. SeP pseudonym a atributy nasbírané z Informačního systému základních registrů a dalších napojených datových zdrojů. Předávaný pseudonym jednoznačně identifikuje danou osobu ve vztahu Národní bod – Service Provider a je předáván atributem „PersonalIdentifier“.

8. Na základě úspěšného splnění předchozích kroků je subjekt autentizován a identifikován a Service Provider může umožnit využití identifikovanému uživateli jím vybranou službu.

Pokud se uživatel snaží využít službu jiného poskytovatele služeb, a již je k jednomu poskytovateli služeb přihlášen, národní bod nejdříve ověří požadované LoA novým poskytovatelem služeb a pokud LoA vyhovuje z předchozího přihlášení, je využito principu SSO.



Obrázek 2 - Zajištění ověření uživatele pro SeP

6. Registrace a konfigurace Service Providera

Následující kroky popisují jednotlivé části procesu, který je naznačen níže, viz Obrázek 3 - Registrace a konfigurace SeP na základě ověření přes ISDS.

Aktuálně je registrace organizace prostřednictvím portálu národního bodu přístupná pouze pro orgány veřejné moci (OVM), ostatní subjekty musí provést registraci přímo u Digitální a informační agentury – Sekce správy základních registrů (viz krok 8).

6.1. Popis procesu registrace a konfigurace

1. Uživatel jako zástupce organizace požaduje po portálu národního bodu, který je Service Providerem, službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů.

2. Portál národního bodu kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).

3. Pro ověření uživatele pro registraci organizace či konfigurací jednotlivých Service Providerů je jako Identity Provider určen Informační systém datových schránek (ISDS). Národní identitní autorita provede přesměrování na přihlášení prostřednictvím datových schránek.

4. Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci na portálu národního bodu, musí být přihlášen prostřednictvím ISDS (v definované roli a typem schránky OVM). V případě, že organizace není OVM, je potřeba provést registraci u Digitální a informační agentury – Sekce správy základních registrů.

5. V případě, kdy je uživatel úspěšně ověřen, Informační systém datových schránek předá Národní identitní autoritě jako výsledek ověření autentizační token obsahující IČO a název subjektu, roli přihlašovaného uživatele a další atributy.

6. Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR) na jehož základě následně provede kontrolu existence IČO.

7. Národní identitní autorita předává portálu národního bodu potřebné atributy z Informačního systému základních registrů a atributy přijaté v autentizačním tokenu z Informačního systému datových schránek, které jsou nutné ke zpracování formuláře pro registraci.

8. Na základě úspěšného splnění předchozích kroků umožní portál národního bodu uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci. Toto platí pouze pro organizace, které jsou OVM. Není-li organizace OVM, jsou místo registračního formuláře zobrazeny podrobné informace o tom, jakým způsobem provést registraci přímo u Digitální a informační agentury.

9. Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).

10. Portál národního bodu zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci (seznam konfigurací kvalifikovaných poskytovatelů).

11. Uživatel provede konfiguraci Service Providera zahrnující následující údaje:

    - **IČO subjektu** – IČO (identifikační číslo osoby) poskytovatele služeb, jehož konfigurace je prováděna.

    - **ID DS** – Identifikátor datové schránky subjektu (organizace), pod kterou konfigurace kvalifikovaného poskytovatele spadá.

    - **Název kvalifikovaného poskytovatele (SeP)** – Název pro vytvářenou konfiguraci poskytovatele služeb. Jedná se o název, kterým bude daná konfigurace reprezentována.

    - **Popis kvalifikovaného poskytovatele (a jeho služby)**, který obsahuje krátké představení vytvářeného kvalifikovaného poskytovatele služeb. Představuje základní informace o činnostech a nabízených službách příslušného poskytovatele služeb.

    - **Právní předpis** a konkrétní ustanovení, na základě kterého vzniká povinnost ověřovat osoby prostřednictvím Národního bodu.

    - **URL adresa odkazující na úvodní webové stránky** kvalifikovaného poskytovatele, na kterých jsou k dispozici zpravidla základní informace a popis činností a služeb, které daný poskytovatel provozuje.

    - **URL adresa pro odeslání požadavků** – Unikátní URL adresa zabezpečené části Vašeho webu, do které bude klient přistupovat s pomocí identifikace a autentizace prostřednictvím národního bodu.

    - **Adresa pro příjem vydaného tokenu (URL)** – URL adresa ACS, kam bude předán token vydaný národním bodem jako odpověď na žádost o autentizaci uživatele, a kam bude uživatel, v případě požadavku

poskytovatele služby, přesměrován. V případě, že v požadavku bude uvedena jiná než zaregistrovaná URL adresa, nebude odpověď vydána.

- **URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu** – URL adresa ACS, kam bude předán token vydaný národním bodem jako odpověď na žádost o LogOut uživatele, a kam bude uživatel, v případě požadavku poskytovatelem služby, přesměrován.

- **Načtení certifikátu** – zobrazí okno pro zadání cesty, odkud má dojít k načtení certifikátu. Cesta k certifikátu může být pouze na portu 80 nebo 443. Tento certifikát je uložen u konfigurace (po stisknutí tlačítka Uložit). V případě, že jsou vyplněny obě možnosti pro získání certifikátu, je upřednostněn certifikát z URL adresy pro metadata. Certifikát je použit pro šifrování předávaných údajů (pro předání údajů je použit SAML token). Použití certifikátu je povinné v produkčním prostředí národního bodu.

- **Adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu** – URL adresa, na které jsou dostupná metadata příslušného certifikátu. V případě, že jsou vyplněny obě možnosti pro získání certifikátu, je upřednostněn certifikát z URL adresy pro metadata. Certifikát je použit pro šifrování předávaných údajů (pro předání údajů je použit SAML token). Použití certifikátu je povinné v produkčním prostředí národního bodu.

- **Zpřístupnění autentizace prostřednictvím brány eIDAS (pro pasivní federaci)** – kvalifikovaný poskytovatel akceptuje přihlášení i prostřednictvím mezinárodního brány eIDAS zajišťující přesměrování na poskytovatele ověření z ostatních členských států EU. Toto nastavení se týká klasického přihlašování k webovým portálům (tzv. pasivní federace), nikoliv k mobilním aplikacím.

- **Logo kvalifikovaného poskytovatele**, které je zapotřebí vložit v podporovaném typu souboru (PNG či JPEG) a zároveň v požadovaném formátu (s minimální velikostí 65 x 65 pixelů). Načtení loga probíhá z lokálního disku skrze tlačítko „Vložit“. Po načtení vybraného loga z adresáře, které odpovídá požadovanému formátu a typu souboru, se ve formuláři pro konfiguraci kvalifikovaného poskytovatele zobrazí náhled na vložené logo.

- **Kontaktní údaje** (telefonní číslo a e-mailovou adresu) na zástupce organizace a telefonní číslo na zákaznickou podporu, pokud je zřízena.

Tyto kontaktní údaje slouží především pro operativní řešení provozních a bezpečnostních problémů

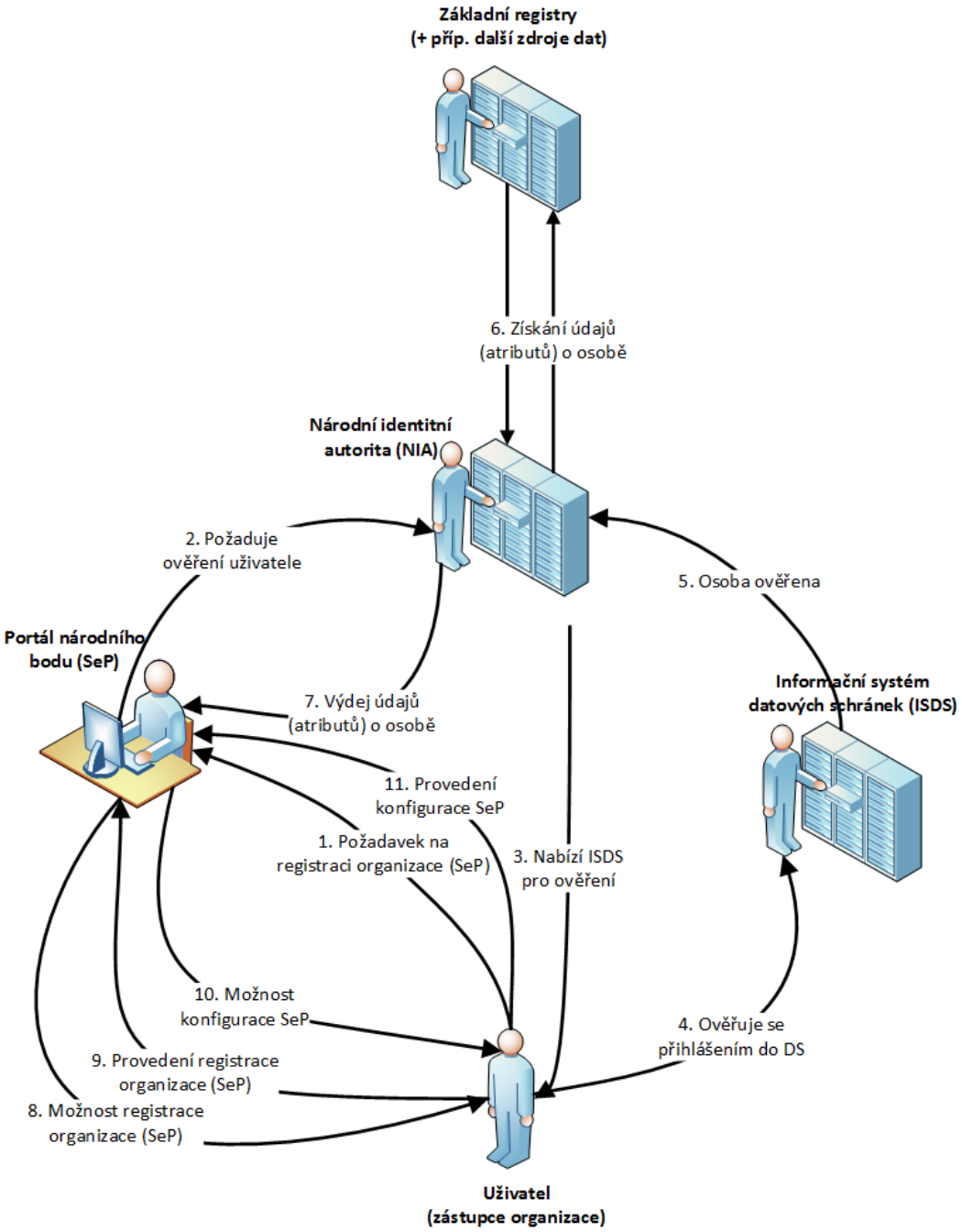
V případě, že má být konfigurace kvalifikovaného poskytovatele využívána i pro přihlašování mobilních aplikací (detailní popis v samostatné kapitole), jsou povinné následující položky konfiguračního formuláře:

- **Checkbox Využít kvalifikovaného poskytovatele pro přihlašování přes mobilní aplikace.** Zaškrtnutím checkboxu zaktivníte další níže uvedené povinné položky, které jsou nutné pro přihlašování mobilní aplikace přes národní bod prostřednictvím tzv. aktivní federace.

- **Uživatelské jméno** je automaticky vygenerované národním bodem a společně s heslem slouží pro volání služby národního bodu kvalifikovaným poskytovatelem.

- **Heslo** musí obsahovat minimálně 17 znaků, a to v kombinaci malých a velkých písmen, číslic a speciálních znaků. Heslo je kontrolováno již v průběhu vyplňování, a tak je ihned viditelné, zda je validní či nikoliv.

Požadované údaje určují, pro jaké údaje bude po občanovi požadován trvalý souhlas s jejich výdejem. Pokud mobilní aplikace využívá přihlašování přes národní bod, je nutné při prvním přihlášení udělit občanem trvalý souhlas a další přihlašování dané mobilní aplikace k národnímu bodu včetně výdeje údajů již probíhá na pozadí bez nutnosti zadávání přihlašovacích údajů občanem.



Obrázek 3 - Registrace a konfigurace SeP na základě ověření přes ISDS

6.2. Atributy vydávané Service Providerům

Níže uvedené atributy, pokud jejich vydání pro určitý SeP schválí fyzická osoba, mohou být vydány jednotlivým SeP, pokud o jejich vydání požádá. Předpokladem je, že je SeP zaregistrovaný na portálu národního bodu a má uloženou konfiguraci SeP, ze které k portálu národního bodu přistupuje. Tučně označené atributy odpovídají standardu eIDAS, ostatní atributy sice standardu neodpovídají, SeP má ale možnost při komunikaci v rámci ČR o jejich vydání zažádat.

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.
E-mail	Email	E-mailová adresa uvedená 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 RUIAN. Obsahuje (pokud je uvedeno v ROB) kódy pro okres, obec, část obce, ulici, PSČ, stavební objekt, adresní místo, číslo domovní a orientační.
Pseudonym	PersonIdentifier	Identifikátor fyzické osoby.
Typ dokladu	IdType	Druh elektronicky čitelného dokladu.
Číslo dokladu	IdNumber	Číslo elektronicky čitelného dokladu.
Doklady	FullIds	Všechny platné doklady (jejich druh, číslo a platnost) vedené u fyzické osoby v registru obyvatel předávané v zakódované formě pomocí BASE64.

Tabulka 1 - Atributy vydávané Service Providerům

6.2.1. Atributy standardu WS-Federation

V rámci standardu WS-Federation může být vydáván i technický atribut LoA. Tento atribut nepodléhá schválení výdeje fyzickou osobou.

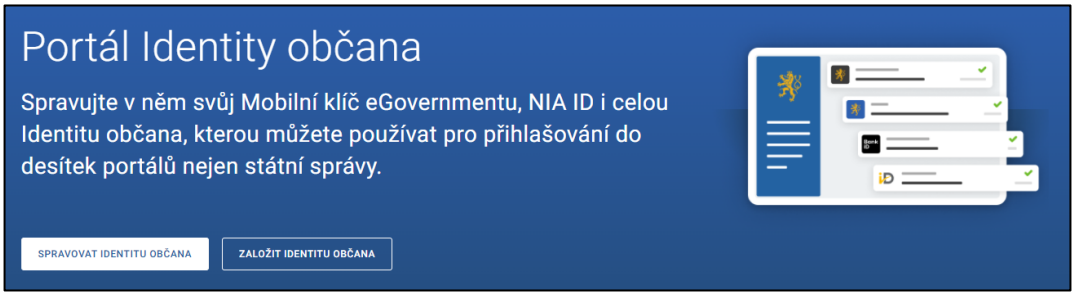
Level of Assurance (LoA)	LoA	Stupeň (úroveň) jistoty nebo zajištění. Viz eIDAS reference.

O tento atribut není možné žádat při použití standardu SAML 2/eIDAS.

7. Detailní popis registrace a konfigurace

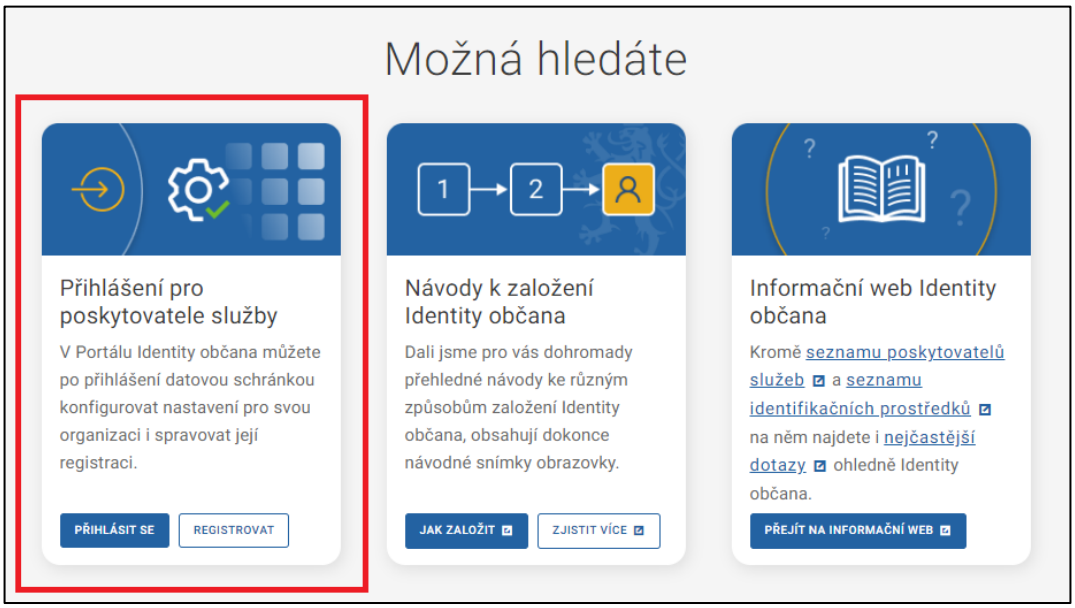
7.1. Registrace organizace

Registraci a konfiguraci poskytovatele služeb provedete na Portálu Identity občana, který se nachází na webových stránkách identitaobcana.cz. Prvním krokem je tedy zadání URL identitaobcana.cz do webového prohlížeče.



