DETAILNÍ TECHNICKÁ SPECIFIKACE DÍLA

Název díla: Rozvoj NIA 2024
Zpracovali: NAKIT – viz RFC 1246
Vedoucí týmu Analýza: [redacted]

Struktura formuláře schválena kým: ***NAKIT***
Datum schválení: 20.11.2023

Schválení obsahu Detailní technická specifikace (zadání)	
Klient / Sponzor Zodpovědný za obsah vyplněný ze strany Žadatele Kapitoly 1, 2, 3	**NAKIT** Zodpovědný za vytvoření kvantity a kvality požadavků na dodávku díla na základě dodaného obsahu Kapitoly 4,5 a 6
[redacted]	**Jméno a pozice pracovníka NAKITu** [redacted]
Odpovědný vedoucí zákazníka	**Odpovědný vedoucí NAKITu**
[redacted]	**Jméno a pozice pracovníka NAKITu** [redacted]
Poznámka	**Architekt**
	Jméno a pozice pracovníka NAKITu [redacted]

Verze a historie dokumentu				
Verze	Datum	Krátký název a popis změny	**Autor**	**Stav** • Draft • Dodán • Schválen
01.	20.10.2023	Vytvoření DTS	NAKIT	Dodán

Obsah

1 Manažerské shrnutí (vytváří DIA)

1.1 Background a cíle

Hlavním cílem této specifikace je:

Co vytvořit?	Vlož (ANO/NE)	Poznámka
Vytvořit zadání pro budoucí projekt	**NE**	
Vytvořit novou aplikaci	**NE**	
Vytvořit novou infrastrukturu	**NE**	
AD HOC - upravit existující aplikaci	**ANO**	
AD HOC - upravit existující infrastrukturu	**NE**	

1.2 Vymezení – proč nevyužít stávající Systém?

Z různých důvodů je třeba vzít v úvahu následující vymezení:

Proč nevyužít stávající systém?	Vlož (ANO/NE)	Poznámka
Požadovaný Systém neexistuje	**NE**	
Systém je zastaralý a nemá podporu	**NE**	
Systém nemá požadovanou funkcionalitu	**ANO**	
Systém je nestabilní a neprovozovatelný	**NE**	

1.3 Obsah díla

Tato přípravná studie bude provedena v částech a bude obsahovat následující aktivity, převážně v pořadí od Part 0 do Part x, k dosažení stanovených cílů:

Part 0: Veřejná zakázka, druh spolupráce

Dodavatele, provozovatele díla budeme vybírat na základě	Vlož (ANO/NE)	Poznámka
Veřejné zakázky – soutěžená klientem	**NE**	
Veřejné zakázky – soutěžená NAKIT	**NE**	
Existujícího smluvního vztahu	**ANO**	

Part 1: Hlavní komponenty s popisem

Název komponenty	IDK	Popis
Aplikace	**App**	**NIA**
Infrastruktura	**Inf**	**N/A**
Integrace	**Int**	**Bez požadavku na integraci nového systému**
Služba	**Slu**	**Nové interní i externí služby**

Part 2: Obrazovky s popisem
Návrhy obrazovek budou řešeny až ve fázi detailní analýzy.

Part 3: Schémata procesů s popisem

ID1 - Kontrola identitního prostředku vůči evidenci v Národním bodu, nastavení jednotlivých IdP (komunikace, konfigurace, řešení problémů)

Při přihlášení přes Národní bod bude kontrolováno, zda je prostředek (kombinace BSI + ID prostředku) zapsán v evidenci Národního bodu. Národní bod musí v rámci autentizace přijímat od IdP kromě BSI nově také ID prostředku, kterým se občan ověřil. Jedná se o ID prostředku, které IdP zapsal do evidence Národního bodu při zápisu nově vydaného prostředku. BSI i ID prostředku již jsou součástí evidence Národního bodu.

Povinnost zasílat ID prostředku bude řešena konfiguračně na úrovni jednotlivých IdP. Tím bude umožněno zapnout u daného IdP povinnost zasílat ID prostředku na vstupu ve chvíli, kdy bude na tuto změnu implementačně připraven.

Pro neúspěšné pokusy bude Národní bod zobrazovat uživatelsky přívětivou informaci, konkrétně:

- v případě, kdy kombinace BSI + ID prostředku nebude v evidenci Národního bodu existovat,
- v případě, že neobdržíme ID prostředku na vstupu, přestože bude jeho povinnost konfiguračně zapnutá.

Neúspěšné pokusy o přihlášení (chybná kombinace BSI + ID prostředku nebo pokus o přihlášení jiným než aktivním prostředkem vyjma Portálu NB) nebudou zaznamenávány do CUL, nicméně takový pokus bude zalogován do databáze. Logována bude identifikace SeP, BSI, ID prostředku, identifikace IdP, důvod nepřihlášení, datum a čas a ProfileID, bude-li v daném případě známo. V případě chybějícího povinného údaje bude požadavek vyhodnocen již na vstupu jako nevalidní, tím pádem ke kontrole kombinace BSI + ID prostředku vůbec nedojde.

Bude upravena služba TR_NOTIFIKACE_IDP pro IdP a to tak, že bude vracet u vybraných záznamů i ID konkrétního prostředku, kterého se notifikace týká (v současné době služba vrací BSI občana). Tam kde to smysl nemá, tj. notifikace se váže na celé IdP, bude nadále vraceno pouze BSI. Konkrétně dojde k rozšíření o ID prostředku u notifikace „Zaznamenání změny v evidenci prostředků“ a „Zaznamenání změny u dokladu“. Ostatní druhy notifikací jsou vázány na občana, tudíž je dostačující již nyní předávané BSI.

NIA ID, MEG a eOP budou upraveny tak, aby při požadavku na autentizaci předávaly do Národního bodu i ID prostředku.

U MEG, NIA ID a evidence mobilních aplikací bude na úrovni uvedených IdP realizována úprava zpracování notifikací ze služby TR_NOTIFIKACE_IDP dle ID prostředku.

ID 3 - Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu

Dojde k rozšíření správy všech prostředků na úrovni Národního bodu o možnost znemožnění a umožnění přihlášení daným prostředkem. Toto se netýká identifikačních prostředků, které vznikají v rámci nevizuálního přihlašování k mobilním aplikacím.

Nastavení znemožnění přihlašování vybraným identifikačním prostředkem bude probíhat na portálu Národního bodu v sekci Přihlašovací prostředky a bude podmíněno ověřenou notifikační e-mailovou adresou nebo ověřeným notifikačním telefonním číslem (nebo oběma kontakty) v Národním bodu. Pokud tuto e-mailovou adresu nebo telefonní číslo občan v Národním bodu nemá, bude vyzván k jejímu vložení a ověření. Pokud bude mít vyplněn pouze jeden notifikační kanál, může mu být doporučeno vyplnění i druhého. Pokud bude mít v Národním bodu vyplněny oba notifikační kanály, bude mu ověřovací kód pro opětovné umožnění přihlašování zaslán na oba kontakty. Prostředkem, u kterého je nastaveno

znemožnění přihlašování k Národnímu bodu, se nebude možné přihlásit ke kvalifikovanému poskytovateli (vyjma speciální „odblokovávací“ stránky). Pokud se uživatel o takovou akci pokusí, zobrazí mu Národní bod příslušnou informaci o dočasném znemožnění přihlašování a jakým způsobem postupovat pro opětovné umožnění přihlašování.

Notifikační e-mailovou adresu nebo telefonní číslo nebude možné smazat, pokud bude existovat prostředek, u kterého je nastaveno znemožnění přihlášení přes Národní bod. To platí i v případě, bude-li začátek znemožnění přihlašování nastaven až v budoucnu (popsáno níže). Vždy musí existovat alespoň jeden z uvedených kontaktů. Smazání jednoho ze dvou kontaktů bude umožněno, uživatel však bude upozorněn, že mu tím zůstane pouze jeden kontakt pro zaslání ověřovacího kódu.