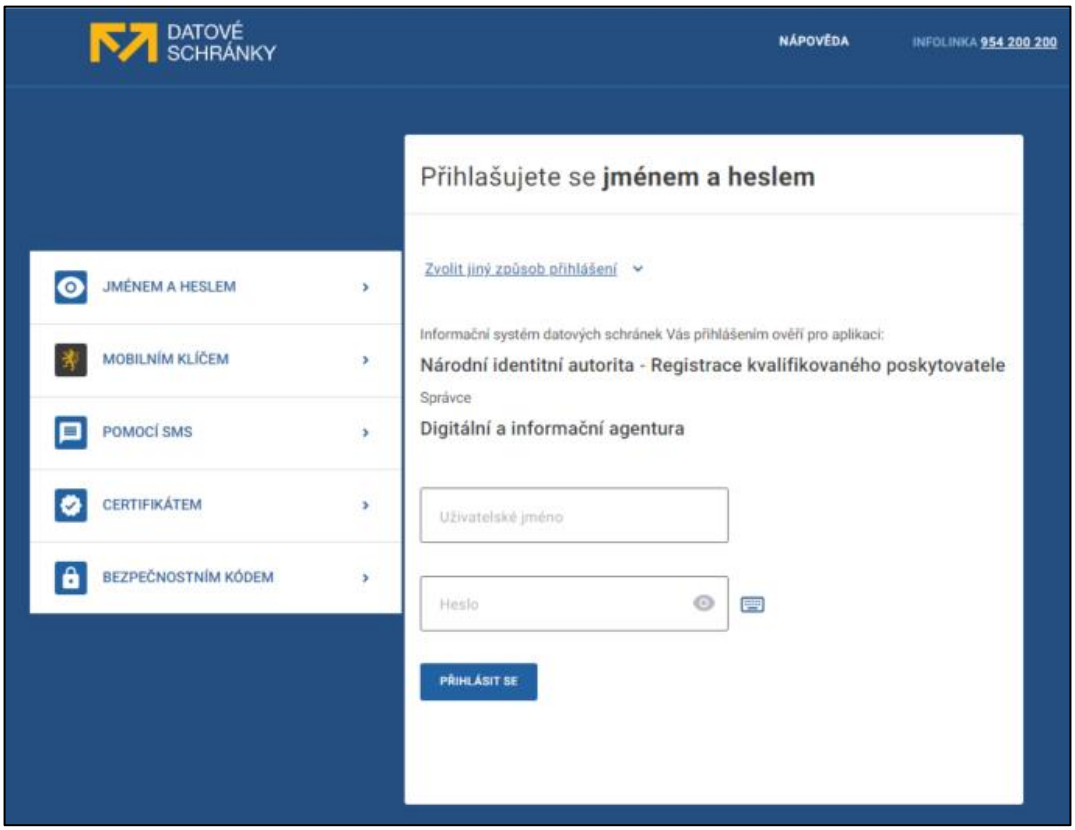
Obrázek 4 - Portál Identity občana

Následně je potřebné provést přihlášení v roli kvalifikovaného poskytovatele služeb. Přístup pro kvalifikované poskytovatele naleznete ve spodní části úvodní stránky.



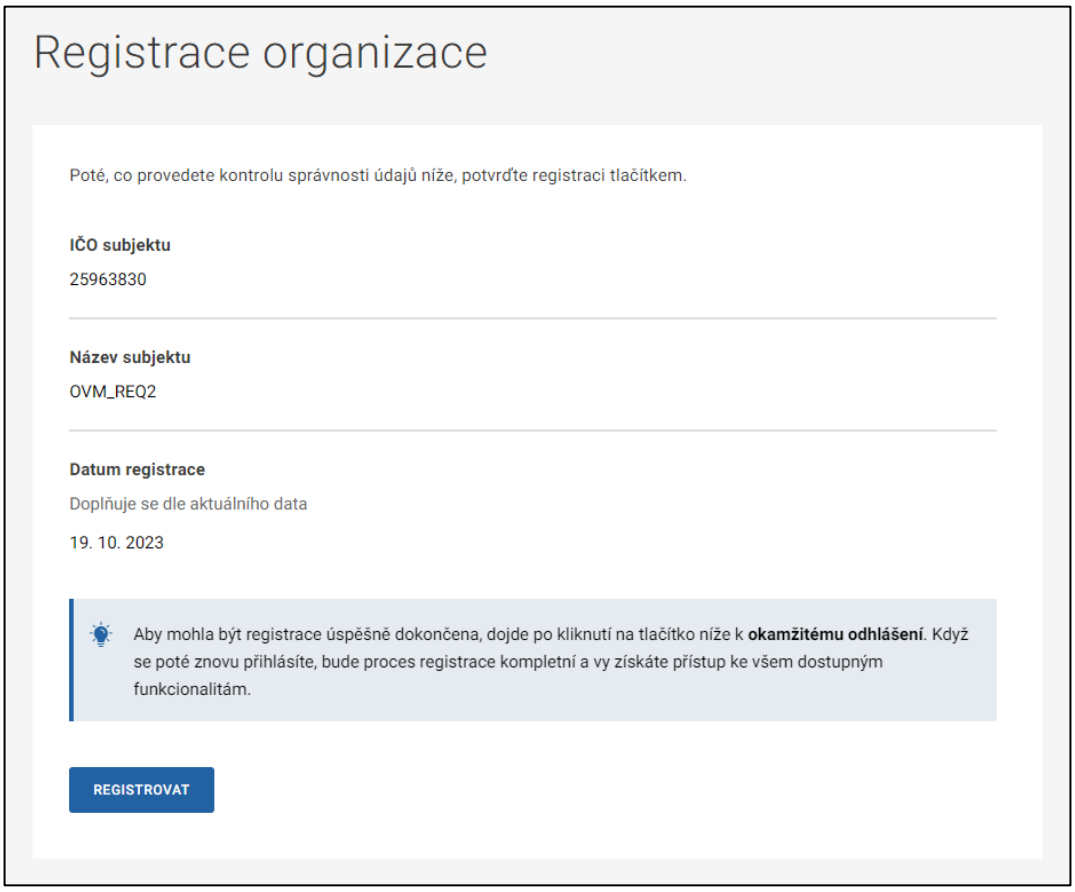
Obrázek 5 - Přihlášení poskytovatele na Portálu Identity občana

Pro potřeby registrace SeP je nutné provést přihlášení přes informační systém datových schránek. Z technických důvodů není možné provést přihlášení prostřednictvím Identity občana. Zvolte tak některou z dalších nabízených možností ověření, kterou vám informační systém datových schránek nabízí.



Obrázek 6 - Přihlášení přes informační systém datových schránek

Po úspěšném přihlášení a znovunačtení webových stránek Portálu Identity občana se Vám zobrazí základní funkcionality portálu. Aby bylo možné vytvářet jednotlivé poskytovatele služeb, je nutné nejprve provést registraci organizace, za kterou vystupujete. Na základě vašeho úspěšného přihlášení prostřednictvím informačního systému datových schránek získáme informace potřebné k registraci organizace, za níž registraci provádíte. Poté, co provedete kontrolu správnosti IČO subjektu a Názvu subjektu, potvrďte registraci tlačítkem „Registrovat“. Datum registrace se doplňuje automaticky dle aktuálního data.
Po úspěšné registraci je nutné vás odhlásit, abyste se následně mohli přihlásit již do nově vytvořeného profilu vaší organizace.



Obrázek 7 - Registrace organizace

Není-li organizace, za kterou se přihlašujete k Portálu Identity občana, orgánem veřejné moci, je vám místo možnosti registrovat organizaci pouze zobrazen postup, jak registraci provést přímo u Digitální a informační agentury.

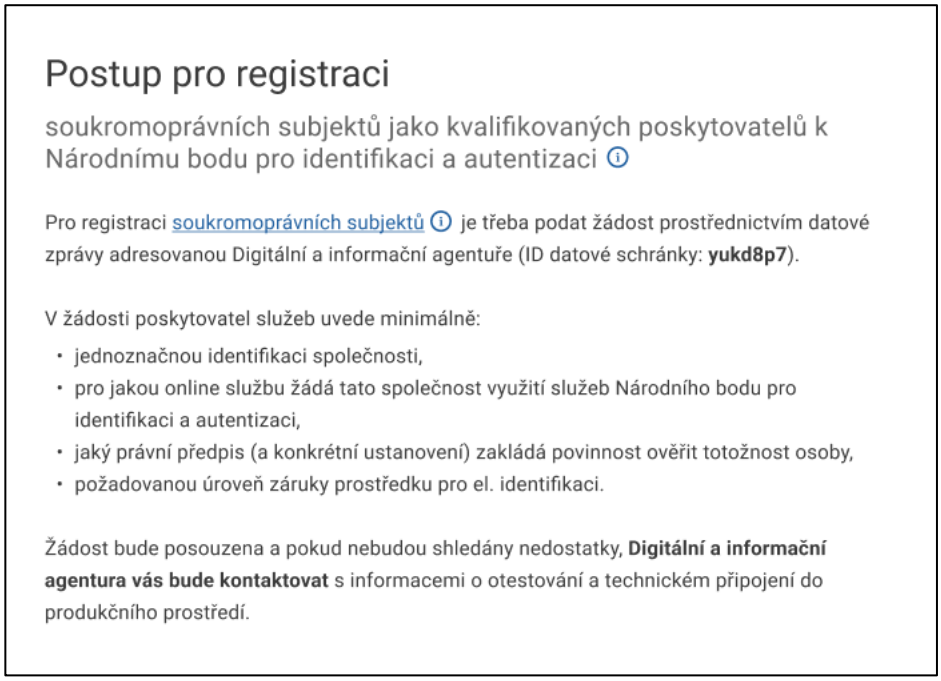
7.2. Připojení soukromoprávního subjektu k NIA

Do produkčního prostředí mohou být připojeni pouze ty soukromoprávní subjekty, kterým právní předpis ukládá ověřovat totožnost s využitím elektronické identifikace. V takovém případě pošle Digitální a informační agentuře do datové schránky žádost s předmětem „Žádost o připojení k produkčnímu prostředí NIA“. V žádosti poskytovatel služeb uvede minimálně:

- jednoznačnou identifikaci společnosti,
- pro jakou online službu žádá tato společnost využití služeb Národního bodu pro identifikaci a autentizaci,

- jaký právní předpis (a konkrétní ustanovení) zakládá povinnost ověřit totožnost osoby,

- požadovanou úroveň záruky prostředku pro el. identifikaci.



Obrázek 8 - Registrace soukromoprávních subjektů

Žádost bude posouzena a pokud nebudou shledány nedostatky, Digitální a informační agentura Vás bude kontaktovat s informacemi o otestování a technickém připojení do produkčního prostředí.

7.3. Připojení soukromoprávního subjektu k testovacímu prostředí NIA

Pokud jako soukromoprávní subjekt chcete využívat testovací prostředí pro služby zaručeného ověřování totožnosti uživatelů pomocí Národního bodu, je třeba, aby vaše společnost poslala oficiálně Digitální a informační agentuře žádost s předmětem „Žádost o připojení k testovacímu prostředí NIA“.

Pro registraci soukromoprávního subjektu, který bude chtít vyvíjet vlastní softwarové řešení s využitím služeb umožňující ověření totožnosti pomocí elektronické identifikace, je třeba podat žádost o připojení k testovacímu prostředí NIA prostřednictvím datové zprávy adresovanou do datové schránky Digitální a informační agentury (ID DS: yukd8p7).

V žádosti uvedete minimálně:

- identifikaci subjektu nebo okruhu subjektů, pro které bude služba vyvíjena,
- popis služby pro kterou budete využívat služeb NIA,
- e-mail a telefonní kontakt na odpovědnou osobu zajišťující testování.

Do produkčního prostředí mohou být připojeni pouze ty soukromoprávní subjekty, kterým právní předpis ukládá ověřovat totožnost s využitím elektronické identifikace.

7.4. Konfigurace poskytovatele služeb

Stisknutím tlačítka „Registrovat“ máte registraci organizace úspěšně za sebou a po opětovném přihlášení, kdy se vám rovnou načte sekce „Kvalifikovaní poskytovatelé“ se můžete pustit do vytvoření konfigurace (nebo i více konfigurací). Zobrazený Seznam konfigurací kvalifikovaných poskytovatelů se základními informacemi o jednotlivých konfiguracích je aktuálně prázdný. Pro vytvoření nové konfigurace klikněte na tlačítko „Přidat poskytovatele“.

Obrázek 9 - Seznam kvalifikovaných poskytovatelů – přidání poskytovatele

V rámci konfigurace poskytovatele služeb (Konfigurace kvalifikovaného poskytovatele) musíte zajistit vyplnění následujících polí (body 1 a 2 jsou vyplněny automaticky).

Základní údaje

1. IČO subjektu je vázáno na organizaci, ke které má uživatel v rámci informačního systému datových schránek přístup. IČO je vždy vyplněno automaticky na základě údajů získaných při přihlášení.

2. ID datové schránky subjektu představující identifikaci datové schránky vaší organizace je vždy vyplněno automaticky na základě údajů získaných při přihlášení.

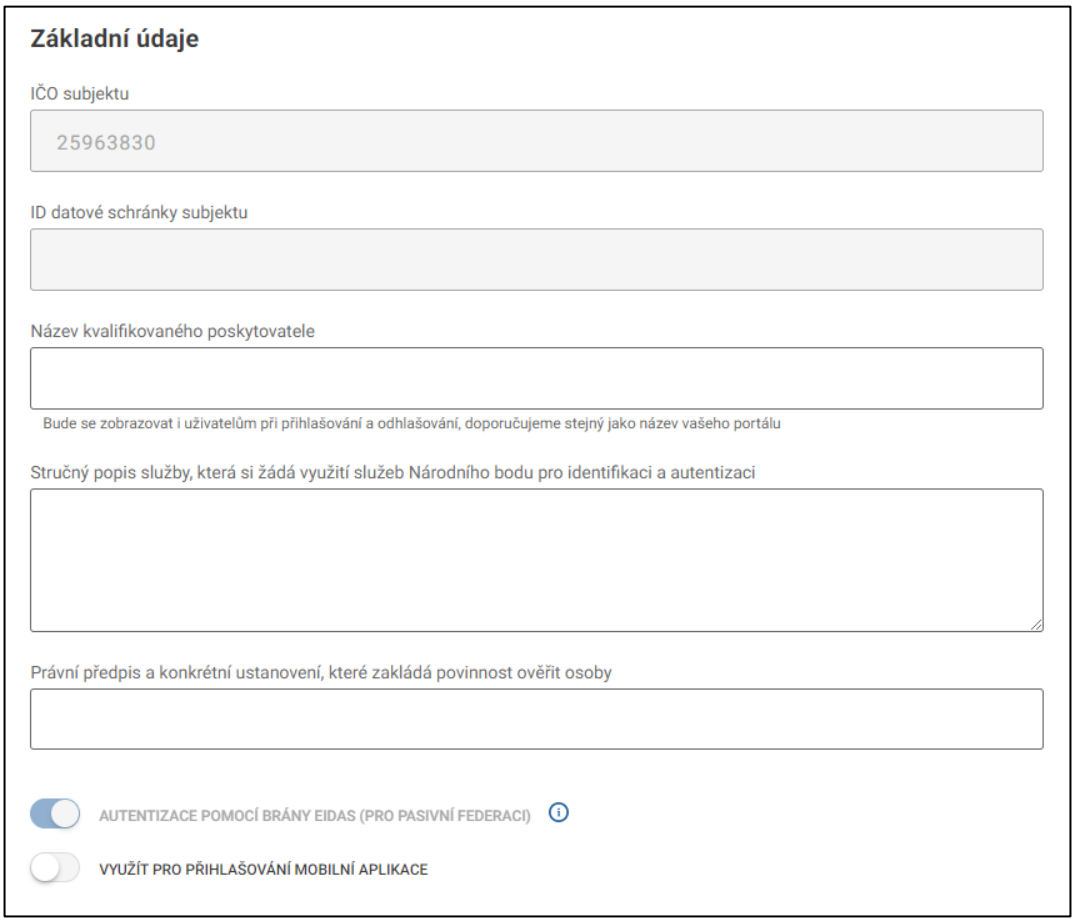
3. Název kvalifikovaného poskytovatele představuje název pro aktuálně vytvářenou konfiguraci poskytovatele služeb. Jedná se o název, kterým bude daná konfigurace reprezentována (např. v seznamu konfigurací) a bude vám sloužit pro odlišení této konfigurace od případných dalších vytvořených konfigurací. Tento název se bude zároveň občanům zobrazovat při přihlašování a odhlašování, proto doporučujeme použít např. stejný název, jako je název vašeho portálu.

4. Stručný popis služby a kvalifikovaného poskytovatele, který žádá využití služeb Národního bodu. Představuje základní informace o činnostech a nabízených službách příslušného poskytovatele služeb.

5. Informace na základě, jakého právního předpisu a konkrétního ustanovení je kvalifikovaný poskytovatel povinen ověřovat osoby prostřednictvím Národního bodu.

6. Autentizace prostřednictvím brány eIDAS (pro pasivní federaci) umožňuje přihlášení občana k Vašemu kvalifikovanému poskytovateli i skrze mezinárodní bránu eIDAS. Občan se tak může přihlásit u poskytovatele ověření, který je registrován mimo Českou republiku, a je prostřednictvím mezinárodní brány dostupný. Toto nastavení se týká klasického přihlašování k webovým portálům (tzv. pasivní federace), nikoliv k mobilním aplikacím.

7. Na závěr části „Základní údaje“ je možné zapnout využití konfigurace i pro přihlašování mobilních aplikací, které je popsáno níže v kapitole 11.1. Rozšíření konfigurace.



Obrázek 10 - Založení konfigurace – část Základní údaje

URL adresy

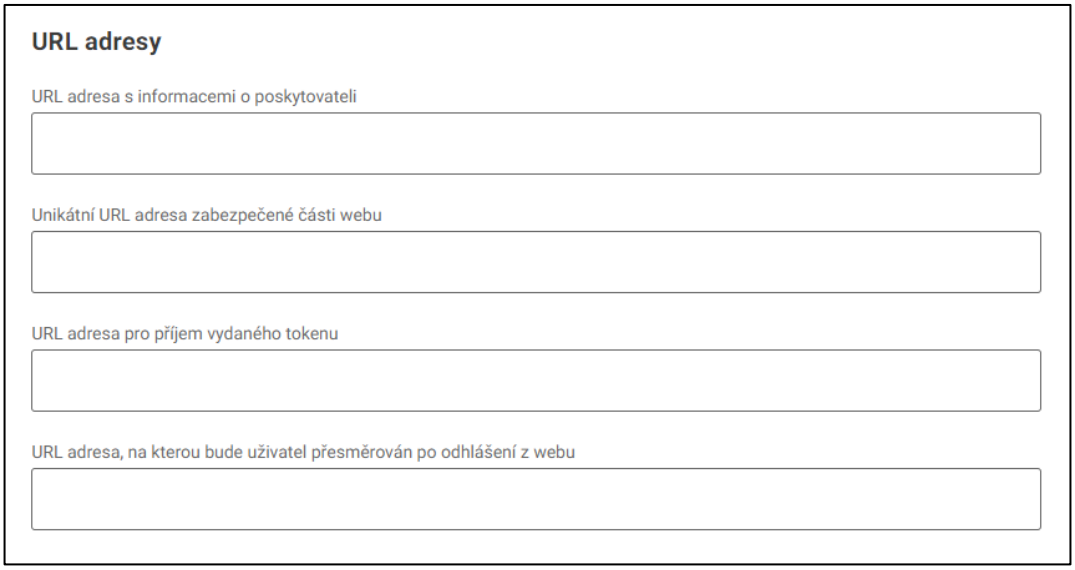
8. URL adresa odkazující na úvodní webové stránky kvalifikovaného poskytovatele, na kterých jsou k dispozici zpravidla základní informace a popis činností a služeb, které daný poskytovatel provozuje.

9. Unikátní URL adresa zabezpečené části vašeho webu, do které bude klient přistupovat s pomocí identifikace a autentizace prostřednictvím národního bodu pro identifikaci a autentizaci. Adresa musí být zabezpečena certifikátem a komunikovat výhradně protokolem HTTPS na standardním portu 443.

10. Adresa pro příjem vydaného tokenu představuje URL adresu endpointu služby ACS (Assertion Consumer Service), na kterou budou poskytovateli služeb zasílány odpovědi na žádosti o přihlášení subjektu. Adresa musí být zabezpečena protokolem HTTPS na standardním portu 443. V rámci

procesu přihlašování a vytváření SAML žádosti o tuto službu je tato adresa uvedena v této žádosti. V případě, že v žádosti bude uvedena jiná než zaregistrovaná URL adresa, nebude odpověď vydána.

11. URL adresa, na kterou bude uživatel následně přesměrován po odhlášení z Vašich webových stránek.



Obrázek 11 - Založení konfigurace – část URL adresy

Načtení veřejné části šifrovacího certifikátu

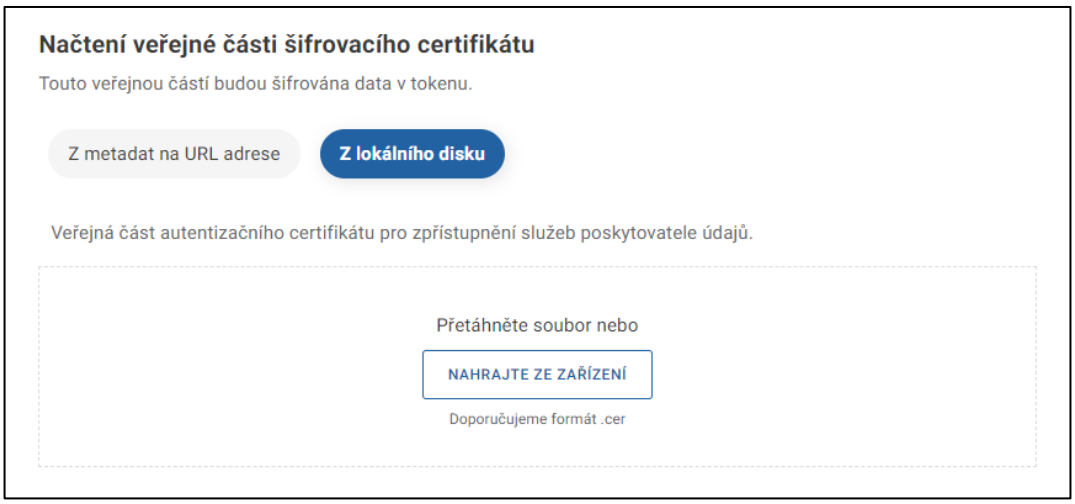
12. Načtení veřejné části certifikátu. V produkčním prostředí národního bodu je použití certifikátu povinné.

    a. Adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu. Okno se základními informacemi o certifikátu (certifikát dostupný z vyplněné URL adresy pro metadata certifikátu) je možné načíst prostřednictvím tlačítka „Zobrazit“. Cesta k certifikátu může být pouze na portu 80 nebo 443.

    Toto slouží pro kontrolu správně zadané cesty k certifikátu. Tato položka nemusí být vyplněna v případě, je-li veřejná část příslušného certifikátu načtena z lokálního disku (viz níže bod 8.b).

Obrázek 12 - Založení konfigurace – část Načtení certifikátu z metadat

b. Druhou možností pro načtení veřejné části šifrovacího certifikátu je načtení z lokálního disku. Tlačítko „Načíst“ zobrazí okno pro zadání cesty, odkud má dojít k načtení certifikátu. Tento certifikát je uložen u konfigurace (po stisknutí tlačítka Uložit). V případě, že jsou vyplněny obě možnosti pro získání certifikátu, je upřednostněn certifikát z URL adresy pro metadata (viz výše bod 8.a).



Obrázek 13 - Založení konfigurace – část Načtení certifikátu z disku

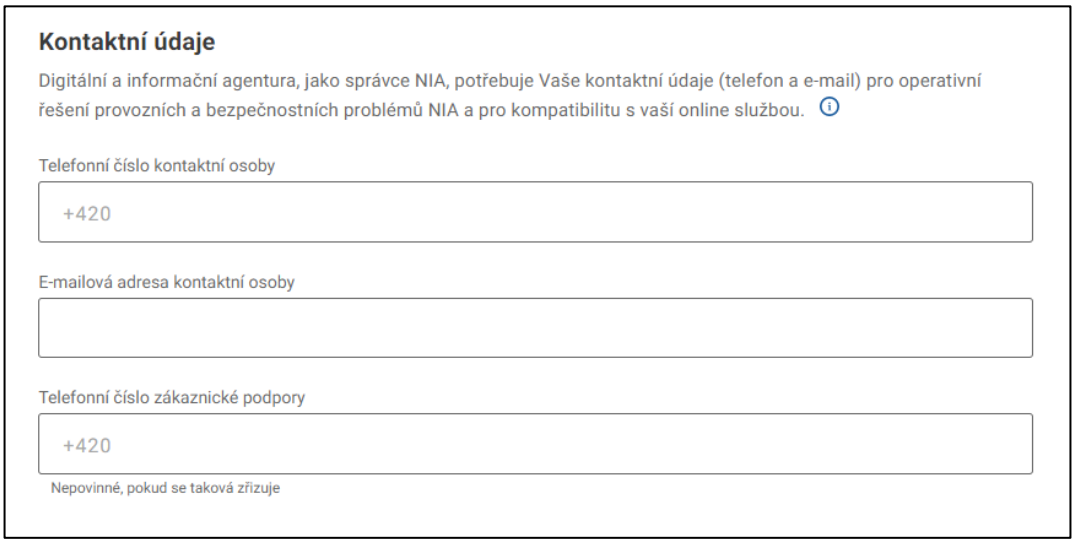
13. Logo kvalifikovaného poskytovatele, které je zapotřebí vložit v podporovaném typu souboru (PNG či JPEG) a zároveň v požadovaném formátu (s minimální velikostí 65 x 65 pixelů). Načtení loga probíhá z lokálního disku skrze tlačítko „Vložit“. Po načtení vybraného loga z adresáře, které odpovídá požadovanému formátu a typu souboru, se ve formuláři pro konfiguraci kvalifikovaného poskytovatele zobrazí náhled na vložené logo.

Obrázek 14 - Založení konfigurace – část Načtení loga

Kontaktní údaje

14. Telefonní číslo kontaktní osoby pro případ nutnosti kontaktování od zástupců Digitální a informační agentury.
15. E-mailová adresa kontaktní osoby pro případ nutnosti kontaktování od zástupců Digitální a informační agentury.
16. Telefonní číslo zákaznické podpory uvádějte v případě, že je takováto podpora zřízena. Kontakt je uváděn pro případ nutnosti kontaktování od zástupců Digitální a informační agentury.

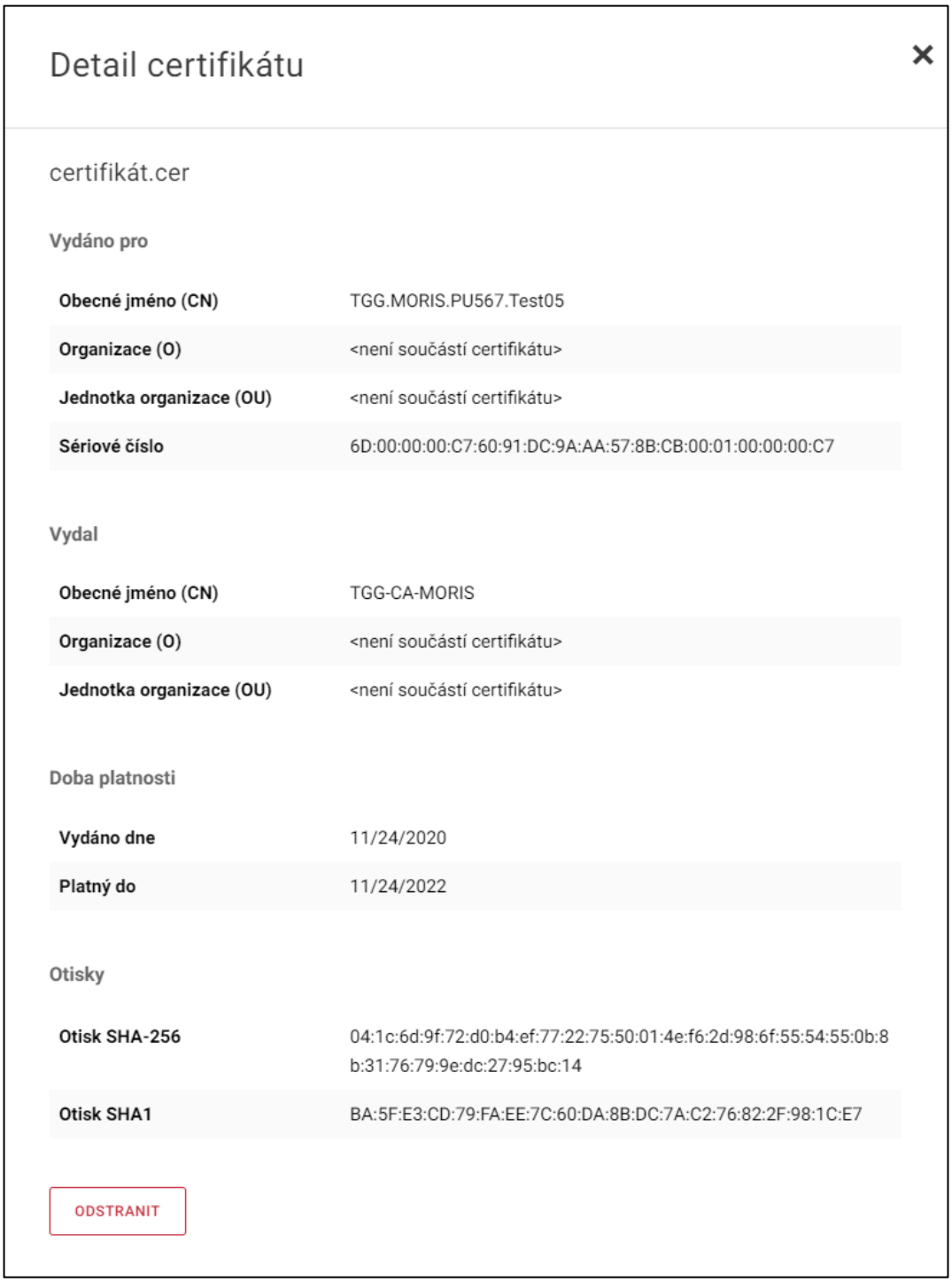
Tyto kontaktní údaje slouží především pro operativní řešení provozních a bezpečnostních problémů.



Obrázek 15 - Založení konfigurace – část Kontaktní údaje

V rámci editace konfigurace je možné provést změnu zařazení kvalifikovaného poskytovatele do jiné skupiny určující výdej pseudonymu (BSI). Kvalifikovaný poskytovatel získá pseudonym konkrétního občana dle skupiny, do které byl poskytovatel přiřazen. Tzn., že kvalifikovaní poskytovatelé, kteří jsou přiřazeni do stejné skupiny, obdrží na základě autentizace občana vždy stejný identifikátor.

Níže je vidět detail veřejné části certifikátu, který byl načten a uložen na serveru. Detail obsahuje informace, pro koho byl certifikát vydán, kdo certifikát vydal, dobu platnosti certifikátu a hodnotu otisků certifikátu.



Obrázek 16 - Načtený certifikát – veřejná část certifikátu uložená na serveru

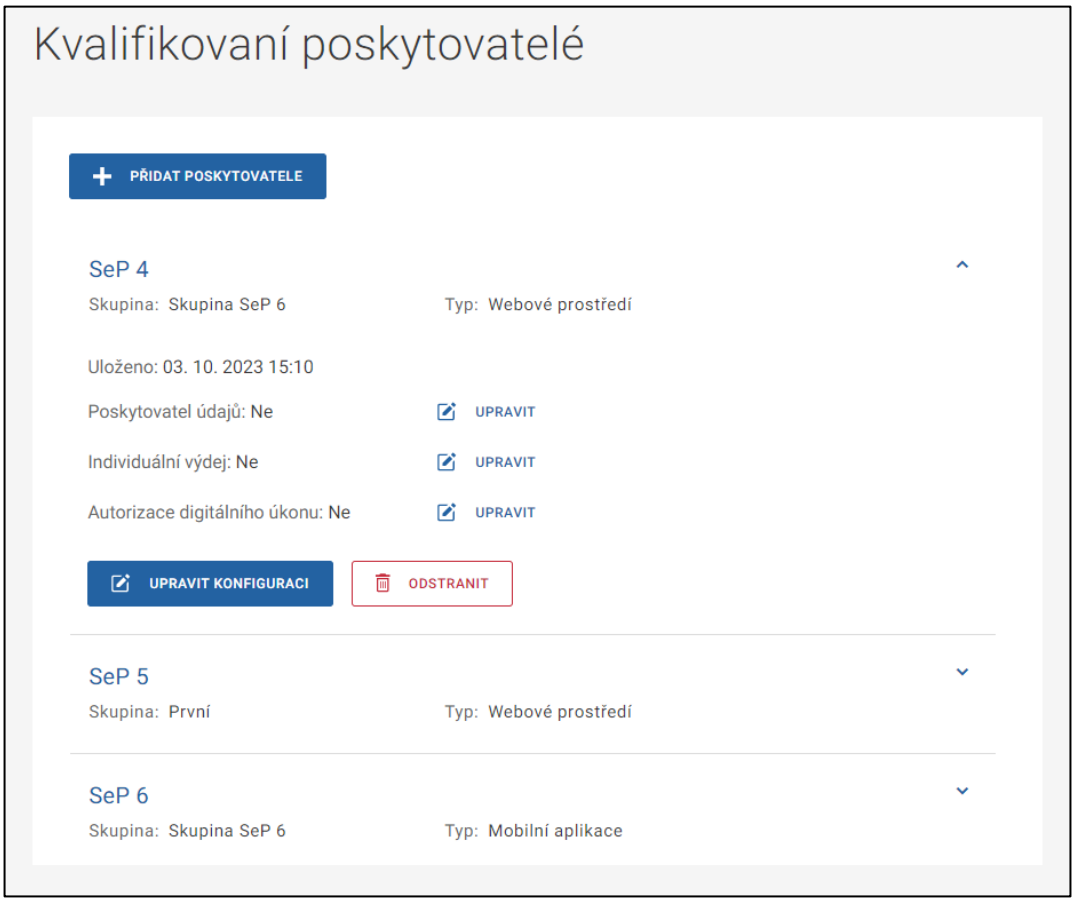
Certifikát z metadat čteme z **encryption** části KeyDescriptor:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="">
  <md:SPSSODescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate></ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Připravenou konfiguraci poskytovatele služeb dokončíte kliknutím na tlačítko „Uložit“.

Obrázek 17 - Dokončení konfigurace kvalifikovaného poskytovatele

Vytvořená konfigurace poskytovatele služeb se vám zobrazí v Seznamu konfigurací kvalifikovaných poskytovatelů včetně základních informací o této konfiguraci. V rámci organizace můžete vytvářet i další konfigurace poskytovatelů služeb. Všechny tyto konfigurace pak uvidíte ve zmíněném Seznamu konfigurací kvalifikovaných poskytovatelů. Z tohoto seznamu pak můžete jednotlivé konfigurace také odstranit nebo jejich nastavení upravit.

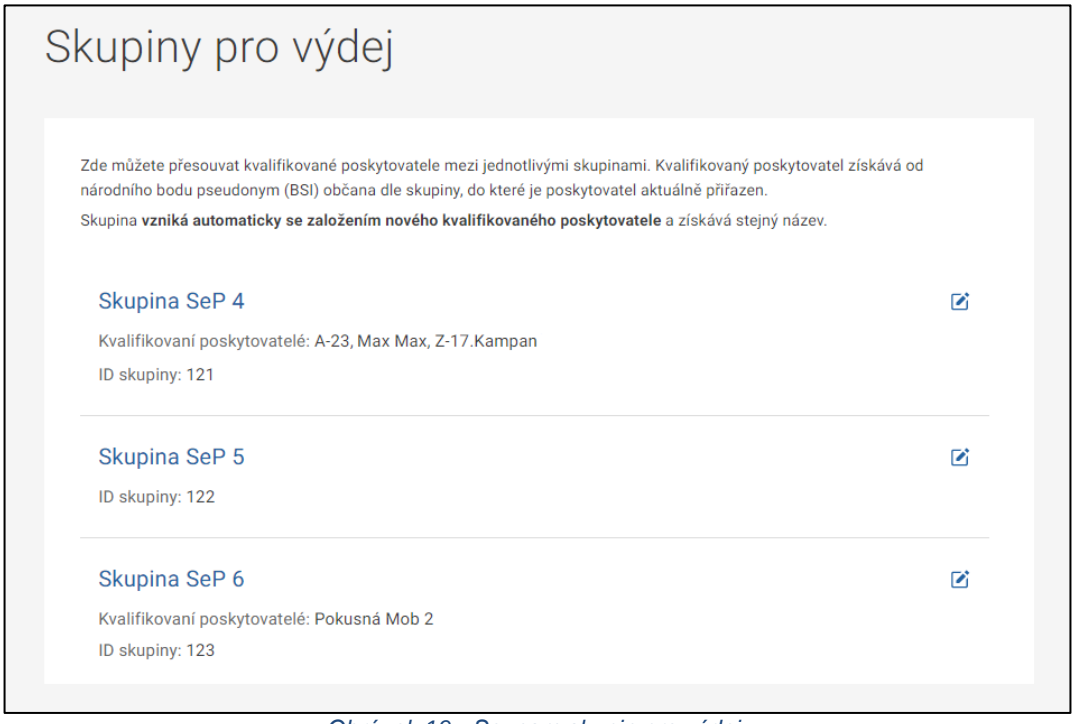


Obrázek 18 - Seznam vytvořených konfigurací kvalifikovaných poskytovatelů

7.5. Správa skupin pro výdej

Po založení jednoho či více kvalifikovaných poskytovatelů (konfigurací) můžete v rámci hlavní nabídky zvolit možnost „Skupiny pro výdej“. Správa skupin pro výdej slouží pro přesun kvalifikovaných poskytovatelů mezi jednotlivými skupinami. Kvalifikovaný poskytovatel získává od národního bodu pseudonym (BSI) občana dle skupiny, do které je poskytovatel aktuálně přiřazen. Tzn., že kvalifikovaní poskytovatelé, kteří jsou přiřazeni do stejné skupiny, obdrží na základě autentizace občana vždy stejný pseudonym (BSI).