Znemožnění přihlašování bude moct uživatel nastavit jak na dobu neurčitou, tak i na určité období (datum od/do). V obou případech bude moct znovu umožnit přihlašování kdykoliv dle popsaných postupů. V případě, že bylo přihlašování znemožněno na určitou dobu (do určitého dne), bude opětovně automaticky umožněno od následujícího dne.

Na Portálu Národního bodu bude umožněno hromadné znemožnění přihlašování všech připojených identifikačních prostředků, kdy uživatel bude moct zvolit, kterých prostředků se má toto hromadné znemožnění přihlašování týkat. Hromadné opětovné umožnění přihlašování bude umožněno na základě zadání jednoho kódu, ale pouze po přihlášení prostředkem, u kterého je přihlašování umožněno (tzn. pokud je znemožněno přihlašování u všech prostředků, musí uživatel nejprve na příslušné stránce umožnit přihlašování u jednoho ze svých prostředků a tím se přihlásit na Portál Národního bodu pro umožnění přihlašování i u ostatních prostředků).

Pokud uživatel znemožnil přihlašování prostřednictvím Národního bodu prostředkem, kterým je k Portálu Národního bodu právě přihlášen, bude následně odhlášen. To platí i v případě hromadného znemožnění přihlašování.

Funkcionalita znemožnění přihlašování a opětovného umožnění bude dostupná jak na Portálu Národního bodu (Přihlašovací prostředky), tak i formou webové služby pro SD DIA. Webová služba pro opětovné umožnění přihlášení určená pro SD DIA bude mít na vstupu identifikaci operátora SD a volitelně telefonní číslo a e-mailovou adresu.

Opětovné umožnění přihlašování jiným prostředkem bude na Portálu Národního bodu možné pouze v případě, že je uživatel přihlášen prostředkem minimálně s LoA stejné úrovně, jako je úroveň (LoA) prostředku, u kterého je znemožněno přihlašování. V případě požadavku na hromadné umožnění přihlašování pak tato funkcionalita bude nabízena pouze u prostředku s LoA stejným nebo nižším, než je LoA přihlášeného prostředku. LoA však nemá vliv na znemožnění přihlašování, tzn. je možné nastavit znemožnění přihlašování u prostředku s vyšším LoA, přestože je uživatel přihlášen s prostředkem s nižším LoA.

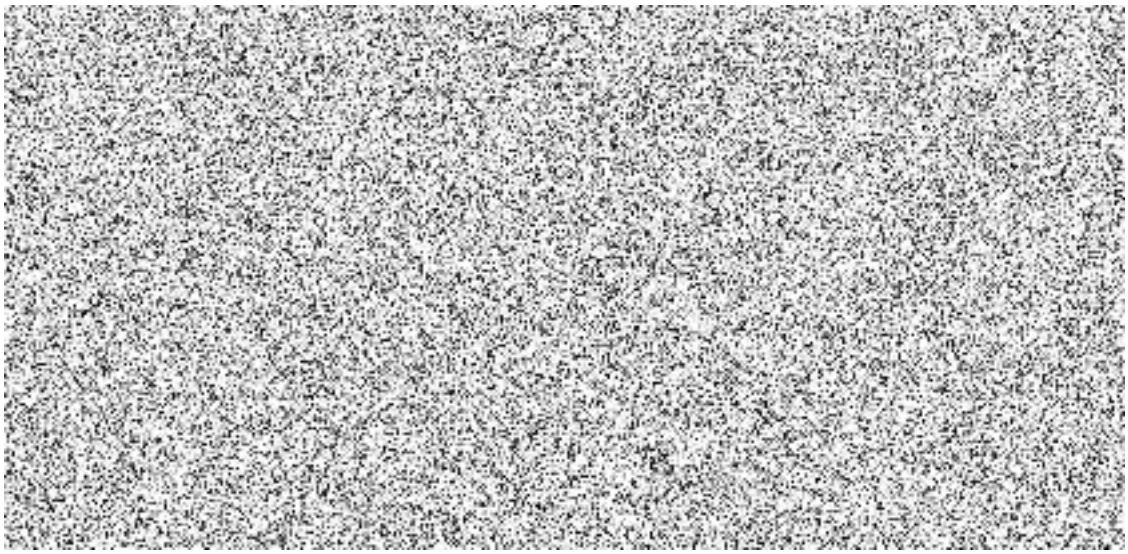
Znovu umožnit přihlašování přes Národní bod bude moct občan nastavit také po přihlášení na příslušnou webovou stránku právě tím prostředkem, u kterého má přihlašování znemožněno a chce ho znovu umožnit. Portál občanovi nabídne novou „odblokovávací“ stránku, žádná jiná funkcionalita nebude pro tyto případy nabízena. Na nové stránce bude občan informován o možnosti znovu umožnit přihlašování, po jehož potvrzení bude vygenerován ověřovací kód a zaslán na evidované notifikační kanály. Po jeho zadání a úspěšném ověření bude přihlašování daným prostředkem k Národnímu bodu opět umožněno.

Ověřovací kód bude vyžadován i v případě, kdy bude přihlášení znovu umožňováno na základě přihlášení jiným identifikační prostředkem k Portálu Národního bodu. Při validaci kódu na straně Národního bodu budou zaznamenávány neúspěšné pokusy (obdržení chybného kódu) a při překročení konfigurovatelného počtu neúspěšných pokusů bude tato funkcionalita pro daného občana na konfigurovatelnou dobu zablokována.

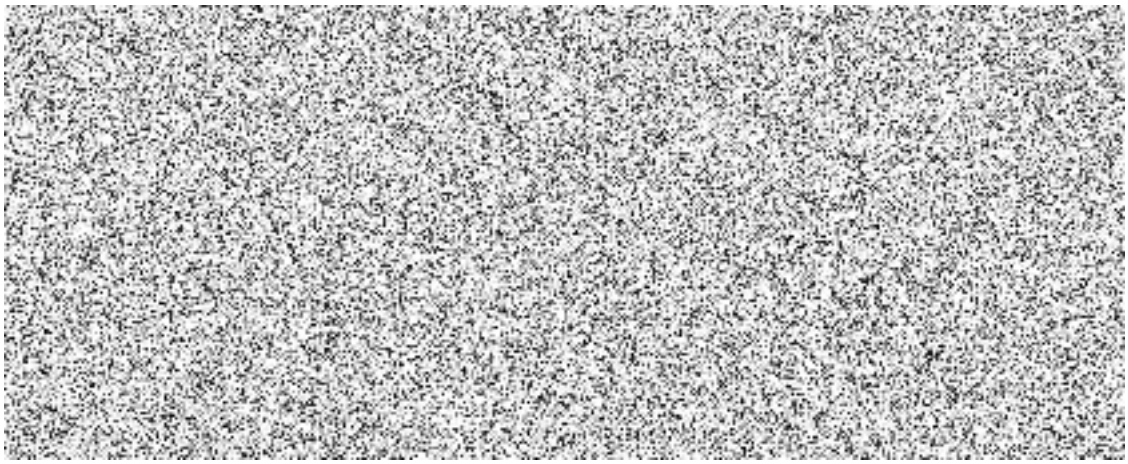
Zakázání se bude propisovat do evidence Národního bodu a bude realizováno formou příznaku u daného záznamu vč. data zápisu příznaku (nemusíme rozšiřovat stavy, pamatovat si předchozí stav atd.). Budou zasílány notifikace při znemožnění a opětovném umožnění přihlašování u jakéhokoliv prostředku, a to na notifikační kanály (telefonní číslo a e-mailovou adresu). Příznak „zakázáno“ bude kontrolován při přihlašování na úrovni Národního bodu – vazba na zapojení evidence Národního bodu do autentizačního procesu (*Kontrola identitního prostředku vůči evidenci v Národním bodu*).