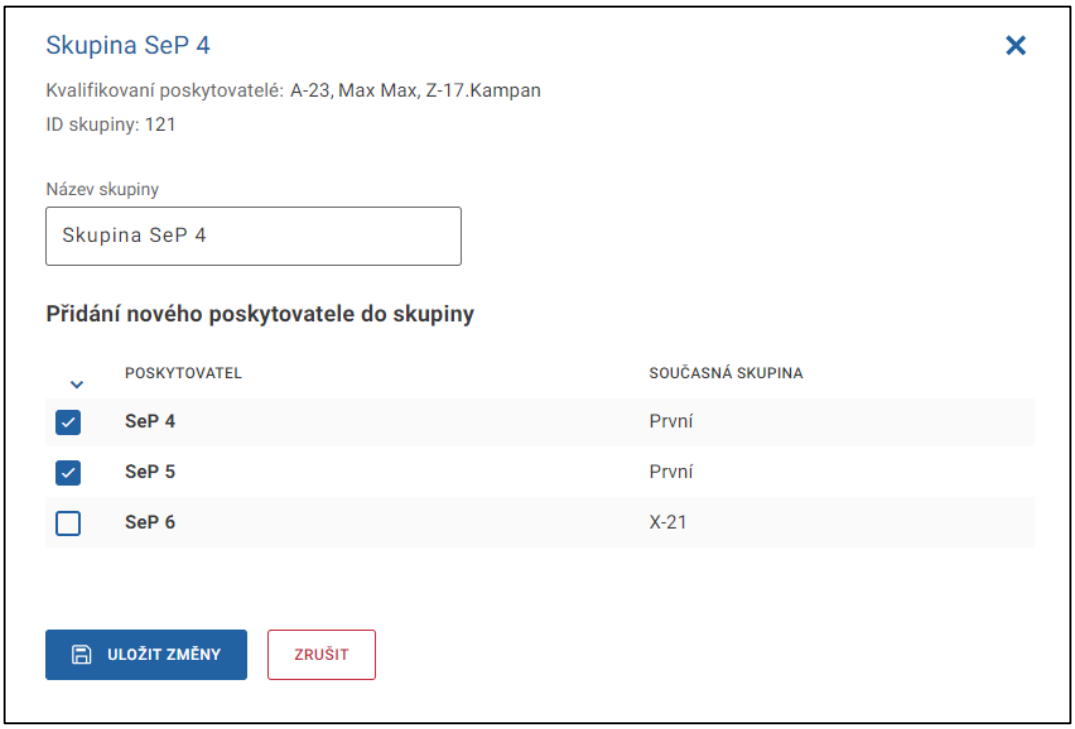
Skupina vzniká automaticky se založením nového kvalifikovaného poskytovatele a získává stejný název. Ve správě skupin pro výdej je pak možné název měnit.



Obrázek 19 - Seznam skupin pro výdej

Na základě výběru konkrétní skupiny ze seznamu se zobrazí detail této skupiny. V detailu je možné změnit název skupiny kvalifikovaných poskytovatelů a přiřadit do této skupiny kvalifikované poskytovatele z jiných skupin. Každý kvalifikovaný poskytovatel musí být zařazen do některé skupiny. Název skupiny je určen především pro vaše odlišení jednotlivých skupin.

Hned v úvodu je uveden výčet těch kvalifikovaných poskytovatelů, kteří jsou přiřazeni do vybrané skupiny („Kvalifikovaní poskytovatelé“). Tito poskytovatelé tak dostávají pro konkrétního občana na základě jeho autentizace shodný identifikátor. Níže uvedený seznam pak obsahuje výčet všech kvalifikovaných poskytovatelů dané organizace, kteří nejsou přiřazeni do zobrazené skupiny. Zaškrtnutím označíte ty kvalifikované poskytovatele, které chcete pod aktuálně zobrazenou skupinu přesunout. Po změně přiřazení kvalifikovaného poskytovatele, případně změně názvu skupiny, je nutné potvrdit změny uložením.



Obrázek 20 - Detail vybrané skupiny a změna zařazení

8. Technické informace

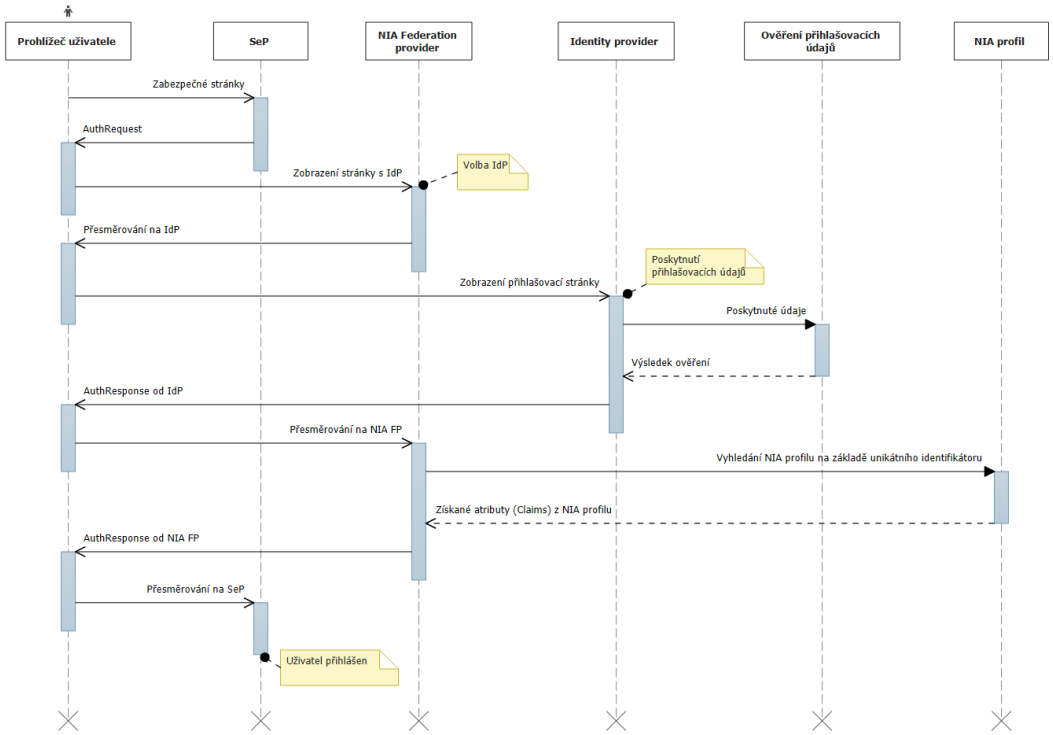
Komunikace mezi web aplikací poskytovatele služeb a národním bodem je založena na principu pasivní federace, kde probíhá výměna SAML tokenů, které musí umět webová aplikace poskytovatele služeb zpracovat.

Komunikace mezi web aplikací a národním bodem může být založena na stávajících standardech:

- WS-Federation,
- SAML 2.

Programátor webové aplikace poskytovatele služeb si může vybrat, který standard komunikace vybere a v něm implementovat proces žádosti o přihlášení, zpracování přijatých tokenů a proces odhlášení uživatele

Následující obrázek ukazuje sekvenční diagram pro celý přihlašovací proces.



Obrázek 21 - Sekvenční diagram přihlašovacího procesu

V případě, kdy bude na Identitu občana směřováno větší množství požadavků na přihlášení, než jaké by zvládla v danou chvíli obsloužit, budou uživatelé frontováni

a odbavováni postupně dle technických možností Identity občana. V takovém případě může přihlašování trvat jednotky až desítky minut.

8.1. Přihlášení pomocí mezinárodního eIDAS uzlu

V případě autentizace uživatele přes mezinárodní eIDAS uzel je předáván omezený seznam atributů a kvalifikovaný poskytovatel tomu musí přizpůsobit svůj systém.
Základní sada údajů je:

- Unikátní identifikátor příslušné země (BSI)
- Jméno
- Příjmení
- Datum narození

U některých zemí je možné předal další atributy:

- Aktuální adresa
- Místo narození

Autentizaci zahraniční identitou může kvalifikovaný poskytovatel detekovat z předaného BSI, které je v případě autentizace některým z českých kvalifikovaných správců.
BSI má následující formát XX/YY/AAA, kdy

- XX = identifikátor vydávající země
- YY = identifikátor země pro kterou byl identifikátor vydán
- AAA = unikátní kód uživatele dle dané země

Zde uvádíme příklady identifikátorů z testovacího prostředí:

1. Identifikátor používaný v rámci ČR
    - CZ/CZ/f46d044b-52ea-4d56-bf33-4cc3fd0f196c
2. Identifikátor vydaný Švédským královstvím pro ČR – přihlášení přes eIDAS
    - SE/CZ/198611062384

Přehled základních informací ohledně stavu notifikace prostředků jednotlivých zemí je možné získat na odkaze: Overview of pre-notified and notified eID schemes under eIDAS

Upozornění: V případě přihlášení zahraniční identity není možné využít služby základních registrů E226 eidentitaCtiAifo pro překlad BSI na AIFO^{AIS} dané agendy.

8.2. Důležité URL adresy

Testovací prostředí	
URL	**Popis**
https://twww.identitaobcana.cz/	Testovací portál národního bodu
https://tnia.identitaobcana.cz/FPSTS/default.aspx	URL pro zasílání AuthRequest a LogoutRequest pro standard WS-Federaton
https://tnia.identitaobcana.cz/FPSTS/saml2/basic	URL pro zasílání AuthRequest a LogoutRequest pro standard SAML2/eIDAS
https://tnia.identitaobcana.cz/FPSTS/FederationMetadata/2007-06/FederationMetadata.xml	Metadata SAML

Tabulka 2 - URL adresy pro testovací prostředí

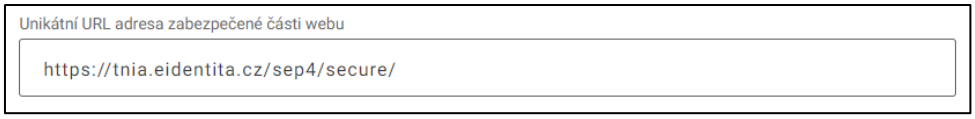
Produkční prostředí	
URL	**Popis**
https://www.identitaobcana.cz/	Produkční portál národního bodu
https://nia.identitaobcana.cz/FPSTS/default.aspx	URL pro zasílání AuthRequest a LogoutRequest pro standard WS-Federaton
https://nia.identitaobcana.cz/FPSTS/saml2/basic	URL pro zasílání AuthRequest a LogoutRequest pro standard SAML2/eIDAS
https://nia.identitaobcana.cz/FPSTS/FederationMetadata/2007-06/FederationMetadata.xml	Metadata SAML

Tabulka 3 - URL adresy pro produkční prostředí

8.3. Mapování registračních kroků na technické specifikace

Výše uvedený postup registrace a konfigurace poskytovatele služeb je nezbytný k tomu, aby byla NIA připravena zpracovat AuthRequest (žádost o ověření) a zaslat zpět AuthResponse (vytvořený SAML token).

1. **Unikátní adresa**



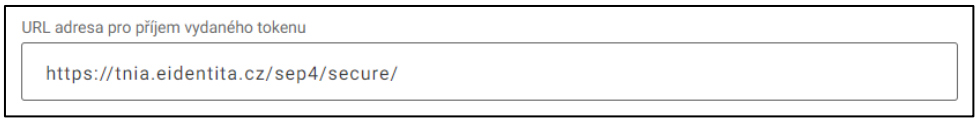
Jedná se o základní rozlišovací údaj SeP v NIA, který musí být ve formátu URI a může být použita pouze jednou. NIA při zadávání kontroluje duplicity této hodnoty. Pro tuto zaregistrovanou URL adresu jsou generovány unikátní identifikátory uživatelů. Změna URL po registraci způsobí, že budou generovány nové identifikátory uživatelů. K této URL adrese se také váží souhlasy, které uživatel při přihlašování k SeP uděluje.

Zaregistrovaná hodnota URL se musí povinně uvádět v zasílaném AuthRequest.

Standard	**Parametr**
WS-Federation	wtrealm
SAML 2/eIDAS	Issuer

Při chybějící registraci, špatné registraci anebo špatně uvedené hodnotě v AuthRequest vyhodnotí NIA žádost o přihlášení jako neplatnou a zobrazí chybové hlášení „Nedůvěryhodný poskytovatel služeb“.

2. **Adresa pro příjem vydaného tokenu**

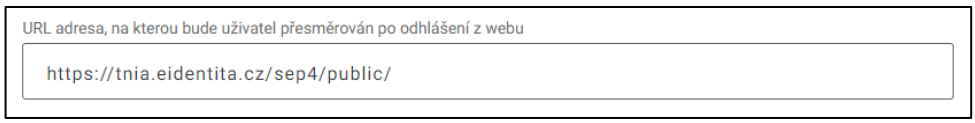


Specifikuje, kam bude NIA přesměrovávat komunikace po vydání finálního tokenu.

Standard	**Parametr**
WS-Federation	wreply
SAML 2/eIDAS	AssertionConsumerServiceURL

Parametry v AuthRequest jsou nepovinné. Pokud nebudou uvedeny, bude pro návrat použita zaregistrovaná URL adresa. Pokud parametry budou uvedeny, pak musí odpovídat zaregistrované adrese. V případě uvedení jiné než zaregistrované URL adresy pro návrat, bude vydávání tokenu zastaveno a bude zobrazeno chybové hlášení „Unable to complete the request“.

3. **URL adresa pro odhlášení**



Specifikuje, kam bude uživatel přesměrován při odhlášení z webové aplikace SeP (Logout Request). Je nutné si uvědomit, že národní bod využívá principy SSO. Tedy pokud se uživatel autentizuje prostřednictvím národního bodu k vám, jako poskytovateli služeb, může být toto přihlášení zpracováno jako SSO, protože je již uživatel přihlášen k jinému poskytovateli služeb. Odhlášení z vaší aplikace tedy neznamená odhlášení od národního bodu a uživatel, při novém přístupu na vaše stránky, může být bez jakékoliv další výzvy autentizován a identifikován na základě neukončeného autentizačního sezení buď s vámi, nebo jiným poskytovatelem služby. Proto je bezpodmínečně nutné implementovat proces odhlášení uživatele a tento LogOut request zasílat i na národní bod.

8.4. Požadavek na LoA

Požadavek na příslušné LoA se liší dle standardu, kterým SeP komunikuje.

8.4.1. Požadavek na LoA – Standard SAML 2/eIDAS

Při požadavku na přihlášení pomocí standardu SAML 2 se požadavek na LoA uvádí v elementu RequestedAuthnContext s atributem Comparison (hodnota = exact, minimum, maximum nebo better). Ve vnořeném elementu AuthnContextClassRef je pak hodnota LoA (hodnota = http://eidas.europa.eu/LoA/low, http://eidas.europa.eu/LoA/substantial nebo http://eidas.europa.eu/LoA/high).

Příklad:

```
<saml2p: RequestedAuthnContext Comparison="minimum">
   <saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/low</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

Více:
Technické specifikace eIDAS
Příklad AuthRequest

8.4.2. Požadavek na LoA – Standard WS-Federation

Při požadavku na přihlášení pomocí standardu WS-Federation se požadavek na LoA uvádí ve dvou elementech ClaimType:

1. **LoA**

Uri = http://eidas.europa.eu/LoA
Value = http://eidas.europa.eu/LoA/low, http://eidas.europa.eu/LoA/substantial nebo http://eidas.europa.eu/LoA/high

2. **Comparison**

Uri = http://schemas.microsoft.com/cgg/2010/identity/claims/LoAComparison
Value = minimum nebo maximum

Příklad:

```
<auth:ClaimType Uri="http://eidas.europa.eu/LoA" Optional="true">
  <auth:Value>http://eidas.europa.eu/LoA/substantial</auth:Value>
</auth:ClaimType>
<auth:ClaimType Uri="http://schemas.microsoft.com/cgg/2010/identity/claims/LoAComparison" Optional="true">
  <auth:Value>minimum</auth:Value>
</auth:ClaimType>
```

Více:
Příklad RequestsSecurityToken

8.5. Příklady

Sestavení AuthRequest/RequestSecurityToken a zpracování AuthResponse se řídí specifikacemi WS-Federation nebo SAML 2 Core a eIDAS.

8.5.1. Příklad AuthRequest

Požadavek o přihlášení musí obsahovat seznam atributů (claims), které jsou požadovány v návratovém SAML tokenu.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
ID="id19cd34deb3c140de8c6eb6790da3de13" Version="2.0" IssueInstant="2018-03-26T14:31:54Z"
Destination="https://tnia.identitaobcana.cz/FPSTS/saml2/basic"
AssertionConsumerServiceURL="https://tnia.identitaobcana.cz/sep5/AuthServices/Acs">
  <saml2:Issuer>https://tnia.identitaobcana.cz/sep5/</saml2:Issuer>
  <saml2p:RequestedAuthnContext Comparison="minimum">

<saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/low</saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
  <saml2p:Extensions xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:eidas="http://eidas.europa.eu/saml-extensions">
    <eidas:SPType>public</eidas:SPType>
    <eidas:RequestedAttributes>
```

```
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/CurrentAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute Name="http://www.stork.gov.eu/1.0/countryCodeOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute Name="http://www.stork.gov.eu/1.0/eMail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute Name="http://www.stork.gov.eu/1.0/age"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute Name="http://www.stork.gov.eu/1.0/isAgeOver"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false">
        <eidas:AttributeValue>18</eidas:AttributeValue>
      </eidas:RequestedAttribute>
      <eidas:RequestedAttribute
Name="http://schemas.eidentita.cz/moris/2016/identity/claims/phonenumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://schemas.eidentita.cz/moris/2016/identity/claims/tradresaid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://schemas.eidentita.cz/moris/2016/identity/claims/idtype"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
      <eidas:RequestedAttribute
Name="http://schemas.eidentita.cz/moris/2016/identity/claims/idnumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false" />
    </eidas:RequestedAttributes>
  </saml2p:Extensions>
</saml2p:AuthnRequest>
```

8.5.2. Příklad AuthResponse

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://eidas-connector.at/post"
ID="_5a15625de8618920748123042db52367" InResponseTo="_171ccc6b39b1e8f6e762c2e4ee4ded3a"
IssueInstant="2015-04-30T19:27:20.159Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://eidas-
service.eu</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#_5a15625de8618920748123042db52367">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
```

```
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="xs"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <ds:DigestValue>t5V4hqAh4Nxjd49H/rC+N9tN/dNHBNuCOco1v1GYfFc=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>GX2==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIDPWA==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </saml2p:Status>
  <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="encrypted-data-0-1152532362-41467517-23174"
Type="http://www.w3.org/2001/04/xmlenc#Content">
      <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <xenc:EncryptedKey Id="encrypted-key-1-1152532362-41467527-29158-c0">
          <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
          <ds:KeyInfo>
            <ds:KeyValue>
              <ds:RSAKeyValue>
                <ds:Modulus>vOD </ds:Modulus>
                <ds:Exponent>AQAB </ds:Exponent>
              </ds:RSAKeyValue>
            </ds:KeyValue>
          </ds:KeyInfo>
          <xenc:CipherData>
            <xenc:CipherValue>MDTq </xenc:CipherValue>
          </xenc:CipherData>
        </xenc:EncryptedKey>
      </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>NhUqASe+jJ0BHqTX4sayQLz7qUNbO8Wdj9qEI4wm+9Mbml3Agfjluw==
</xenc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedData>
  </saml2:EncryptedAssertion>
</saml2p:Response>
```

8.5.3. SAML Assertion

```
<?xml version="1.0" encoding="UTF-8"?>
<Assertion ID="_f831b636-e495-4e40-afef-c6a03001ad8a" IssueInstant="2018-03-
26T14:32:32.692Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  <Issuer>urn:microsoft:cgg2010:FPSTS</Issuer>
  <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">CZ/CZ/2e3883ee-
7e0d-47cb-8fee-2ea231a58ee6</NameID>
    <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <SubjectConfirmationData InResponseTo="id19cd34deb3c140de8c6eb6790da3de13"
NotOnOrAfter="2018-03-26T15:32:32.692Z"
Recipient="https://tnia.identitaobcana.cz/sep5/AuthServices/Acs" />
```

```
    </SubjectConfirmation>
  </Subject>
  <Conditions NotBefore="2018-03-26T14:32:32.692Z" NotOnOrAfter="2018-03-
26T15:32:32.692Z">
    <AudienceRestriction>
      <Audience>https://tnia.identitaobcana.cz/sep5/</Audience>
    </AudienceRestriction>
  </Conditions>
  <AttributeStatement>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="CurrentFamilyName" a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:CurrentFamilyNameType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">FORMÁNEK</AttributeValue>
    </Attribute>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="CurrentGivenName" a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:CurrentGivenNameType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">MILAN</AttributeValue>
    </Attribute>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="DateOfBirth"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:DateOfBirthType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">1968-03-29</AttributeValue>
    </Attribute>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="PlaceOfBirth"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:PlaceOfBirthType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">Hlízov</AttributeValue>
    </Attribute>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentAddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="CurrentAddress"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:CurrentAddressType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchemainstance">PGVpZGFzOkxvY2F0b3JEZXNpZ25hdG9yPjM4PC9
laWRhczpMb2NhdG9yRGVzaWduYXRvcj4KPGVpZGFzOlRob3JvdWdoZmFyZT48L2VpZGFzOlRob3JvdWdoZmFyZT4KP
GVpZGFzOlBvc3ROYW1lPlN0YXLDqSBLxZllxI1hbnk8L2VpZGFzOlBvc3ROYW1lPgo8ZWlkYXM6UG9zdENvZGU+NDA
3NjE8L2VpZGFzOlBvc3RDb2RlPgo8ZWlkYXM6Q3ZhZGRyZXNzQXJlYT5TdGFyw6kgS8WZZcSNYW55PC9laWRhczpDd
mFkZHJlc3NBcmVhPg==</AttributeValue>
    </Attribute>
    </Attribute>
    <Attribute Name="http://www.stork.gov.eu/1.0/isAgeOver"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="IsAgeOver"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue>True</AttributeValue>
    </Attribute>
    <Attribute Name="http://www.stork.gov.eu/1.0/age"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Age"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue>49</AttributeValue>
```

```
    </Attribute>
    <Attribute Name="http://www.stork.gov.eu/1.0/countryCodeOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="CountryCodeOfBirth" a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue>CZ</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.eidentita.cz/moris/2016/identity/claims/idnumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="ZR10 IdNumber"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue>111111980</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.eidentita.cz/moris/2016/identity/claims/idtype"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="ZR10 IdType"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue>ID</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.eidentita.cz/moris/2016/identity/claims/tradresaid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="TRadresaID"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">

<AttributeValue>PFRSYWRyZXNhSUQgeG1sbnM9Imh0dHA6Ly9zY2hlbWFzLmVpZGVudGl0YS5jei9tb3Jpcy8yMD
E2L2lkZW50aXR5L2NsYWltcy90cmFkcmVzYWlkIj4NCiAgPG9rcmVzS29kPjM1MDI8L29rcmVzS29kPg0KICA8b2Jl
Y0tvZD41NjIzNDM8L29iZWNLb2Q+DQogIDxjYXN0T2JjZUtvZD40MzQ8L2Nhc3RPYmNlS29kPg0KICA8dWxpY2VLb2
Q+PC91bGljZUtvZD4NCiAgPHBvc3RhS29kPjQwNzE0PC9wb3N0YUtvZD4NCiAgPHN0YXRlYm5pT2JqZWt0S29kPg0KICA8YWRyZXNuaU1pc3RvS29kPjEyMzY8L2FkcmVzbmlNaXN0b0tvZD4NCi
AgPGNpc2xvRG9tb3ZuaT4xNjc8L2Npc2xvRG9tb3ZuaT4NCiAgPGNpc2xvT3JpZW50YWNuaT48L2Npc2xvT3JpZW50
YWNuaT4NCiAgPGNpc2xvT3JpZW50YWNuaVBpc21lbm8+PC9jaXNsb09yaWVudGFjbmlQaXNtZW5vPg0KPC9UUmFkcm
VzYUlEPg==</AttributeValue>
    </Attribute>
    <Attribute Name="http://www.stork.gov.eu/1.0/eMail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Email"
a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:string"
xmlns:tn="http://schemas.microsoft.com/cgg/2016/identity/claims/approvedclaim"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">petr.xxx@yyy.cz</AttributeValue>
    </Attribute>
    <Attribute Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
FriendlyName="PersonIdentifier" a:OriginalIssuer="urn:microsoft:cgg2010:FPSTS"
xmlns:a="http://schemas.xmlsoap.org/ws/2009/09/identity/claims">
      <AttributeValue b:type="tn:PersonIdentifierType"
xmlns:tn="http://eidas.europa.eu/attributes/naturalperson"
xmlns:b="http://www.w3.org/2001/XMLSchema-instance">CZ/CZ/1x3953xx-7e0d-47xx-8fee-
2ea231a58ee6</AttributeValue>
    </Attribute>
  </AttributeStatement>
</Assertion>
```

Dekódované CurrentAddress:

```
<eidas:LocatorDesignator>38</eidas:LocatorDesignator>
<eidas:Thoroughfare></eidas:Thoroughfare>
<eidas:PostName>Staré Křečany</eidas:PostName>
<eidas:PostCode>40761</eidas:PostCode>
<eidas:CvaddressArea>Staré Křečany</eidas:CvaddressArea>
```

Dekódované TRadresaID:

```
<TRadresaID xmlns="http://schemas.eidentita.cz/moris/2016/identity/claims/tradresaid">
<okresKod>3502</okresKod>
<obecKod>562343</obecKod>
<castObceKod>434</castObceKod>
<uliceKod></uliceKod>
<postaKod>40714</postaKod>
<stavebniObjektKod>1236</stavebniObjektKod>
<adresniMistoKod>1236</adresniMistoKod>
<cisloDomovni>167</cisloDomovni>
<cisloOrientacni></cisloOrientacni>
<cisloOrientacniPismeno></cisloOrientacniPismeno>
</TRadresaID>
```

8.5.4. Příklad LogoutRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://tnia.identitaobcana.cz/FPSTS/saml2/basic"
ID="a2ci56eag134d254336gi635a85ffh0" IssueInstant="2018-07-13T08:22:27.075Z"
Version="2.0">
  <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://123xxx123.com/auth</saml2:Issu
er>
  <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">CZ/CZ/6e252c2e-xxxx-xxxx-
xxxx-be65f7b6a689</saml2:NameID>
  <saml2p:SessionIndex>_05ee8e73fa8043f3aafcf148e7bcceeb</saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

8.5.5. Příklad LogoutResponse

```
<LogoutResponse ID="_a78e9b68-d2df-4948-9505-3ecb8ef5d302" Version="2.0"
IssueInstant="2018-07-13T08:23:16Z" InResponseTo="a2ci56eag134d254336gi635a85ffh0"
Destination="https:// 123xxx123.com/auth/nia/sso"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">urn:microsoft:cgg2010:FPSTS</Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </Status>
</LogoutResponse>
```

8.5.6. Příklad RequestSecurityToken

HTTP method: GET
String Query Parameters:

1. **wa:**

   wsignin1.0

2. wtrealm:

https://www.sep.cz/secure

3. wctx:

rm=0&id=passive&ru=%2fsecure%2f

4. wct:

2023-11-21T13:44:17Z

5. wreq:

```
<RequestSecurityToken xmlns="http://schemas.xmlsoap.org/ws/2005/02/trust">
  <Claims xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" Dialect="http://docs.oasis-
open.org/wsfed/authorization/200706/authclaims" xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
    <auth:ClaimType Uri="http://schemas.microsoft.com/cgg/2010/identity/claims/profileid" Optional="true" />
    <auth:ClaimType Uri="http://schemas.microsoft.com/cgg/2010/identity/claims/profilestate" Optional="true" />
    <auth:ClaimType Uri="http://schemas.microsoft.com/cgg/2010/identity/claims/profiletype" Optional="true" />
    <auth:ClaimType Uri=" http://schemas.microsoft.com/cgg/2010/identity/claims/idprealm" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/CurrentAddress" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth" Optional="true" />
    <auth:ClaimType Uri="http://schemas.eidentita.cz/moris/2016/identity/claims/idtype" Optional="true" />
    <auth:ClaimType Uri="http://schemas.eidentita.cz/moris/2016/identity/claims/idnumber" Optional="true" />
    <auth:ClaimType Uri="http://schemas.eidentita.cz/moris/2022/identity/claims/fullids" Optional="true" />
    <auth:ClaimType Uri="http://eidas.europa.eu/LoA" Optional="true">
      <auth:Value>http://eidas.europa.eu/LoA/substantial</auth:Value>
    </auth:ClaimType>
    <auth:ClaimType Uri="http://schemas.microsoft.com/cgg/2010/identity/claims/LoAComparison" Optional="true">
      <auth:Value>minimum</auth:Value>
    </auth:ClaimType>
  </Claims>
</RequestSecurityToken>
```

8.6. Atributy NIA dostupné při přihlášení

Obsah návratového SAML tokenu je definován vstupním seznamem atributů NIA. Přiložená tabulka obsahuje seznam atributů NIA, jejichž názvy (ClaimType) musí obsahovat požadavek o přihlášení, pokud jsou požadovány v návratovém SAML tokenu.

Atribut/ Element	FriendlyName	Type	Name (ClaimType)
Příjmení	CurrentFamilyName	eidas:CurrentFamilyNameType	http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName
Jméno	CurrentGivenName	eidas:CurrentGivenNameType	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
Datum narození	DateOfBirth	eidas:DateOfBirthType	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth
Místo narození	PlaceOfBirth	eidas:PlaceOfBirthType	http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth
Země narození	CountryCodeOfBirth	xs:string	http://www.stork.gov.eu/1.0/countryCodeOfBirth
Adresa pobytu	CurrentAddress	eidas:CurrentAddressType	http://eidas.europa.eu/attributes/naturalperson/CurrentAddress
E-mail	Email	xs:string	http://www.stork.gov.eu/1.0/eMail
Je starší než X	IsAgeOver	xs:string	http://www.stork.gov.eu/1.0/isAgeOver
Věk	Age	xs:string (po konverzi z interního int)	http://www.stork.gov.eu/1.0/age
Telefon	PhoneNumber	xs:string	http://schemas.eidentita.cz/moris/2016/identity/claims/phonenumber
Adresa pobytu (RUIAN kódy)	TRadresaID	xs:string	http://schemas.eidentita.cz/moris/2016/identity/claims/tradresaid
Pseudonym	PersonIdentifier	eidas:PersonIdentifierType	http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
Typ dokladu	IdType	xs:string	http://schemas.eidentita.cz/moris/2016/identity/claims/idtype
Číslo dokladu	IdNumber	xs:string	http://schemas.eidentita.cz/moris/2016/identity/claims/idnumber
Doklady	FullIds	xs:string	http://schemas.eidentita.cz/moris/2022/identity/claims/fullids

Tabulka 4 - Seznam jednotlivých ClaimType

8.6.1. Schéma CurrentAddressType

XSD schéma atributu CurrentAddressType, který je složen z více elementů.

```
<xsd:complexType name="CurrentAddressType">
  <xsd:annotation>
    <xsd:documentation>
      Current address of the natural person.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="LocatorDesignator" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="CvaddressArea" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="Thoroughfare" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="PostName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="PostCode" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```

8.6.2. Schéma TRadresaIDType

XSD schéma atributu TRadresaIDType, který je složen z více elementů.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns="http://schemas.eidentita.cz/moris/2016/identity/claims/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://schemas.eidentita.cz/moris/2016/identity/claims/"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="1">
  <xsd:attribute name="LatinScript" type="xsd:boolean" default="true"/>
  <xsd:complexType name="TRadresaIDType">
    <xsd:annotation>
      <xsd:documentation>Current address of the natural person.</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="okresKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="obecKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="castObceKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="uliceKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="postaKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="stavebniObjektKod" type="xsd:string" minOccurs="0"
maxOccurs="1"/>
      <xsd:element name="adresniMistoKod" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="cisloDomovni" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="cisloOrientacni" type="xsd:string" minOccurs="0" maxOccurs="1"/>
      <xsd:element name="cisloOrientacniPismeno" type="xsd:string" minOccurs="0"
maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

8.6.3. Schéma a kódování FullIds

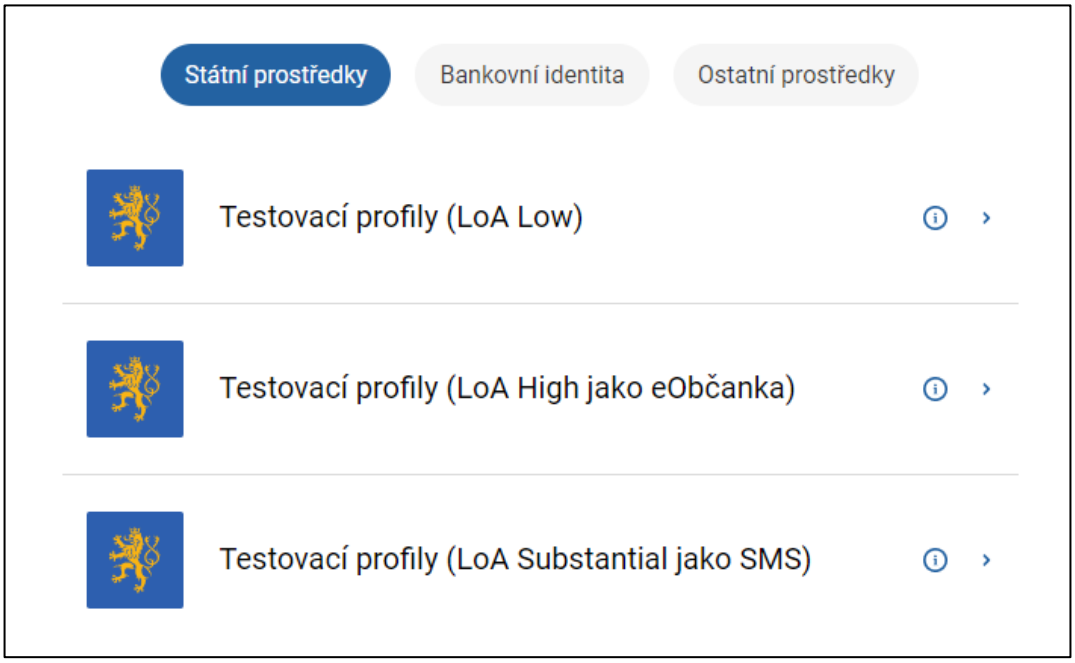
Hodnota atributu FullIds je XML zakódované pomocí Base64. XML odpovídá níže uvedenému XSD schématu.