Změna příznaku prostředku se bude zapisovat do CUL jako nový typ záznamu. Zároveň dojde k rozšíření obsahu WS, která vydává údaje z CUL SePům (např. Portálu Národního bodu) a rozšíření Historie Vaší činnosti o tento nový záznam.

Proces znemožnění přihlašování prostředkem na Portálu Národního bodu:



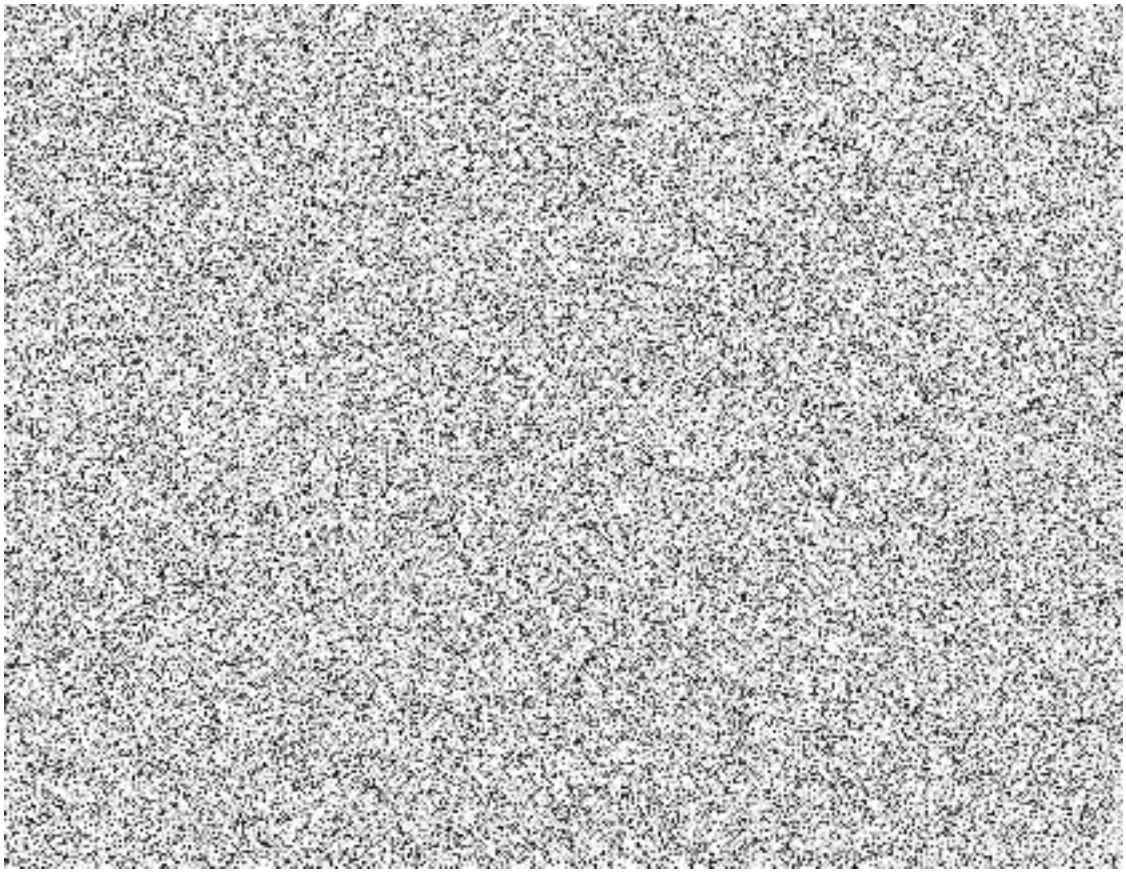
Proces opětovného umožnění přihlašování prostředkem po přihlášení na speciální „odblokovávací“ stránku:



Proces opětovného umožnění přihlašování po přihlášení na Portál Národního bodu, kdy je uživatel přihlášen prostředkem, který nemá znemožněno přihlašování, je prakticky totožný a taktéž vyžaduje ověření prostřednictvím kódu zaslaného na notifikační kontakty. Opětovné umožnění je však možné provést pouze u těch identifikačních prostředků, které mají LoA stejné nebo nižší než prostředek, kterým je uživatel přihlášen.

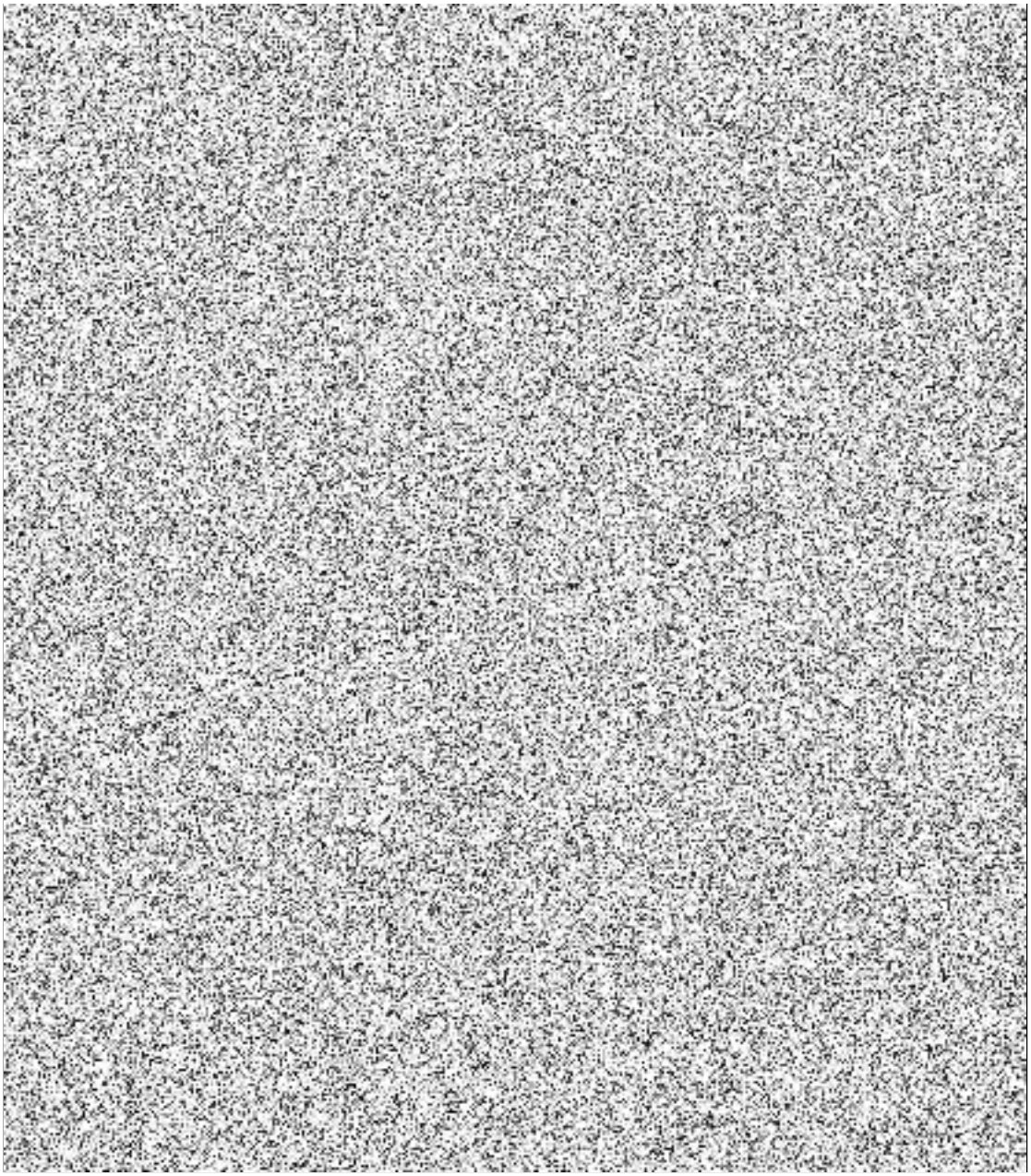
Návrh rozšíření CUL o nový záznam NIA ID

Pozn.: Údaje označené „+“ mohou být vydávány SePům, údaje označené „-“ jsou drženy pouze pro interní účely.