XSD schéma atributu FullIds:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace=http://schemas.eidentita.cz/moris/2022/identity/claims/fullids
xmlns:xsd=http://www.w3.org/2001/XMLSchema>
  <xsd:element name="FullIds">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="Doklad" maxOccurs="unbounded" minOccurs="0">
          <xsd:complexType>
            <xsd:sequence>
              <xsd:element type="xsd:string" name="Cislo"/>
              <xsd:element type="xsd:string" name="Druh"/>
              <xsd:element name="PlatnostDo">
                <xsd:simpleType>
                  <xsd:union>
                            <xsd:simpleType>
                      <xsd:restriction base="xsd:date"></xsd:restriction>
                    </xsd:simpleType>
                    <xsd:simpleType>
                      <xsd:restriction base="xsd:string">
                        <xsd:whiteSpace value="collapse" />
                        <xsd:length value="0" />
                      </xsd:restriction>
                    </xsd:simpleType>
                  </xsd:union>
                </xsd:simpleType>
              </xsd:element >
            </xsd:sequence>
          </xsd:complexType>
        </xsd:element>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

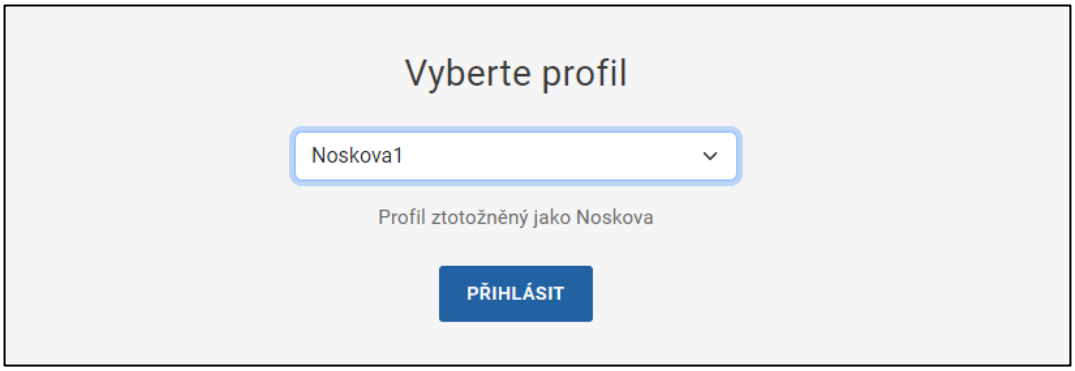
8.7. Testovací profily

Na testovacím prostředí národního bodu je k dispozici interní IdP s názvem "Testovací profily". Tento způsob ověření slouží pro otestování přihlášení k SeP.



Obrázek 22 - Výběr z testovacích profilů

Pro využití těchto přednastavených Testovacích profilů není potřeba znalosti žádných přihlašovacích údajů.



Obrázek 23 - Přihlášení vybraným testovacím profilem

9. Individuální výdej

Po úspěšném založení konfigurace vám portál národního bodu zpřístupní funkcionalitu pro nastavení tzv. individuálního výdeje. Individuální výdej umožní kvalifikovanému poskytovateli zažádat o údaje občana kdykoliv, kdy je k němu občan přihlášen a souhlasí s výdejem požadovaných údajů. Tímto způsobem může kvalifikovaný poskytovatel požádat o doplnění údajů, které nezískal v rámci autentizace občana skrze národní bod. Pro představu fungování individuálního výdeje je v následující podkapitole uveden celý proces v jednotlivých krocích.

Popisy všech služeb uvedených v této kapitole jsou dostupné v samostatných dokumentech na úložišti vývojářské dokumentace.

9.1. Základní informace

Fungování individuálního výdeje národního bodu přiblíží následující body, které popisují celý proces od nastavení individuálního výdeje na portálu národního bodu až po získání požadovaných údajů. Detailní informace jsou uvedeny v dalších podkapitolách.

1. Kvalifikovaný poskytovatel provede nastavení individuálního výdeje na portálu národního bodu (viz následující podkapitola).
2. Po provedení nastavení zavolá kvalifikovaný poskytovatel službu TR_IV_SEP_SEZNAM_VSECH_UDAJU a získá seznam údajů (včetně detailnějších popisů), které jsou v rámci individuálního výdeje aktuálně poskytovány.
3. Kvalifikovaný poskytovatel provede na své straně příslušné implementační kroky, aby dokázal o dané údaje zažádat a následně je zpracovat.
4. Kvalifikovaný poskytovatel potřebuje získat v rámci svého procesu údaje o již přihlášeném uživateli. Zavolá službu TR_IV_SEP_SEZNAM_UDAJU a zjistí, zda má k požadovaným údajům od občana platný souhlas, příp. souhlasy.
5. Kvalifikovaný poskytovatel zjistí, že nemá pro všechny požadované údaje souhlasy a provede přesměrování občana na stránku národního bodu pro schválení výdeje údajů v rámci individuálního výdeje. V rámci přesměrování definuje kvalifikovaný poskytovatel údaje, ke kterým požaduje získat souhlas.
6. Občan udělí kvalifikovanému poskytovateli souhlas s výdejem požadovaných údajů a kvalifikovaný poskytovatel obdrží potřebné ID

souhlasu (případně souhlasů). Občan může udělit jednorázový nebo trvalý souhlas, případně může odmítnou udělení souhlasu s výdejem údajů.

7. Zavolá znovu službu TR_IV_SEP_SEZNAM_UDAJU a zjistí, zda má již všechny potřebné souhlasy a jaká jsou ID těchto souhlasů. Udělení trvalého souhlasu zneplatňuje původní trvalý souhlas a vzniká nový trvalý souhlas s novým ID. Proto je vhodné volat tuto službu znovu po udělení souhlasu občanem.
8. Kvalifikovaný poskytovatel má všechny potřebné souhlasy a zavolá službu TR_IV_SUBJEKT_VYDEJ_UDAJU pro výdej údajů v rámci individuálního výdeje, ve které definuje požadované údaje a k nim přiřadí ID souhlasu/ů.
9. Národní identitní autorita sesbírá v rámci individuálního výdeje požadované údaje z příslušných (a zároveň aktuálně dostupných) datových zdrojů a odešle výsledky v odpovědi kvalifikovanému poskytovateli.

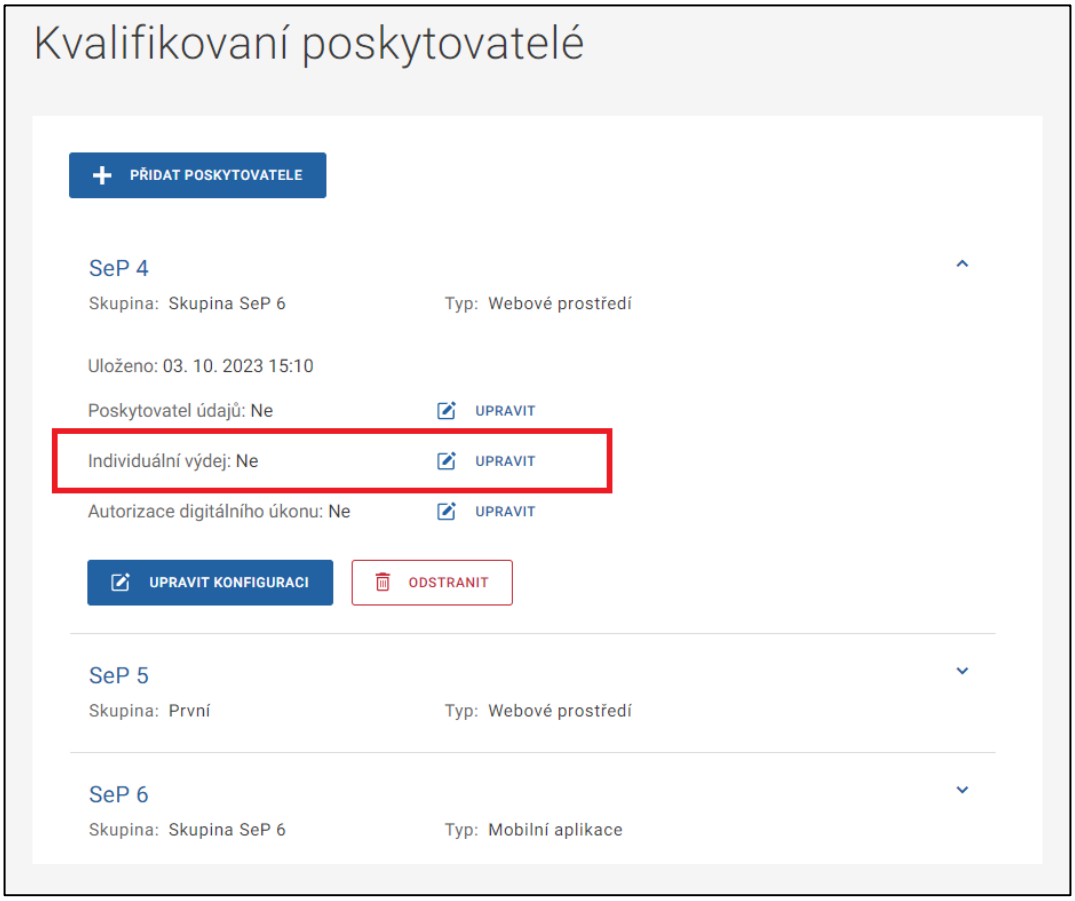
9.2. Poskytované atributy

Individuální výdej je připraven poskytovat data o občanovi z registru obyvatel, z registru osob (je-li podnikající fyzickou osobou) a z údajů vyplněných občanem samotným na portálu národního bodu („Moje údaje“). Dále mohou být poskytovány údaje od kvalifikovaných poskytovatelů, kteří se rozhodnou být zároveň poskytovatelem údajů (viz kapitola Poskytovatel údajů). Individuální výdej je zároveň do budoucna připraven pro získávání dat z dalších agend veřejné správy. Seznam poskytovaných údajů skrze individuální výdej, který je dostupný prostřednictvím služby TR_IV_SEP_SEZNAM_VSECH_UDAJU, se tak může měnit/rozšiřovat.

Vzor odpovědi obsahující aktuálně nabízené údaje z registru obyvatel, registru osob a vámi vyplněných údajů na portálu národního bodu je obsažen v dokumentaci popisující službu TR_IV_SUBJEKT_VYDEJ_UDAJU.

9.3. Nastavení individuálního výdeje

Po přihlášení k portálu národního bodu vyberete v seznamu konfigurací takového kvalifikovaného poskytovatele, pro kterého chcete nastavit možnost využívání individuálního výdeje a výběr potvrdíte tlačítkem „Nastavení individuálního výdeje“.

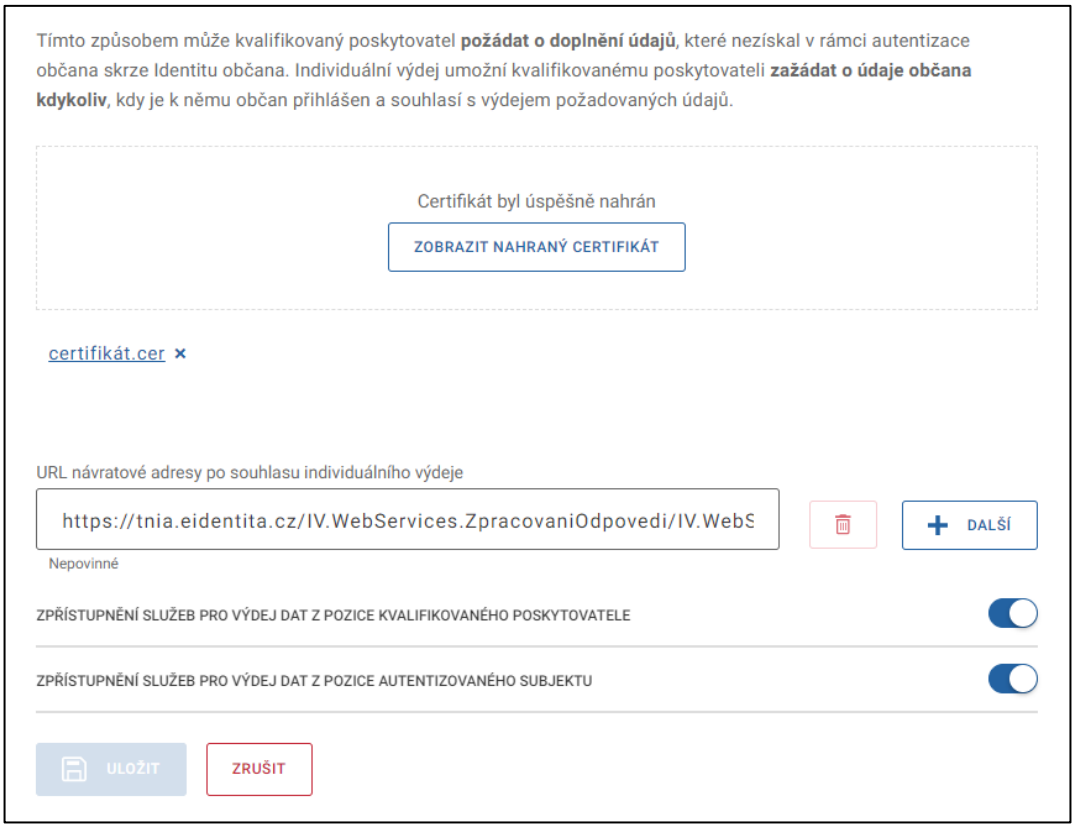


Obrázek 24 - Volba nastavení individuálního výdeje

Pro úspěšné nastavení individuálního výdeje u vybraného kvalifikovaného poskytovatele je potřeba vyplnit následující položky:

1. URL návratové adresy po souhlasu individuálního výdeje. Tlačítko „Přidat“ zobrazí okno pro zapsaní URL adresy, po úspěšném uložení URL adresy bude adresa zapsána do příslušného pole ve formuláři. Návratových adres je možné definovat více.
2. Načtení veřejné části autentizačního certifikátu pro zpřístupnění služeb pro individuální výdej dat je provedeno z lokálního disku. Tlačítko „Načíst“ zobrazí okno pro zadání cesty, odkud má dojít k načtení certifikátu. Tento certifikát je uložen u vybraného kvalifikovaného poskytovatele (po stisknutí tlačítka Uložit). Autentizační certifikát musí být podporován národní identitní autoritou a může se jednat o stejný autentizační certifikát jako v případě nastavení poskytovatele údajů. Totožný autentizační certifikát může být použit pouze v rámci stejného kvalifikovaného poskytovatele.

Služby pro výdej dat z pozice kvalifikovaného poskytovatele či autentizovaného subjektu mohou být zakázány či opětovně povoleny pouze prostřednictvím Service Desku DIA a není je tedy možné z pozice uživatele upravovat. Nastavení individuálního výdeje dokončíte kliknutím na tlačítko „Uložit“.



Obrázek 25 - Nastavení individuálního výdeje

9.4. Služby individuálního výdeje

V rámci individuálního výdeje nabízí národní identitní autorita následující služby:

- Služba pro zjištění aktuálně nabízených údajů
- Služba pro zjištění souhlasů s výdejem údajů udělených občanem
- Přesměrování na stránky národní identitní autority pro udělení souhlasu
- Služba pro výdej požadovaných údajů

Popisy těchto služeb jsou dostupné v samostatných dokumentech na úložišti vývojářské dokumentace.

Služba pro zjištění aktuálně nabízených údajů

Národní identitní autorita vystavuje kvalifikovanému poskytovateli službu označenou jako *TR_IV_SEP_SEZNAM_VSECH_UDAJU*, která vrací informace o tom, které údaje jsou prostřednictvím individuálního výdeje aktuálně nabízeny. Ke každému údaji je uveden jeho identifikátor, název, popis, zdroj odkud údaj pochází a odkazy na dokumentaci. Na základě těchto informací se kvalifikovaný poskytovatel může připravit na příjem a zpracování požadovaných údajů.

Služba pro zjištění souhlasů s výdejem údajů udělených občanem
Služba označená jako *TR_IV_SEP_SEZNAM_UDAJU* na základě pseudonymu občana (SePP) na vstupu vrací informace o tom, k jakým atributům má občan pro daného kvalifikovaného poskytovatele aktuálně udělen souhlas/y s jejich výdejem. V odpovědi služby je tak vždy uveden identifikátor údaje a identifikátor uděleného souhlasu. Pokud nemá kvalifikovaný poskytovatel od občana souhlas/y ke všem požadovaným atributům, musí provést přesměrování občana na stránky národní identitní autority pro udělení souhlasu s výdejem údajů.

Přesměrování na stránky národní identitní autority pro udělení souhlasu
Pro zajištění potřebných souhlasů s výdejem údajů provede kvalifikovaný poskytovatel přesměrování přihlášeného občana na příslušnou stránku národní identitní autority. V rámci přesměrování definuje kvalifikovaný poskytovatel údaje, pro které požaduje souhlas. Na této stránce má občan možnost udělit trvalý souhlas, jednorázový souhlas nebo odmítnou výdej údajů o své osobě. Udělí-li občan jednorázový souhlas, je v odpovědi uveden i čas konce platnosti souhlasu. Občan má zároveň možnost určit, pro které požadované údaje chce souhlas udělit a tím tak rozsah údajů pro výdej omezit.

Udělením nového trvalého souhlasu se původní trvalý souhlas (existuje-li) pro daného kvalifikovaného poskytovatele zneplatní. Nový trvalý souhlas bude udělen jak k nově požadovaným údajů, tak k údajům z původního souhlasu. Nově vytvořený souhlas, který je identifikovaným novým ID, je tak rozšířením původního souhlasu.

Udělí-li občan jednorázový souhlas, má tento souhlas určitou dobu platnosti, po kterou může být použit. Použije-li kvalifikovaný poskytovatel daný souhlas pro výdej atributů (služba *TR_IV_SUBJEKT_VYDEJ_UDAJU*), má po krátkou dobu

možnost tento jednorázový souhlas použít znovu. Doba platnosti jednorázového souhlasu se tak může měnit.