Návrh možného zobrazení logu na Portálu Národního bodu

Záznam o pozastavení platnosti identifikačního prostředku bude obsahovat informaci, jakého prostředku se daná změna týká a kdo je jeho vydavatelem. Dále bude uvedeno, zda došlo k pozastavení možnosti přihlašování nebo zda bylo přihlašování opětovně povoleno a kdo příslušnou změnu provedl, tzn. zda sám uživatel nebo operátor Service Desku DIA.



ID 36 - Úpravy v rámci identity proofingu

Úprava logiky zpracování ZR10 pro využívání i takových údajů, které jsou poskytovány ze zákona

Cílem tohoto požadavku je vytěžení takových údajů obdržených na základě formuláře ZR10, aby mohlo dojít k provolání ztotožnění ideálně s maximálním doporučeným rozsahem údajů, kterými jsou Doklad, Jmeno, Prijmeni, DatumNarozeni, AdresaPobytu. Nyní dochází k volání ztotožnění pouze s Dokladem nebo s menšími kombinacemi údajů bez Dokladu (např. Jmeno, Prijmeni, DatumNarozeni).

Příchozí XML s údaji ze ZR10 bude vytěženo následujícím způsobem:

1. Doklad – Pokud obdržíme atribut *Doklad* (občan sám poskytl údaj), pracujeme s tímto údajem.
2. Jméno – Pokud obdržíme atribut *Jmeno* (občan sám poskytl údaj), pracujeme s tímto údajem. Pokud není v XML obdržen atribut *Jmeno*, použijeme atribut *jmeno_zadatele*, který je předávaný automaticky ze zákona.

3. Příjmení – Pokud obdržíme atribut *Prijmeni* (občan sám poskytl údaj), pracujeme s tímto údajem. Pokud není v XML obdržen atribut *Prijmeni*, použijeme atribut *prijmeni_zadatele*, který je předávaný automaticky ze zákona.
4. Adresa pobytu – Pokud obdržíme atribut *AdresaPobytu* (občan sám poskytl údaj), pracujeme s tímto údajem. Pokud není v XML obdržen atribut *AdresaPobytu*, pak použijeme atribut *misto_pobytu_zadatele,* který je předávaný automaticky ze zákona a převedeme jej na kód adresního místa, se kterým je možné volat ztotožnění.
5. Datum narození – Pokud obdržíme atribut *DatumNarozeni* (občan sám poskytl údaj), pracujeme s tímto údajem. Pokud není v XML obdržen atribut *DatumNarozeni*, použijeme atribut *datum_narozeni_zadatele*, který bude taktéž předávaný automaticky ze zákona, a to pravděpodobně od 1/2024, případně od 7/2024 (aktuálně je novela v legislativním procesu).

Ztotožnění bude následně voláno s maximální možnou kombinací údajů na vstupu. V případě neúspěšného ztotožnění skončí aktivace prostředku okamžitě neúspěchem, tzn. nedojde k volání ztotožnění s dalšími (menšími) kombinacemi.

Úprava Identity proofingu jiným prostředkem pro využití Profile ID namísto dokladu

Při Identity proofingu NIA ID prostřednictvím jiného identifikačního prostředku s alespoň stejným LoA je pro potřeby ztotožnění vyzván občan k udělení souhlasu s výdejem Typu dokladu a Čísla dokladu. Ty jsou plněny pouze hodnotami občanského průkazu nebo povolení k pobytu. Pokud tedy občan nemá ani jeden z těchto dokladů, proces identity proofingu skončí neúspěchem, přestože má občan jiný doklad evidovaný v ROB.

V rámci rozvoje Národního bodu, konkrétně při realizaci Mobilního klíče eGovernmentu, byl proces ztotožnění na úrovni Národního bodu rozšířen o možnost použít na vstupu Profile ID namísto údajů o občanovi vedených v ROB. Nově bychom v rámci identity proofingu nemuseli používat Typ dokladu a Číslo dokladu (ani nový claim Doklady, který vrátí všechny doklady vedené v ROB), ale občana bychom ztotožnili za pomoci Profile ID z „proofingového“ přihlášení, které si v rámci ztotožnění interně přeložíme na AIFO a zavoláme ROB. Na základě této úpravy bychom měli jistotu, že občana ztotožníme a zároveň by se zjednodušil proces identity proofingu, kdy občan nebude muset udělovat souhlas s výdejem údajů.

ID 55 - Historie činností u NIA ID – rozšířené ukládání auditovacích informací

V rámci stávajících procesů NIA ID dojde k zaznamenávání nových typů logů do CUL. Konkrétně se jedná o tyto nové záznamy:

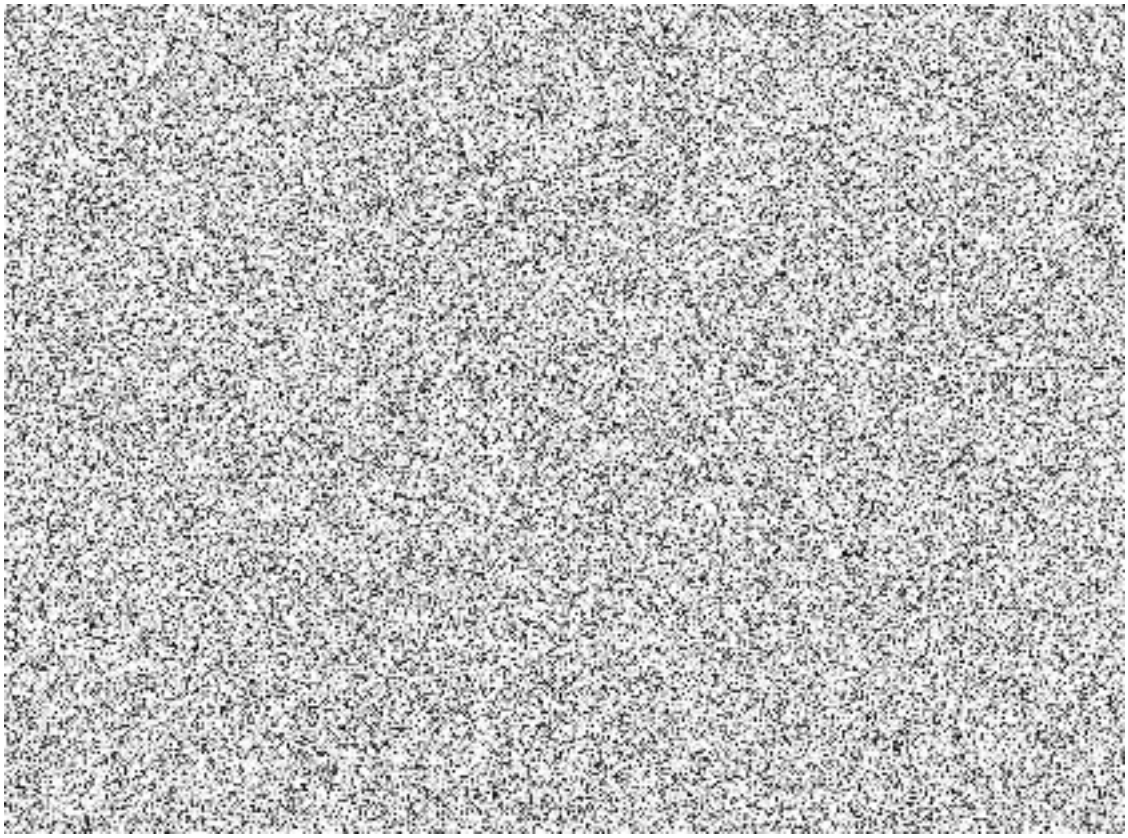
- změna telefonního čísla a e-mailové adresy (po nasazení redesignu již vždy vč. ověření),
- změna hesla/reset zapomenutého hesla,
- změna bezpečnostní otázky a odpovědi na bezpečnostní otázku.

Založení NIA ID a zrušení NIA ID je již nyní zaznamenáváno na úrovni Národního bodu prostřednictvím logu „Zápis Identifikačního prostředku“ („Nový identifikační prostředek“/“Změna stavu prostředku“). Stejně tak schválení podmínek používání je nyní již logováno.

Dojde k rozšíření obsahu WS, která vydává údaje z CUL SePům (např. Portálu Národního bodu) a rozšíření Historie Vaší činnosti o tyto nové záznamy.

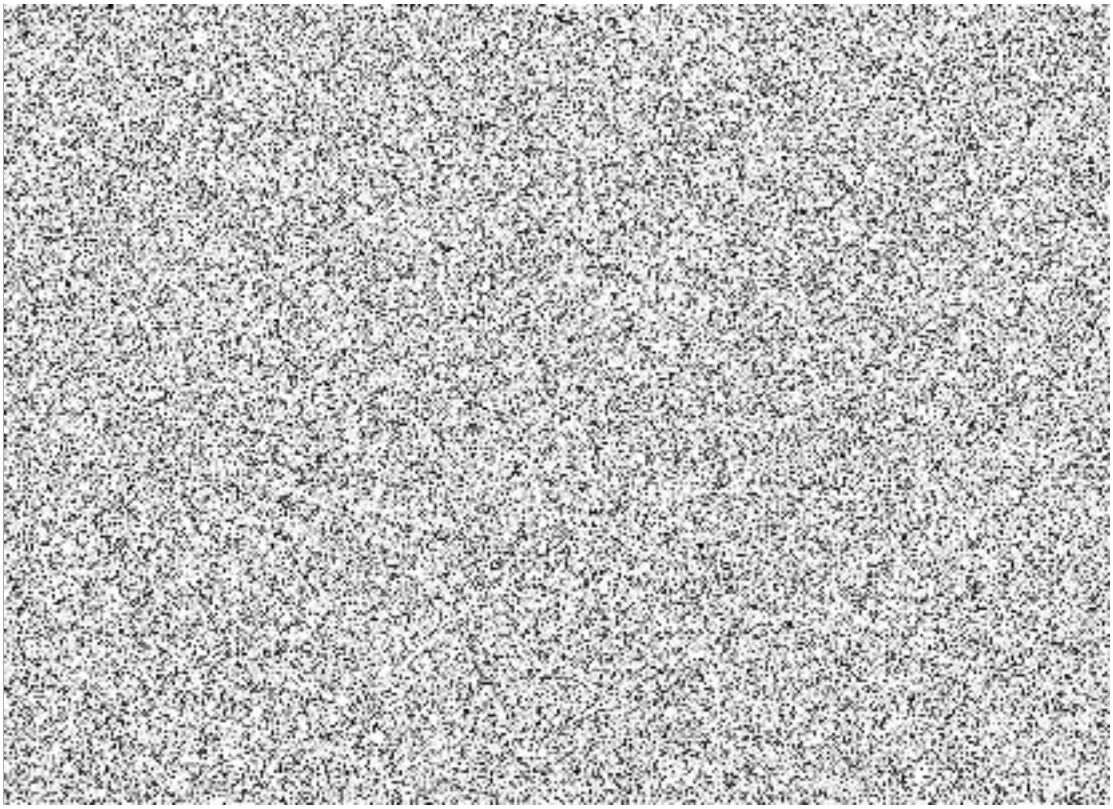
Návrh rozšíření CUL o nové záznamy NIA ID

Pozn.: Údaje označené „+“ mohou být vydávány SePům, údaje označené „-“ jsou drženy pouze pro interní účely.

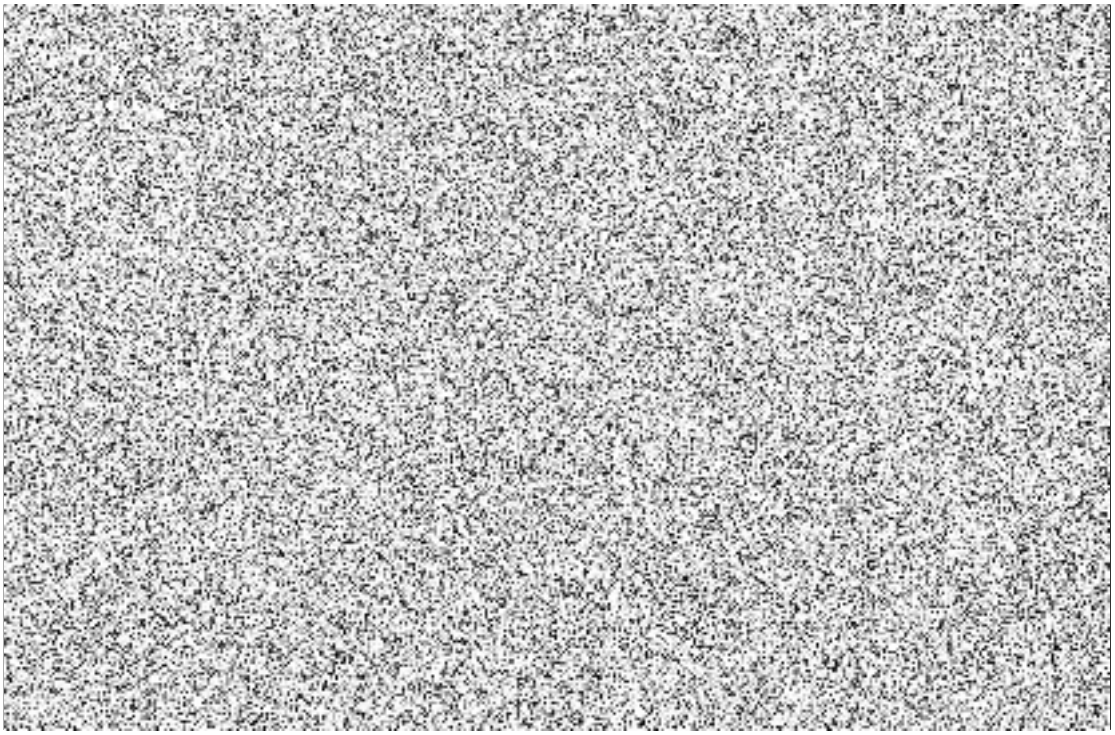


Návrh možného zobrazení logů na Portálu Národního bodu

Změna kontaktního údaje pro identifikační prostředek NIA ID bude rozlišovat, zda došlo ke změně telefonního čísla nebo e-mailové adresy. Pro každou změnu je vytvořen samostatný log. Jelikož může kromě uživatele provést změnu kontaktního údaje taktéž operátor Service Desku DIA prostřednictvím GG Helpdesku, bude log obsahovat informaci právě o tom, kdo danou změnu provedl.