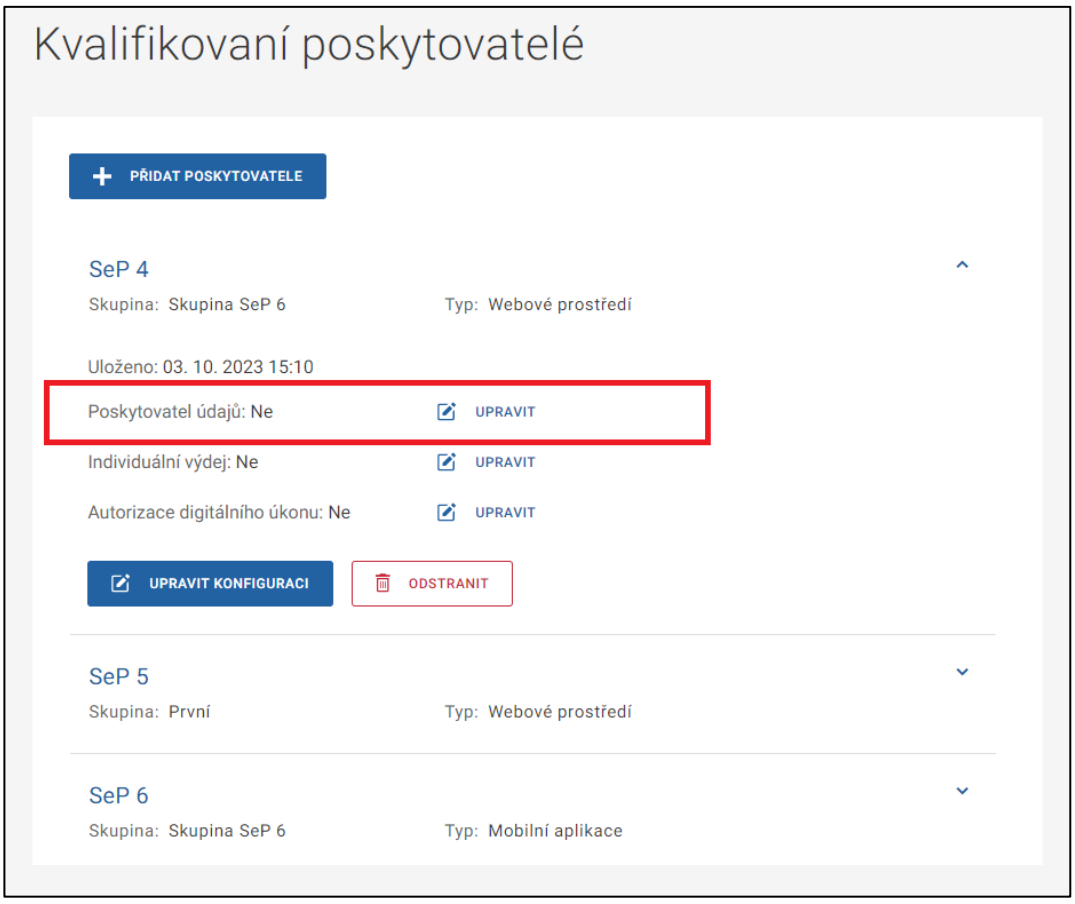
Souhlasy udělené v rámci individuálního výdeje jsou odlišné od souhlasů s výdejem údajů udělených v rámci autentizace občana. Není tak možné použít souhlasy individuálního výdeje pro výdej v rámci autentizace a opačně.

Služba pro výdej požadovaných údajů
Ve chvíli, kdy má kvalifikovaný poskytovatel zajištěn souhlas/y s výdejem požadovaných údajů, volá službu *TR_IV_SUBJEKT_VYDEJ_UDAJU* pro výdej údajů v rámci individuálního výdeje. V rámci žádosti uvádí identifikátory požadovaných údajů a k nim přiřadí identifikátory příslušných souhlasů. Identifikátor souhlasu musí být uveden u každého požadovaného údaje. Na základě korektního požadavku se kvalifikovanému poskytovateli vrátí tyto údaje, pokud jsou ve zdrojích dat dostupné. Např. soukromoprávní poskytovatel údajů totiž nemusí mít daného občana ve své evidenci.

10. Poskytovatel údajů

Každého kvalifikovaného poskytovatele je zároveň možné nastavit do role soukromoprávního poskytovatele údajů. V seznamu konfigurací kvalifikovaných poskytovatelů vyberete kvalifikovaného poskytovatele, kterého chcete nastavit právě do role poskytovatele údajů a výběr potvrdíte kliknutím na tlačítko „Nastavení poskytovatele údajů“.

Technické popisy služeb a rozhraní z této kapitoly jsou dostupné v samostatných dokumentech na úložišti vývojářské dokumentace.



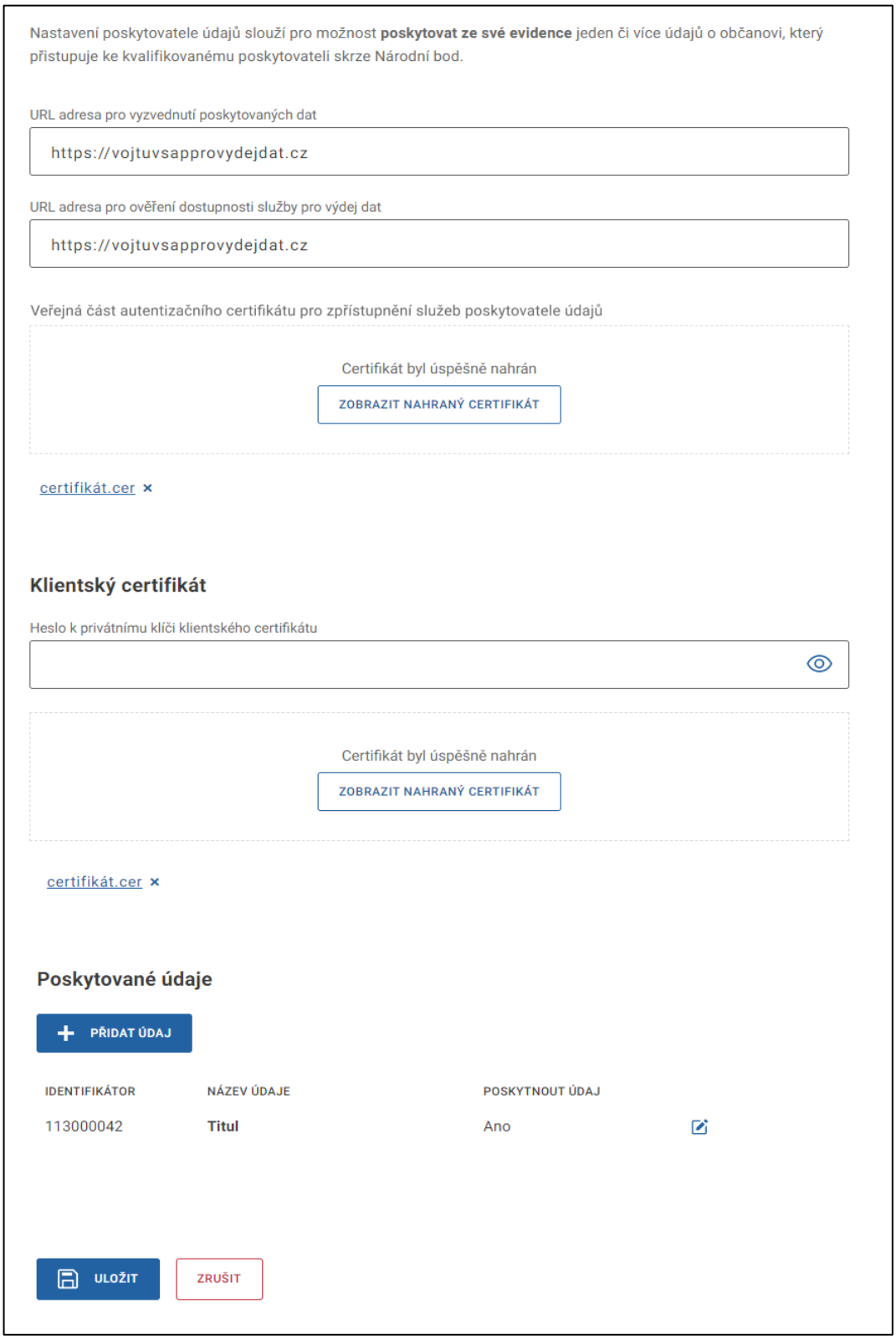
Obrázek 26 - Volba nastavení poskytovatele údajů

10.1. Nastavení URL a certifikátů

Nastavení poskytovatele údajů slouží pro možnost poskytovat ze své evidence jeden či více údajů o občanovi, který přistupuje ke kvalifikovanému poskytovateli skrze národní bod. Jste-li kvalifikovaným poskytovatelem a chcete poskytovat některý z vlastních údajů o osobách využívajících národní bod jiným kvalifikovaným

poskytovatelům, můžete využít právě tuto možnost. V rámci založení poskytovatele údajů jsou vyžadovány následující informace:

1. URL adresa pro vyzvednutí dat poskytovaných o občanovi musí být unikátní a nesmí být použita u jiného poskytovatele údajů.
2. URL adresa pro ověření dostupnosti služby pro výdej dat na straně poskytovatele musí být unikátní a nesmí být použita u jiného poskytovatele údajů.
3. Načtení veřejné části **autentizačního** certifikátu pro zpřístupnění služeb z pozice poskytovatele údajů provedete z lokálního disku. Tlačítko „Načíst“ zobrazí okno pro zadání cesty, odkud má dojít k načtení certifikátu. Autentizační certifikát musí být podporován národní identitní autoritou a může se jednat o stejný autentizační certifikát jako v případě individuálního výdeje. Totožný autentizační certifikát může být použit pouze v rámci stejného kvalifikovaného poskytovatele.
4. Heslo k privátnímu klíči **klientského** certifikátu, které je potřeba zadat dříve, než vložíte certifikát samotný.
5. Načtení **klientského** certifikátu, kterým bude národní bod volat webové služby poskytovatele údajů, provedete z lokálního disku. Tlačítko „Načíst“ zobrazí okno pro zadání cesty, odkud má dojít k načtení certifikátu. Při zvolení certifikátu je kontrolována správnost zadaného hesla a při kladném výsledku je tento certifikát uložen (po stisknutí tlačítka „Uložit“). Je pouze na rozhodnutí kvalifikovaného poskytovatele, jaký klientský certifikát vloží.



Obrázek 27 - Nastavení poskytovatele údajů

Nastavení poskytovatele údajů dokončíte kliknutím na tlačítko „Uložit“. Jakmile provedete úspěšné nastavení URL adres a certifikátů, zaktivní se tlačítko „Nový údaj“ a můžete začít nastavovat údaje určené k poskytování ostatním kvalifikovaným poskytovatelům.

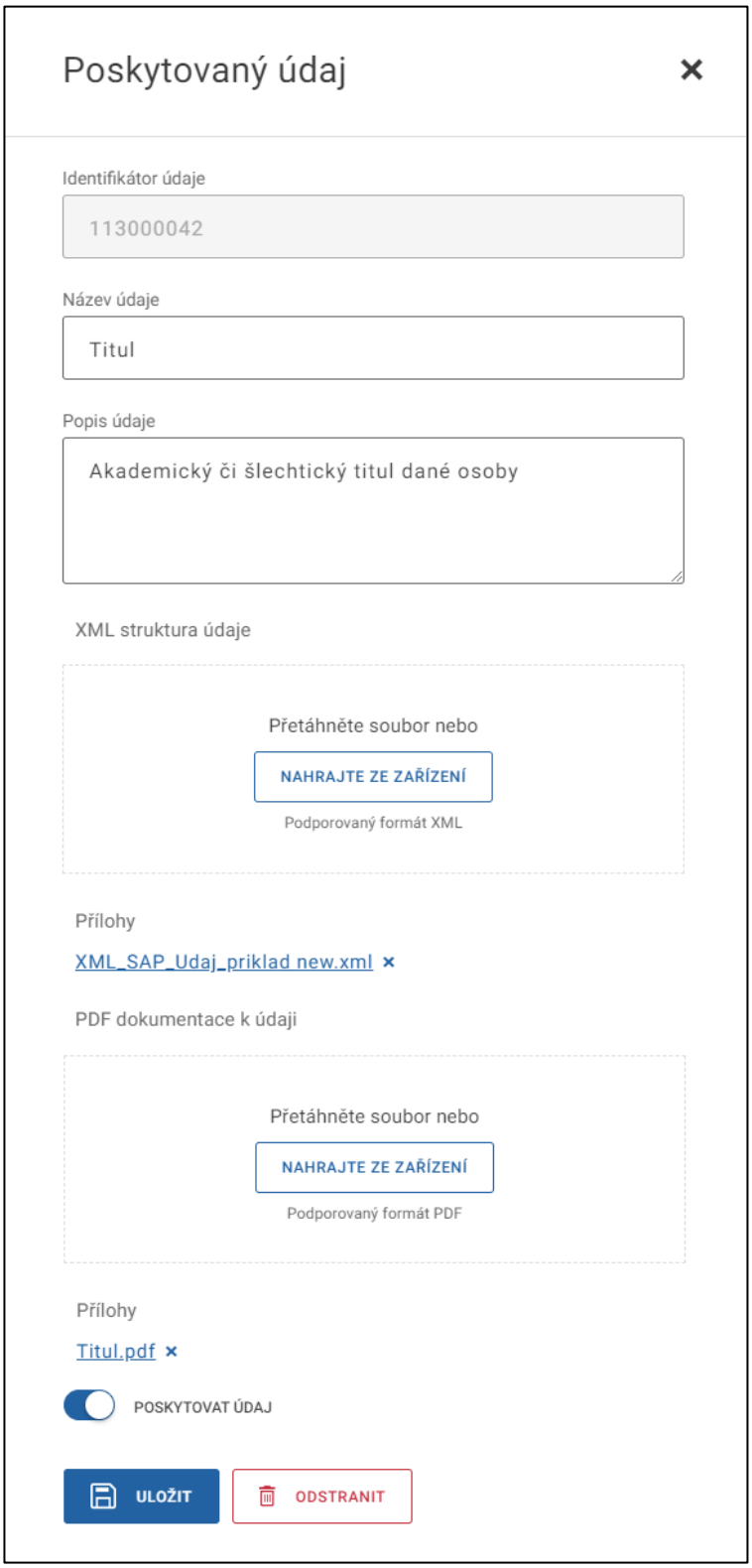
Informace o založení poskytovatele údajů je viditelná v Seznamu konfigurací kvalifikovaných poskytovatelů. Nastavení poskytovatele údajů můžete v případě potřeby editovat nebo prostřednictvím tlačítka „Odstranit poskytovatele údajů“ trvale odebrat.

10.2. Nastavení vydávaných údajů

Nastavení poskytování vybraného údaje započnete stisknutím tlačítka „Nový údaj“. Následně se vám zobrazí detail pro definici nového údaje, v rámci kterého je potřeba vyplnit následující informace:

1. Identifikátor údaje, který na vstupu služby pro získání poskytovaného údaje jednoznačně identifikuje požadovaný údaj. Identifikátor je vygenerován automaticky po úspěšném nastavení poskytovaného údaje.
2. Název údaje, který musí být v rámci daného poskytovatele údajů jedinečný.
3. Stručný popis údaje o občanovi, který budete nabízet.
4. Struktura údaje musí být nahrána v souboru typu XML, jiný typ souboru není podporován. Vzorové XSD pro XML strukturu údaje, které musí být dodrženo, je uvedeno v samostatném dokumentu na úložišti vývojářské dokumentace.
5. Detailnější dokumentace k údaji musí být nahrána v souboru typu PDF, jiný typ souboru není podporován. Velikost souboru nesmí přesáhnout definovanou hranici.
6. Volbou „Poskytovat údaj“ můžete výdej daného údaje povolit či zakázat.

Založení nového údaje potvrdíte tlačítkem „Uložit“. Založený údaj máte možnost kdykoliv upravit či odstranit.



Obrázek 28 - Kroky pro založení nového údaje

10.3. Služby poskytovatele údajů

Mezi národní identitní autoritou a poskytovatelem údajů musí být vystaveny následující služby:

- Služba pro poskytnutí údajů
- Služba pro zjištění aktuální dostupnosti poskytovatele údajů (Probe)
- Služba pro získání informací o souhlasu

Technické popisy těchto služeb a rozhraní jsou dostupné v samostatných dokumentech na úložišti vývojářské dokumentace.

Služba pro poskytnutí údajů
Služba *VydejUdajuService*, kterou vystavuje poskytovatelů údajů, slouží pro předání údaje či údajů do modulu individuálního výdeje v rámci národní identitní autority a dále ke kvalifikovanému poskytovateli, který údaje požadoval. V nastavení poskytovatele údajů je požadována URL adresa, na které poskytovatel údajů umožní vyzvednout požadované údaje. Na vstupu služby jsou identifikátory občana, údaje nebo údajů a identifikátor souhlasu (případně souhlasů). Odpověď poskytovatele údaje je ve formě XML převedeného na Base64 string.

Služba pro zjištění aktuální dostupnosti poskytovatele údajů (Probe)
Služba *ProbeService* je určena pro získání informace o aktuální dostupnosti poskytovatele údajů, aby mohlo uskutečněno vyzvednutí nabízených údajů. V nastavení poskytovatele údajů je požadována URL adresa, na které vystaví tuto službu. V rámci služby Probe je nutné informovat o plánovaných odstávkách poskytovatele údajů. Vystavenou službu bude národní identitní autorita volat v pravidelných intervalech.

Služba pro získání informací o souhlasu
Služba TR_IV_SAP_INFO_O_SOUHLASU, kterou vystavuje národní identitní autorita, je určena pro získání detailnějších informací o souhlasu pro výdej údajů. V odpovědi služby jsou k danému souhlasu uvedeny následující informace:

- typ souhlasu (trvalý/jednorázový),
- datum a čas udělení souhlasu,
- datum a čas ukončení souhlasu (byl-li již ukončen),
- název kvalifikovaného poskytovatele, pro kterého byl daný souhlas udělen,
- údaje, pro které byl souhlas udělen (uvedeny jsou pouze údaje daného poskytovatele údajů).

11. Přihlašování mobilních aplikací

Mechanismus (tzv. pasivní federace), který provede přesměrování z webových stránek kvalifikovaného poskytovatele na výběr poskytovatele ověření, následné přesměrování na stránku poskytovatele ověření, kde občan zadá své přihlašovací údaje a po přihlášení je přesměrován zpět na NIA pro udělení souhlasu s výdejem údajů s následným přesměrováním na stránky poskytovatele služeb, není ideální pro přihlašování k mobilním aplikacím. Z tohoto důvodu byl vybudován mechanismu tzv. aktivní federace, kdy mobilní aplikace provede přihlášení aktivně pomocí volání webových služeb bez potřeby prohlížeče a přesměrování. Podporovány jsou protokoly OpenID Connect a OAuth 2.

Po implementaci tohoto zjednodušeného přihlašování pro mobilní aplikace je nutná interakce s uživatelem pouze jednou, a to v rámci registrace dané aplikace vůči NIA, kdy proběhne přihlášení obdobným způsobem jako u pasivní federace. Při každém dalším spuštění aplikace (případně přihlášení do aplikace) se sama aplikace na pozadí ověří vůči národnímu bodu a obdrží požadované atributy, ke kterým má udělen souhlas občana.