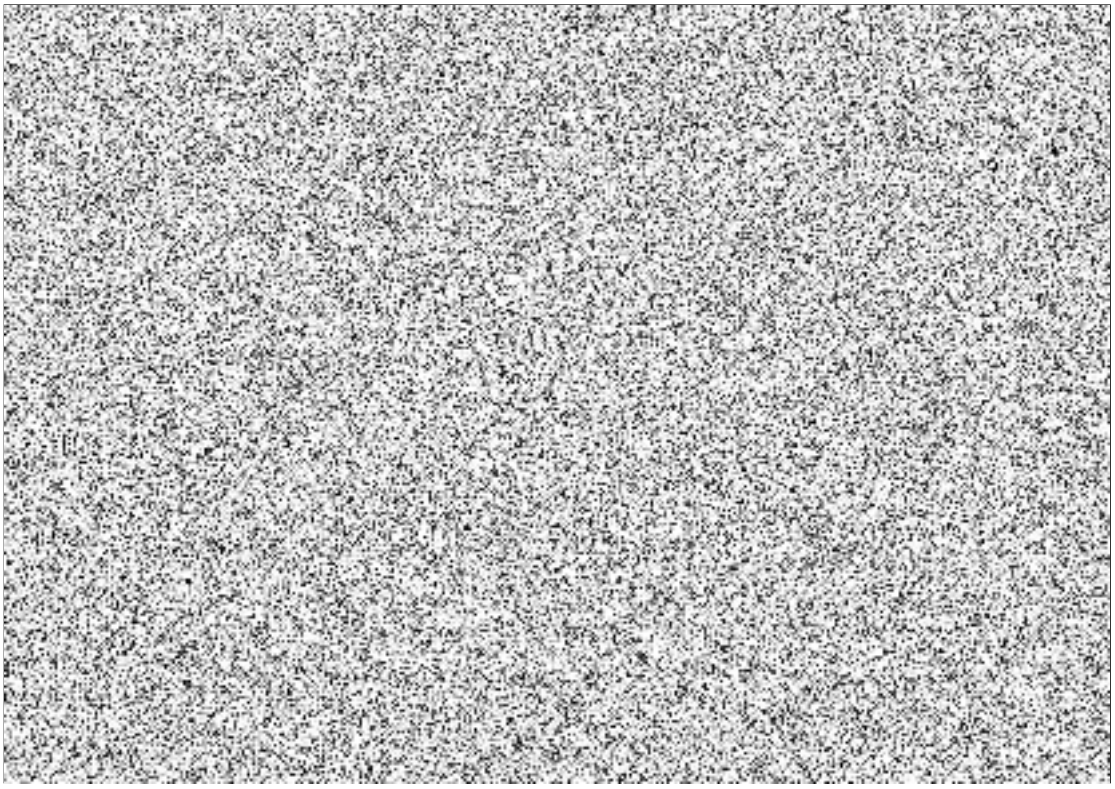


Změna hesla u NIA ID v sobě zahrnuje variantu jak pro změnu hesla, tak pro reset zapomenutého hesla. Změnu hesla provádí vždy sám uživatel, reset hesla může být iniciován uživatelem i operátorem Service Desku DIA prostřednictvím GG Helpdesku.



Záznam o změně bezpečnostní otázky/odpovědi u NIA ID v sobě nese informaci o tom, zda uživatel změnil pouze odpověď na bezpečnostní otázku (bezpečnostní otázka zůstala stejná)

nebo zda došlo ke změně obou údajů, tedy bezpečnostní otázky a odpovědi na bezpečnostní otázku.



ID59 - Využití telefonního čísla a e-mailové adresy uložené v ROB

V rámci sekce Moje údaje na portálu Národního bodu má uživatel nyní možnost použít telefonní číslo a e-mailovou adresu, které má použité u NIA ID (pokud je držitelem NIA ID). Zároveň má možnost kopírovat údaje vyplněné pro výdej SePům i do notifikačních údajů a opačně. Nově bude mít možnost využít telefonní číslo a e-mailovou adresu evidovanou v registru obyvatel. Pokud zvolí tuto možnost, dojde k provolání služby E276 - robCtiAifo2 (nový DuvodUcel) s požadavkem na výdej telefonního čísla a e-mailové adresy. Pokud má uživatel nějaký z kontaktů v registru obyvatel evidován (ať už jeden z nich nebo oba), dojde k jejich výdeji.

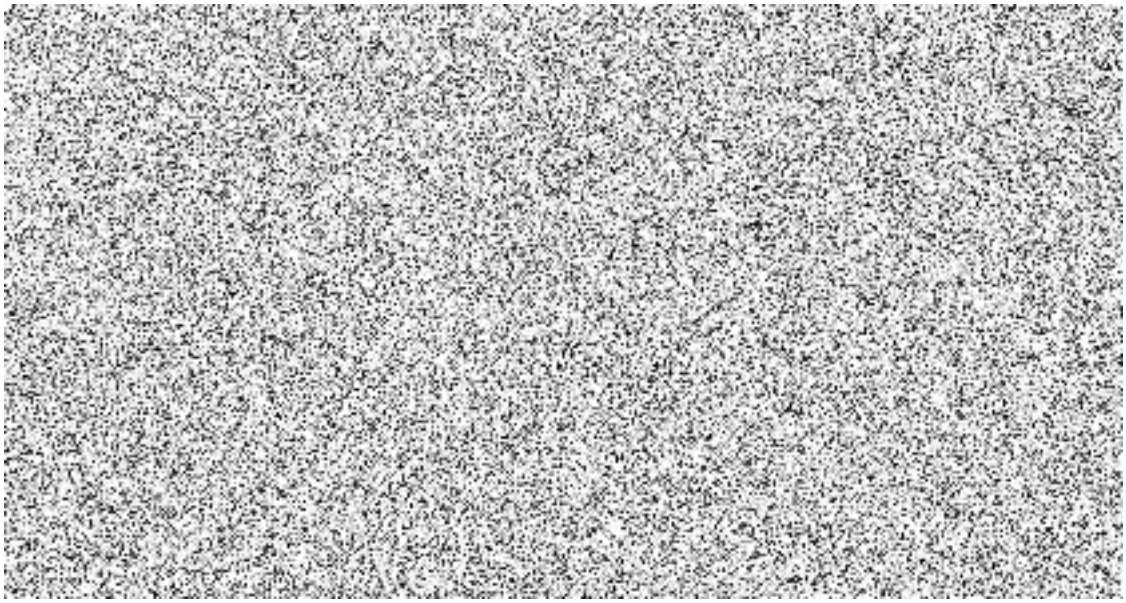
Portál Národního bodu údaje uloží a zároveň nabídne uživateli možnost uložit kontaktní údaje i do druhé sekce, než ze které danou funkcionalitu spouštěl (tzn. pokud zvolil využití údajů z ROB v části „Údaje předávané ostatním portálům“, bude mu nabídnuto jejich využití i do části „Notifikační údaje“.). Údaje převzaté z ROB budou považovány za ověřené.

Národní bod se bude nočními joby doptávat na změnu v ROB nově i pro telefonní číslo a e-mailovou adresy (u těch uživatelů, kteří použili kontaktní údaje právě z ROB). Jakmile dojde ke změně v ROB, provede Národní bod aktualizaci údajů i u sebe. Následně zašle na nový kontakt notifikaci, že došlo k aktualizaci údaje v Národním bodu.

Pokud uživatel údaje dotažené z ROB smaže, neproběhne v případě změny v ROB jejich aktualizace v Národním bodu. Pokud by změna znamenala odebrání údajů v ROB a uživatel by měl zároveň nastaveno dočasné znemožnění přihlašování prostředkem (ID 3), nemůže takováto aktualizace na úrovni Národního bodu u notifikačních kontaktů proběhnout. Uživatel může být o této neaktualizaci notifikován.

Použití údajů z ROB bude logováno do CUL jako standardní přidání/úprava údajů v subjektem definovaných údajích (SDÚ).

Proces získání kontaktních údajů z ROB pro využití v Národním bodu:



ID62 - Služby pro SeP ke zpřístupnění vybraných funkcionalit

Níže uvedené služby č. 1-5 budou vystaveny obecně pro SeP (počítá se využití např. Portálem občana). Služby budou vystaveny na veřejně dostupném API Národního bodu a volání bude ověřeno:

1. pomocí ActAs tokenu, tj. ve jménu přihlášeného občana (občan je u SeP přihlášen prostřednictvím Národního bodu),
2. pomocí podpisu certifikátem (občan může být u SeP přihlášen jakýmkoliv způsobem, případně i nepřihlášen).

Každá služba č. 1-5 bude implementována ve dvou provedeních dle výše popsaných způsobů ověřování.

1. Služba pro získání seznamu připojených identifikačních prostředků

Služba bude na základě identifikace občana vracet seznam všech identifikačních prostředků, které má občan aktuálně připojen k Národnímu bodu a jsou ve stavu "aktivní". Kromě seznamu samotného budou na výstupu např. loga jednotlivých poskytovatelů ověření či datum a čas posledního přihlášení či samotného připojení k Národnímu bodu.