11.1. Rozšíření konfigurace

Nejprve je nutné rozšířit již existující konfiguraci kvalifikovaného poskytovatele o níže uvedené body. Možností je také založit kompletní konfiguraci kvalifikovaného poskytovatele a využívat ji pouze pro potřeby aktivní federace. V rámci dané konfigurace kvalifikovaného poskytovatele, ke které se mobilní aplikace váže, je nejprve nutné zvolit checkbox *Využít kvalifikovaného poskytovatele pro přihlašování přes mobilní aplikace*, který je na konci konfiguračního formuláře. Tím dojde k zobrazení další části tohoto formuláře.

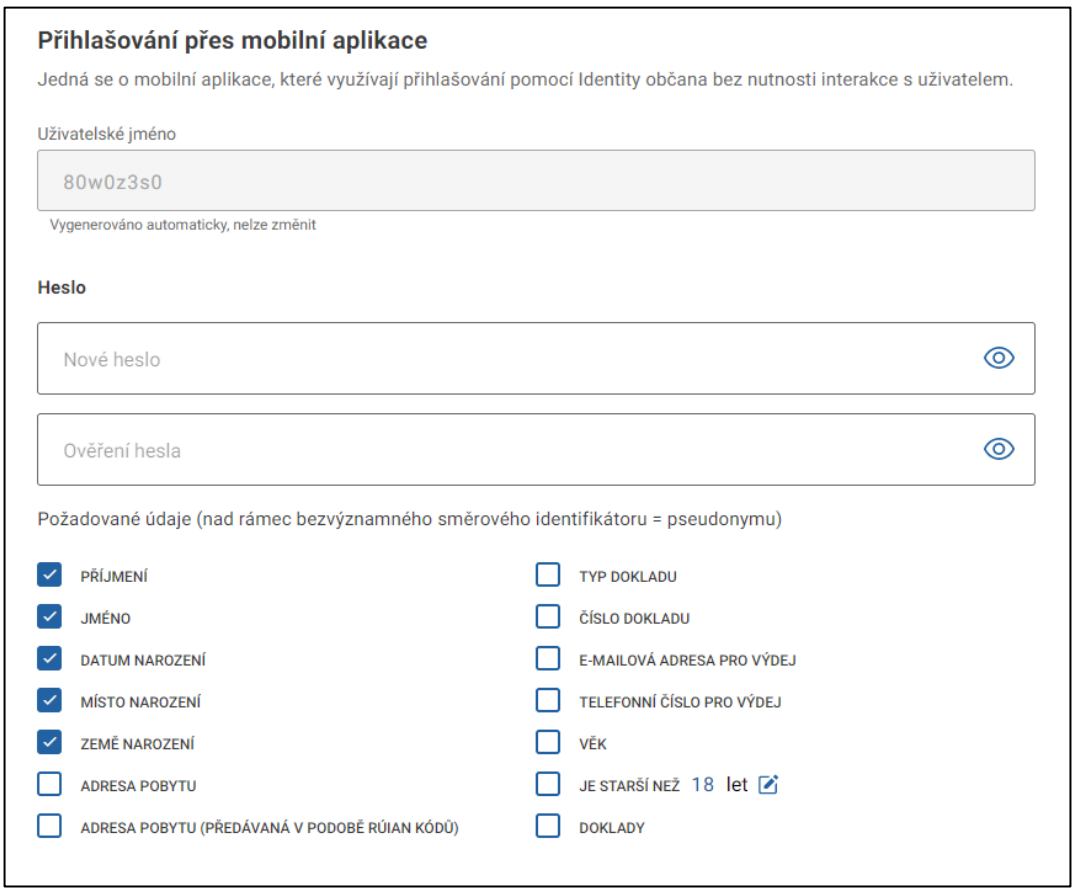
1. Unikátní uživatelské jméno automaticky vygeneruje NIA. Přihlašovací jméno tvoří 8 náhodně generovaných znaků [0-9], [a-z].

2. Heslo musí obsahovat minimálně 17 znaků, a to v kombinaci malých a velkých písmen, číslic a speciálních znaků. Heslo je kontrolováno již v průběhu vyplňování, a tak je ihned viditelné, zda je validní či nikoliv. Pro kontrolu zadejte heslo ještě jednou.

   Kombinace přihlašovacího jména a hesla slouží pro volání NIA kvalifikovaným poskytovatelem. Tato služba je určená pro vyzvednutí vydaných atributů v rámci přihlášení mobilní aplikace.

3. Seznam nabízených údajů s checkboxy určuje, pro jaké údaje bude po občanovi požadován trvalý souhlas s jejich výdejem. Pokud mobilní

aplikace využívá přihlašování přes NIA, je nutné při prvním přihlášení udělit občanem trvalý souhlas a další přihlašování dané mobilní aplikace k NIA včetně výdeje údajů již probíhá na pozadí bez nutnosti zadávání přihlašovacích údajů občanem. Rozsah údajů odpovídá klasické webové autentizaci pro portálová řešení. Bezvýznamový směrový identifikátor je vydáván automaticky.



Obrázek 29 - Rozšíření konfigurace pro přihlašování mobilní aplikace

Při změně rozsahu požadovaných údajů dojde k ukončení všech trvalých souhlasů mobilních aplikací navázaných na danou konfiguraci kvalifikovaného poskytovatele. Při následném použití mobilní aplikace bude nutné znovu provést přihlášení občana přes webový prohlížeč a udělit občanem nový souhlas s výdejem údajů.

11.2. Registrace mobilní aplikace vůči NIA

Po prvním spuštění aplikace anebo v případě, že registrace aplikace již není platná, provede mobilní aplikace přesměrování na NIA. Doporučenou metodou je využití

tzv. embedded browseru. Jedná se o způsob, kdy je prohlížeč zobrazen jako součást mobilní aplikace a neotevírá se samostatné okno prohlížeče. Způsob využití a programování záleží na operačním systému mobilní platformy a na frameworku použitého pro programování mobilní aplikace. Po přesměrování na NIA provede uživatel přihlášení zvolenou přihlašovací metodou, udělí trvalý souhlas s výdejem údajů (jsou-li vyžadovány) a aplikaci bude vrácen access token. Tento access token bude následně použit pro autorizaci volání webové služby při registraci.

Mobilní aplikace volá službu pro registraci mobilního zařízení. NIA vygeneruje přihlašovací jméno pro mobilní aplikaci a zároveň připraví konfigurační parametry pro systém generování OTP (one-time password). Po úspěšném ztotožnění občana odešle NIA v odpovědi uvedené údaje. Mobilní aplikace přijme odpověď a do zabezpečeného úložiště mobilního zařízení uloží registrační údaje, které následně budou sloužit pro přihlašování. Bezprostředně po dokončení registrace je nutné provést přihlášení a tím ověřit úspěšnost registrace. V opačném případě bude registrace zneaktivněna.

Detailnější informace jsou uvedeny v dokumentech na úložišti vývojářské dokumentace.

11.3. Přihlášení mobilní aplikace

Mobilní aplikace vytvoří žádost o přihlášení a zašle ji na definované rozhraní REST NIA pro přihlašování z mobilních aplikací. Rozhraní přijme žádost a vyhledá zařízení v databázi mobilních aplikací a provede další potřebné kontroly. Následně se vytvoří odpověď obsahující Access Token, kterou předá mobilní aplikaci.

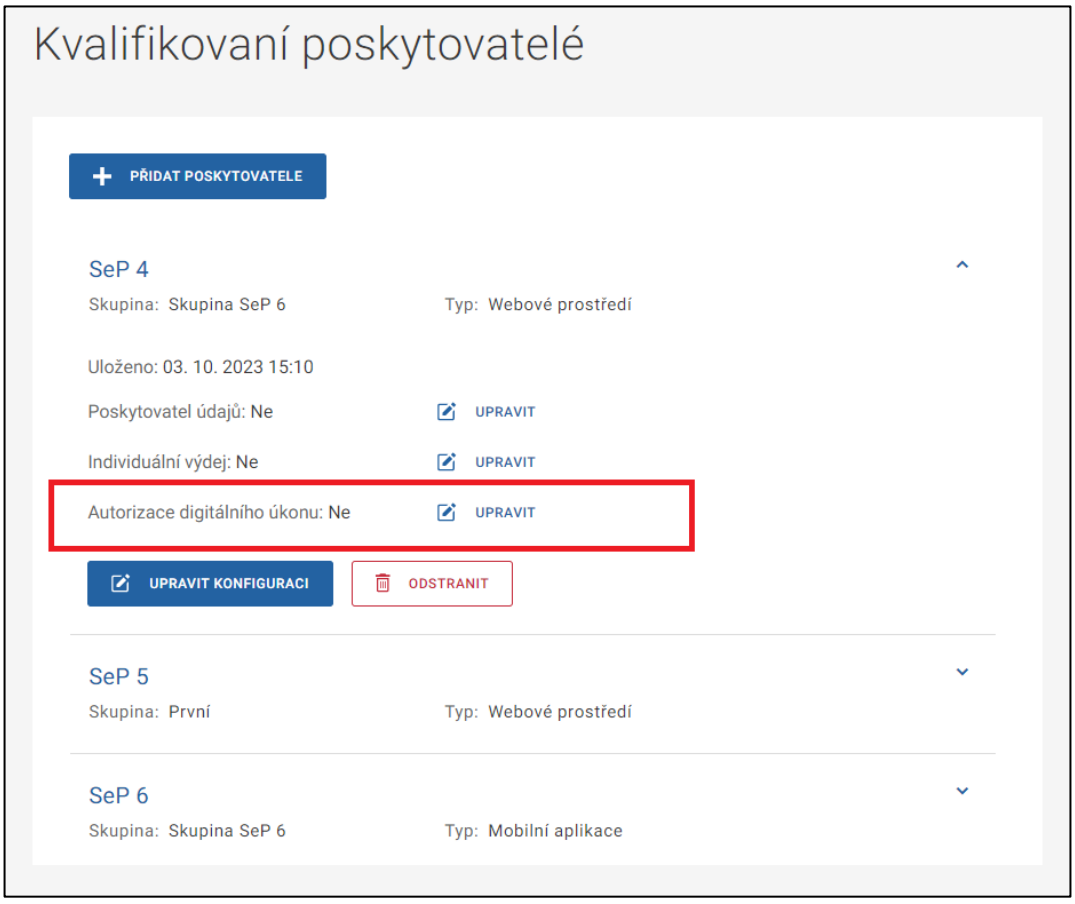
Mobilní aplikace zpracuje odpověď, ze které získá Access Token a zavolá rozhraní kvalifikovaného poskytovatele (protokol je plně v jeho kompetenci) a předá Access token, popř. další informace, které bude vyžadovat tvůrce aplikace.

Kvalifikovaný poskytovatel připraví žádost o vydání tokenu a zavolá službu pro vydání JWT (JSON Web Tokenu) na základě Access Tokenu. Komunikace bude založena na specifikaci OAuth. Při volání musí kvalifikovaný poskytovatel poskytnout své přihlašovací údaje a Access Token. Na základě úspěšných kontrol a transformačních pravidel jsou sesbírány požadované údaje o občanovi. Vytvoří se finální JWT pro kvalifikovaného poskytovatele, který tak obdrží příslušné informace o přihlášeném občanovi

Detailnější informace jsou uvedeny v dokumentech na úložišti vývojářské dokumentace.

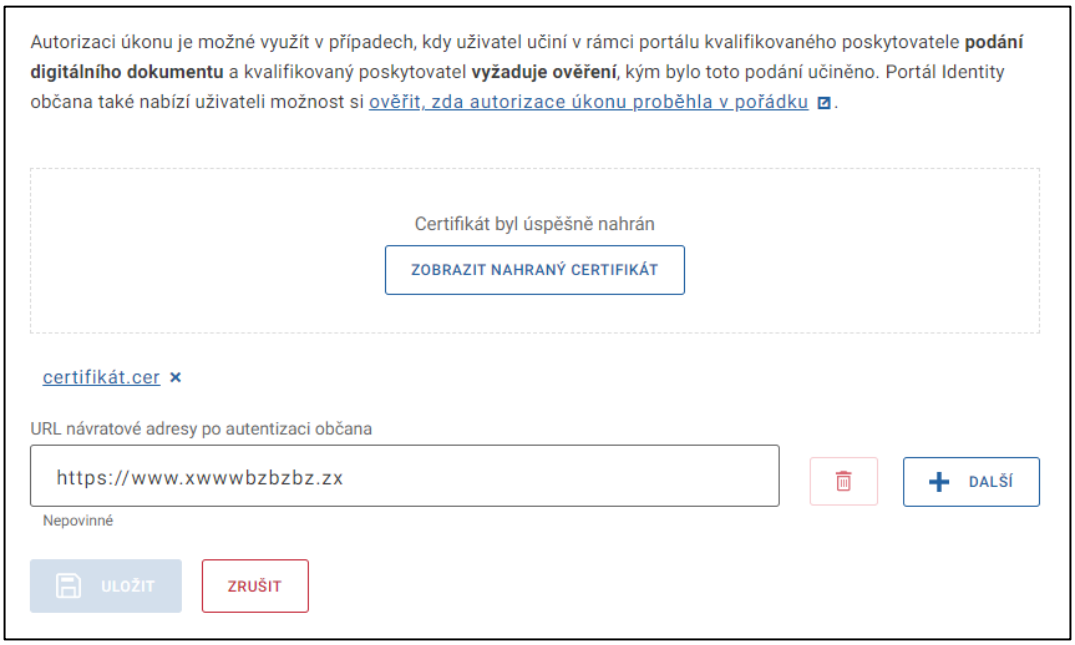
12. Autorizace digitálního úkonu

Tato kapitola popisuje proces autorizace digitálního úkonu. Autorizaci úkonu je možné využít v případech, kdy uživatel učiní v rámci portálu kvalifikovaného poskytovatele podání digitálního dokumentu a kvalifikovaný poskytovatel vyžaduje ověření, kým bylo toto podání učiněno. Portál Národního bodu také nabízí uživateli možnost si ověřit, zda autorizace úkonu proběhla v pořádku.



Obrázek 30 - Volba nastavení autorizace digitálního úkonu

Pro možnost využívat služby pro autorizaci digitálního úkonu, je nutné provést konfiguraci na portálu Národního bodu. V rámci této konfigurace je potřeba nahrát veřejnou část autentizačního certifikátu, případně uvést návratové URL pro případ autorizace přihlášením podavatele přes Identitu občana prostřednictvím jeho identifikačního prostředku (autentizací). Vývojářská dokumentace obsahuje seznam příslušných certifikačních autorit. Všechny služby v rámci autorizace digitálního úkonu je nutné volat s ActAs tokenem přihlášeného občana.



Obrázek 31 - Nastavení autorizace digitálního úkonu

Níže jsou popsány základní obecné informace k procesu autorizace úkonu. Detailnější popisy služeb potřebných pro implementaci jsou k dispozici na úložišti vývojářské dokumentace.

Zjištění možností autorizace digitálního úkonu

Pro ověření digitálního úkonu učiněného uživatelem je potřeba nejprve digitální úkon zaregistrovat a zjistit, jaké možnosti autorizace jsou pro tohoto uživatele k dispozici. K tomu je určena služba TR_ADU_START.

V rámci zaregistrování jsou od kvalifikovaného poskytovatele předávány údaje o přihlášeném občanovi a digitálním úkonu (dokumentu) určenému k autorizaci. Národní bod vrací informaci o tom, jaké způsoby autorizace je možné u daného občana použít. Autorizaci digitálního úkonu je možné provést dvěma způsoby – jedním z nich je zaslání ověřovacího kódu prostřednictvím SMS zprávy na telefonní číslo registrované profilu uživatele v Národním bodu (pokud je takové evidováno), případně prostřednictvím notifikace v aplikaci Mobilního klíče eGovernmentu (pokud má tento prostředek připojen). Druhým způsobem je ověření jeho totožnosti přihlášením přes Identitu občana, kam bude přesměrován po učinění digitálního úkonu na portálu kvalifikovaného poskytovatele.

Autorizace autentizací

1. Kvalifikovaný poskytovatel provede přesměrování (obsahující ID úkonu) na Národní bod, který následně vynutí autentizaci. Autentizace je volána bez žádosti o výdej dat, bez omezení na LoA (volitelně může být požadováno od kvalifikovaného poskytovatele).

2. Pokud se občan úspěšně autentizuje, je přesměrován zpět na stránky kvalifikovaného poskytovatele. Národní bod zároveň provede kontrolu, zda se autentizoval stejný občan, který je přihlášen u kvalifikovaného poskytovatele. Pokud obě přihlášení ukazují na stejného občana, je uložen úspěšný výsledek autorizace, v opačném případě je výsledek autorizace neúspěšný.
3. Kvalifikovaný poskytovatel volá s ID úkonu na vstupu službu TR_ADU_STATUS, která mu vrátí výsledek autorizace.
4. Kvalifikovaný poskytovatel poskytne uživateli potvrzení o výsledku autorizace v podobě dokumentu, jehož maximální povolená velikost je 750 MB.

Autorizace kódem

1. Kvalifikovaný poskytovatel volá službu TR_ADU_SEND_CODE, kde kromě ID úkonu na vstupu dále určuje, zda má odeslání proběhnout prostřednictvím SMS na telefonní číslo uložené v Národním bodu nebo prostřednictvím FCM notifikace na Mobilní klíč.
2. Národní bod vytvoří autorizační kód, který zašle zvolenou formou občanovi. Následně Národní bod vytvoří definovaným způsobem z tohoto kódu hash (SHA-256), který vrátí jako odpověď kvalifikovanému poskytovateli. Zároveň vytvoří druhý hash kódu (SHA-512) pro vlastní kontrolu a oba hash kódy si uloží.
3. Kvalifikovaný poskytovatel umožní občanovi zadat zaslaný autorizační kód. Z tohoto kódu vytvoří definovaným způsobem hash kódu (SHA-256), který porovná s hashem kódu získaným od Národního bodu. Pokud jsou obě hodnoty shodné, vytvoří kvalifikovaný poskytovatel druhý hash kódu (SHA-512) a volá službu TR_ADU_CONFIRM_CODE s ID úkonu a hashem kódu (SHA-512) na vstupu.
4. Národní bod provede porovnání a vrátí kvalifikovanému poskytovateli výsledek. Pokud byl výsledek porovnání kladný, provede národní bod zápis úspěšné autorizace.
5. Kvalifikovaný poskytovatel poskytne uživateli potvrzení o výsledku autorizace v podobě dokumentu, jehož maximální povolená velikost je 750 MB.

13. Seznam obrázků

14. Seznam tabulek