- Vstup:
    - Identifikátor občana (SePP)
- Výstup
    - Názvy připojených aktivních prostředků (vč. identifikátorů) a jejich poskytovatelů
    - Loga
    - Datum a čas posledního přihlášení
    - Datum a čas připojení

2. Služba pro znemožnění přihlašování prostředkem (dočasné zablokování)

Předpoklad: realizace Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu.

Služba bude umožňovat znemožnění přihlašování (dočasné zablokování) identifikačním prostředkem prostřednictvím Národního bodu. Toto znemožnění přihlašování bude možné

realizovat jak pro konkrétní prostředek, tak pro všechny prostředky naráz. Podmínkou úspěšného zpracování služby je existence alespoň jednoho ověřeného notifikačního kontaktu v Národním bodu, v opačném případě nemůže být u identifikačního prostředku zaznamenáno dočasné znemožnění přihlašování. Na základě úspěšného znemožnění přihlášení bude v odpovědi služby obsažena informace, jaký druh kontaktu má občan nastaven jako notifikační (telefon/e-mail/oboje).

- Vstup
    - Identifikátor občana (SePP)
    - Volitelně identifikátor daného prostředku
    - Platnost znemožnění (neomezeně/od-do)
- Výstup
    - Stav zpracování služby
    - Nastavené notifikační kontakty

3. Služba pro umožnění přihlašování prostředkem – zaslání kódu

Předpoklad: realizace Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu.

Jedná se o první ze dvou služeb nutných k opětovnému umožnění využívat identifikační prostředek k přihlašování prostřednictvím Národního bodu. Na základě identifikace občana a identifikace daného prostředku dojde k odeslání zprávy s ověřovacím kódem na notifikační kontakty vedené v Národním bodu. Ověřovací kód si Národní bod uloží pro ověření správnosti kódu, který mu předá SeP pro umožnění přihlášení prostředku. Identifikace daného prostředku je vyžadována v případě požadavku na umožnění přihlašování u jednoho konkrétního prostředku, v případě hromadného umožnění přihlašování není tento údaj vyžadován. Výstupem služby je pak ID požadavku, které bude požadováno na vstupu navazující služby společně s ověřovacím kódem.

- Vstup
    - Identifikátor občana (SePP)
    - Volitelně identifikátor daného prostředku
    - LoA přihlášeného prostředku
- Výstup
    - ID požadavku

4. Služba pro umožnění přihlašování prostředkem – potvrzení kódem

Předpoklad: realizace - Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu.

Jedná se o druhou (navazující) službu potřebnou k opětovnému umožnění využívat identifikační prostředek k přihlašování prostřednictvím Národního bodu. Na základě ID požadavku z předchozí služby a správného ověřovacího kódu je opětovně umožněno využívat identifikační prostředek/ky pro přihlašování. Výstupem služby je pak pouze informace o tom, zda zpracování služby dopadlo úspěšně, příp. detail v případě neúspěchu.

- Vstup
    - Identifikátor občana (SePP)
    - ID požadavku
    - Ověřovací kód
- Výstup
    - Stav zpracování služby

5. Služba pro odpojení mobilní aplikace

Služba bude umožňovat odpojení mobilní aplikace od Národního bodu. To bude možné provést jak obecně pro danou aplikaci (tzn. odpojuji aplikaci ze všech svých zařízení), tak pouze pro konkrétní instanci aplikace (tzn. odpojuji aplikaci pouze z jednoho zařízení) na základě její identifikace prostřednictvím kombinace ApplicationID a PartitionID.

- Vstup
    - Identifikátor občana (SePP)
    - Identifikace IdP (mobilní aplikace)
    - Volitelně identifikace konkrétní instance aplikace (ApplicationID)
    - Volitelně PartitionID
- Výstup
    - Stav zpracování služby

6. Služba pro odpojení instance mobilní aplikace přímo z aplikace

Služba bude umožňovat odpojení konkrétní instance mobilní aplikace od Národního bodu, a to přímo provoláním příslušné služby z mobilní aplikace. Pokud bude mít tedy uživatel danou aplikaci na více zařízeních, dojde k odpojení pouze z konkrétního zařízení. Na rozdíl od výše popsaných služeb 1-5, které jsou vystaveny na podávacím rozhraní Národního bodu, bude tato služba vystavena na rozhraní pro mobilní aplikace.

- Vstup
    - Identifikace konkrétní instance aplikace (ApplicationID)
    - PartitionID
- Výstup
    - Stav zpracování služby

Výše popsané zadání (Obsah díla) může být na základě výsledků detailní analýzy po odsouhlasení oběma stranami upraveno.

Part 4: Integrace s popisem

Název integrovaného Systému	**Požadavky na integraci (Proč integrovat?)**
Bez požadavku na integraci nového systému	

Part 5: Provoz a servis Systému bude zajišťován dle platné provozní smlouvy DIA vs. NAKIT

Provozní parametry definují provozní požadavky klienta na Systém

Provozní režim	**5 dní v týdnu**	**7 dní v týdnu**	**Poznámka**
	Vlož (ANO/NE)	**Vlož (ANO/NE)**	
Režim provozu Systému		**ANO**	
Bude se vést Provozní deník?		**ANO**	
Bude se pravidelně reportovat?		**ANO**	

Provozní SLA parametry	**5 dní v týdnu**	**7 dní v týdnu**	**Poznámka**
	Vlož (ANO/NE)	**Vlož (ANO/NE)**	
Bude se měřit dostupnost?		**ANO**	
Bude se měřit výkonnost?		**ANO**	

Servisní parametry definují provozní požadavky klienta na zajištění servisních služeb Provozovatelem

Servisní režim	5 dní v týdnu	7 dní v týdnu	Poznámka
	Vlož (ANO/NE)	Vlož (ANO/NE)	
Režim servisu Systému		**ANO**	
Budou se evidovat záznamy o provedení servisu v Provozním deníku?		**ANO**	
Budou se pravidelně reportovat záznamy o provedení servisu?		**ANO**	

Provozní SLA parametry	5 dní v týdnu	7 dní v týdnu	Poznámka
	Vlož (ANO/NE)	Vlož (ANO/NE)	
Budou se vyhodnocovat dosažené SLA parametry pro incidenty?		**ANO**	
Budou se vyhodnocovat dosažené SLA parametry pro změny?		**ANO**	

1.4 Odhad kapacit a požadované termíny dodávky

Odhad nákladů:	Náklady vložené na projekt klientem
Počet MD odborů klienta	
CZK – subdodávka klienta	-
Požadované termíny	(Od mm. rr - do mm. rr)
Počátek dodávky díla:	TBD
Předání díla:	Do 30.11.2024

2 Rozpočet (vytváří DIA)

Typ rozpočtu	
Odhad rozpočtu	*Do 9 000 000,- Kč bez DPH*
Rozpočet	-
Rámec řešení	-
Schvalovatel rozpočtu	
Jméno a pozice	

3 Kontext, souvislosti (vytváří DIA)

3.1 Iniciátor a poskytovatel finančních zdrojů

Kdo / **Co**	Název odboru
Iniciátor dodávky díla	*DIA – OŘPZ*
Schvalující rozpočtu	
Držitel finančních zdrojů (FZ)	
Subdodavatel FZ	

3.2 Popis souvislostí a odůvodnění dodávky díla

Odůvodnění potřeb realizace jednotlivých navrhovaných funkcionalit, jejichž cílem je primárně rozvoj Národního bodu, jsou často rozličná. Rozvojové požadavky by se daly rozdělit do níže uvedených tří skupin dle jejich potřeby a dopadů.

Požadavky mající především bezpečnostní povahu:

- Kontrola identitního prostředku vůči evidenci v Národním bodu
- Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu
- Historie činností u NIA ID – rozšířené ukládání auditovacích informací.

Požadavky řešící zjednodušení činností uživatelům a optimalizaci vybraných procesů:

- Úpravy v rámci identity proofingu
- Využití telefonního čísla a e-mailové adresy uložené v ROB.

Služby pro kvalifikované poskytovatele pro poskytnutí funkcionalit Národního bodu i uživatelům jiných portálů:

- Služby pro SeP ke zpřístupnění vybraných funkcionalit.

3.3 Cíle dodávky díla

Cílem dodávky díla je implementace nových funkcionalit pro rozvoj IS NIA.

3.4 Funkční požadavky a cíle na dodání díla

-- Přehled a rozpad cílů a požadavků --				
IDK[1]	**ID C / FP**	**Funkční požadavky (FP) a cíle (C)**	**Dodá - Klient (A/N)**	**Dodá - NAKIT (A/N)**
	D/001	**Kontrola identitního prostředku vůči evidenci v Národním bodu**	N	A
	D/002	**Rozšíření Připojených identifikačních prostředků o možnost znemožnit a umožnit jejich využívání vůči Národnímu bodu**	N	A
	D/003	**Úpravy v rámci identity proofingu**	N	A
	D/004	**Historie činností u NIA ID – rozšířené ukládání auditovacích informací**	N	A
	D/005	**Využití telefonního čísla a e-mailové adresy uložené v ROB**	N	A
	D/006	**Služby pro SeP ke zpřístupnění vybraných funkcionalit**	N	A

1 Zvoleno v kapitole 1.3

3.5 Povaha příspěvku ICT k realizaci cílů

Bez dalších informací

4 Obsah zadání pro dodávku díla (vytváří NAKIT)

4.1 Úvahy

- Jedná se o další rozvojové aktivity Národního bodu, které mají za cíl především zpřístupnit nové funkcionality občanům a rozšířit tak nabídku služeb pro občany i jejich dostupnost. Jak již bylo výše uvedeno, některé požadované funkcionality mají především bezpečnostní charakter, jiné mají za cíl optimalizovat vybrané procesy a zjednodušit je občanům a vybrané funkcionality obecnějšího charakteru taktéž umožnit využívat nejen na Portálu Národního bodu.
- V rámci realizace požadavků dojde k následujícím aktivitám:
    - úprava dotčených procesů, případů užití a návrhů obrazovek,
    - příprava testovacích scénářů,
    - otestování, nasazení a zaškolení,
    - rozdílové analýzy rizik D/001 až D/006,
    - penetrační testy.
- Na těchto aktivitách se budou podílet pracovníci NAKIT a na vybraných aktivitách i jeho subdodavatelé.

4.2 Předpoklady

- Splnění potřebných součinností ze strany objednatele popsaných v samostatné příloze.
- Předpokladem pro dodání celého Díla v roce 2024 je včasné zahájení prací na výše uvedených funkcionalitách.
- Předpokladem realizace vybraných požadavků je nutná realizace jiných požadavků popsaných v tomto dokumentu. Tyto předpoklady jsou uvedeny v kapitole 1.3 Obsah díla.

4.3 Součást dodávky díla

- Analytické podklady obsahující zpracovanou problematiku Obsahu díla. Rozsah analytických podkladů: nové či aktualizované procesní diagramy, UC diagramy s detailními popisy scénářů, class diagramy, návrhy obrazovek na úrovni drátových modelů, v případě potřeby další doplňující diagramy. Podklady jsou drženy na straně NAKIT.
- UX a UI návrhy frontendových částí řešení prezentované v nástroji Figma.
- Bezpečnostní politika NIA aktualizovaná na základě provedené rozdílové analýzy rizik s přihlédnutím k požadavkům
    - zákona č. 181/2014 Sb., o kybernetické bezpečnosti
    - a návazné vyhl. č. 82/2018 Sb., o kybernetické bezpečnosti
- Zdrojové kódy
- Úprava provozní dokumentace
- Popisy testovacích scénářů
- Protokoly o provedení testovacích scénářů
- Součástí dodávky díla je dále školení, nasazení a penetrační test.

4.4 Součásti mimo dodávku díla

-

4.5 Přehled výstupů pro dodávku díla

Výstupem výše uvedených činností bude rozšíření a aktualizace Národního bodu o:

- Kontrolu ID prostředku při přihlášení a práci s ID prostředku v dalších potřebných procesech.
- Možnost znemožnění přihlašování (dočasné zablokování) a opět umožnění přihlašování uživatelem samotným u všech prostředků evidovaných v Národním bodu.
- Změnu ve zpracování údajů ze ZR10 a následného volání ztotožnění.
- Změnu ve volání ztotožnění v rámci identity proofingu jiným prostředkem a zjednodušení tohoto procesu.
- Nové záznamy v Centrálním uživatelském logování týkající se činností u NIA ID a rozšíření Historie všech činností na Portálu Identity občana o tyto nové záznamy.
- Možnost využívat v rámci Národního bodu ty kontaktní údaje (telefon a e-mail), které občan zapsal do registru obyvatel.
- Nové služby pro kvalifikované poskytovatele, které umožní získání údajů o evidovaných aktivních prostředcích v Národním bodu, nové služby pro dočasné znemožnění a opětovné umožnění přihlašování zvolenými identifikačními prostředky, nové služby pro odpojení mobilní aplikace spárované s Národním bodem.

4.6 Plánování dodávek

- Kompletní dodávka bude zákazníkovi předána ve 4. kvartálu r. 2024 do 30.11.2024.

5 Důsledky a kritické faktory úspěchu (vytváří NAKIT)

5.1 Důsledky

- Zvýšení bezpečnosti Národního bodu odlišením jednotlivých prostředků stejného poskytovatele ověření při přihlášení, umožněním dočasného znemožnění přihlašování prostředkem, který občan např. nepoužívá, nemůže ho nalézt či došlo k jeho odcizení a zalogování změn na úrovni NIA ID, konkrétně změn údajů potřebných pro přihlášení nebo reset hesla.
- Optimalizace vybraných procesů, která zjednoduší a zrychlí uživateli vybrané kroky v rámci Národního bodu, např. identity proofing na základě přihlášení jiným prostředkem bude využívat ProfileID namísto údajů z ROB, u přihlašování NIA ID bude možné místo opisování ověřovacího SMS kódu ověřit své přihlášení v Mobilním klíči eGovernmentu.
- Na základě zpřístupnění vybraných funkcionalit Národního bodu kvalifikovaným poskytovatelům by mělo dojít ke zvýšení využívání těchto funkcionalit, jelikož budou pro občana dostupné i na dalších místech, jako je např. Portál občana.

5.2 Kritické faktory úspěchu

- Informování kvalifikovaných správců o změnách v rámci přihlašování (“Kontrola identitního prostředku vůči evidenci v Národním bodu”).
- Zakomponování nových funkcionalit z pohledu UX tak, aby byly pro uživatele srozumitelné a snadno použitelné.

6 Další kroky a návrhy (vytváří NAKIT)

6.1 Oblast nákladů

Cenová kalkulace je:

	Cena za NAKIT	Cena 3. strany	Cena celkem
Cena bez DPH	[illegible]	[illegible]	**8 947 799,90 Kč**

6.2 Oblast řízení dodávek díla

Práce NAKITu a jeho subdodavatelů budou řízeny projektovým manažerem NAKITu.

6.3 Harmonogram dodávky díla (milníky)

Po podepsání Dílčí smlouvy bude vytvořen samostatný harmonogram, který bude obsahovat podrobný seznam úkolů a milníků, které se budou v rámci IZ2024 realizovat.

- Do konce roku 2023 dodat upřesnění co bude obsahem IZ2024
- 01/2024 Příprava smlouvy DS č.4
- Začátek 02/2024 podpis nové DS č.4
- 02/2024 vytvoření harmonogramu + zahájení prací
- 03 – 07/2024 realizace vývoje
- 10-11/2024 nasazení do PROD prostředí
- 11/2024 akceptace