

5 - Elektronická identifikace osob pomocí různých prostředků ztotožnění na národní úrovni (identitaobcana.cz, základní registry aj.), využití datových schránek, elektronizace v oblasti spisové služby a dalších podpůrných nástrojů pro rozhodování univerzity

Univerzita Pardubice





Financováno
Evropskou unií
NextGenerationEU



Národní
plán
obnovy



Napojení na ISZR

V průběhu let 2023-24 došlo na ZČU k úspěšnému napojení na ISZR a úspěšnému získání informací o osobách několika vývojářů IS/STAG ze státních základních registrů.

Tento dokument obsahuje návod, jak napojení na ISZR zprovoznit pro každého zákazníka s IS/STAG a jak modul nakonfigurovat.

Primárně je potřeba mít postaven nový server stag-cms.SKOLA.cz napojený na státní síťovou infrastrukturu CMS - [viz návod uvedený zde](#).

Co napojení na ISZR přinese fakultám

Ve stručnosti, co toto napojení přinese studijním oddělením fakult:

- Veškeré evidované osoby (studentů, uchazečů) budou uvnitř IS/STAG vůči státním registrům nalezeny a identifikovány (pokud se to na základě příjmení+jméno+datum narození(+RČ) podaří jednoznačně)
 - Osoby studentů (tabulka OSOBY)
 - Osoby uchazečů převedených (PR_UCHAZECI) a e-příhláškových (PR_UCHAZECI_WWW)
 - Příjezdoví studenti (STUDENTI_PRIJEZDY_OSOBY)
 - Žádosti uchazečů (ZF_ZADOSTI)
- Některé osobní údaje těchto osob budou pravidelně aktualizovány ze státních registrů
 - Pravidelně = 1x denně (typicky v noci)
 - Údaje = jméno, příjmení, adresa trvalého bydliště, adresa datové schránky (stav k 1.5.2024)
- Důsledky pro studijní oddělení:
 - U osob, které byly s ISZR "spojeny" (tj. byly dohledány, identifikovány a jejich změny od státu synchronizujeme), nebude umožněno manuálně změnit ty položky, které získáváme od státu. V případě pokusu o změnu dojde k vypsání konkrétní chybové hlášky.

Příprava a konfigurace na straně zákazníka

Zde vidíte popis toho, co všechno musíte absolvovat ve "státních systémech", abyste vše správně zaregistrovali a získali potřebné identifikátory a certifikáty... popis sepsal Tomáš Kotouč poté, co se mu po dlouhých týdnech experimentů podařilo docílit úspěchu na napojení do ISZR na ZČU. Pokud Vám to podle návodu nepůjde, napište RT:

Abyste mohli v IS/STAG používat napojení na státní systémy (základní registry a Agendové informační systémy), je nutné váš IS/STAG zaregistrovat ve dvou státních informačních systémech: "AIS RPP Působnostní" a "RAZR". Pro svůj IS/STAG (v terminologii státu to bude "AIS" = "Agendový Informační Systém") získáte ID, které bude potřeba při volání příslušných webových služeb.

V obou systémech budete muset u svého AIS uvádět, jakých agend a jejich činnostních rolí se jeho činnost týká. Seznam těchto agend a činnostních rolí se v průběhu času bude jistě měnit, ale nebojte, my vás vždy upozorníme, když bude třeba něco doplnit.

O agendách, ve kterých jako škola figurujete, vás informuje MVČR (možná, že nyní již DIA) datovou schránkou. To, že vám byla přiřazena určitá agenda ale nestačí, váš zástupce školy musí v "AIS RPP Působnostní" provést oznámení o vykonávání působnosti OVM v agendě. Teprve až vám DIA vykonávání agendy schválí, tak ji budete moci přiřadit ke svému AIS.

Pro nahlášení IS/STAG jako svého AIS jako ISVS (Informační Systém Veřejné Správy) použijete nejprve "AIS RPP Působnostní". Tam mimo jiné uvedete i "Agendovost ISVS", tj. vyjmenujete agendy, kterých se váš AIS týká.

Zatím v IS/STAG budeme potřebovat tyto agendy (a činnostní role):

- agendu A3791 „Vysoké školy“, a činnostní role CR73908 (pro studenty) a CR44328 (pro uchazeče)
- agendu A8566 „Právo na digitální služby“ a činnostní roli CR102729
- možná, že pro počáteční ztotožnění současných studentů budeme potřebovat i agendu A9145 „Spisová služba“ a činnostní roli CR83065.

Státní systémy, které budeme volat, nejsou přístupné k veřejného internetu, ale jsou za jakousi státní VPN nazývanou CMS (Centrální Místo Služeb). Popis technického připojení k CMS byl poskytnut jako výstup CRP DEPO 2022. Jakmile Vám "AIS RPP Působnostní přidělí" pro AIS jeho ID, bude potřeba získat certifikát pro připojování k CMS. Ten získáte registrací AIS v RAZR. Opět popsáno ve výstupu projektu CRP DEPO 2022. Získaný certifikát vaši správci laskavě vloží na filesystém serveru stag-cms.SKOLA.cz do /opt/tomcat/PORTAL-data/konfigurace/iszr/ais.pfx. Nezapomeňte akceptaci vaší žádosti v RAZR tlačítkem převzít. V "AIS RPP Působnostní" je třeba u daného AIS přiřadit všechny agendy a činnostní role, které budete potřebovat využívat a to samé je třeba udělat i v RAZR. Teprve po jejich akceptaci ze strany DIA vás stát k údajům pustí.

Máte-li již nakonfigurovaný a běžící IS/STAG modul na lokálním tomcatu, usnadnili jsme Vám získání/obnovení certifikátu takto - je to popsáno v následující kapitole:

Získání a obnova certifikátu pro klientský systém AIS (= IS/STAG)

Pokud již máte IS/STAG nakonfigurovaný a aplikaci spuštěnou (tj. konfigurace co je uvedena v kapitolách níže je již hotova a modul běží, byť si možná stěžuje na to, že nemá platný certifikát a nebo ještě ani není nutné mít zapnutý parametr ISZR_AKTIVNI - pouze nastavte ty ostatní parametry IS/STAG), **můžete** využít toto zjednodušení pro získání/obnovu certifikátu. IS/STAG vám umí předgenerovat soubor s informací pro vygenerování "certificate requestu" a vy tudíž můžete provést následující postup. Výhoda je ta, že private key neopustí daný server. Nicméně - pokud nemáte přístup na server nebo prostě tento způsob využít nechcete, nemusíte, je to pouze možnost. Podstatné je, abyste postup zhruba od bodu 12/13 níže pak relaivovali a aby tedy byl k dispozici správně vyrobený soubor ais.pfx . Postup nemusíte nutně provádět na našem serveru přímo (provádějte kdekoliv jinde, ale pak nám budete ten soubor ais.pfx muset předat nějakou bezpečnou cestou).

Několik zkušeností ze získání certifikátu jinými školami (děkujeme ZČU, OSU):

- v certreq.config musí být položka organizationalUnitName vyplněna takto:
organizationalUnitName = cisloAIS-P/PROD
pro OU tedy 11582-P/PROD kde /PROD je produkční prostředí nebo /TEST pro testovací prostředí.
- Na RAZRu se mi nepodařilo obejít požadavek na test prostředí, které ale nemáme. Takže jsem si vygeneroval 2 žádosti o certifikát jednou s tím /TEST a jednou s tím /PROD a nejdříve jsem podal žádost pro TEST prostředí (stejně názvy serveru, ip adresy jen ta žádost o certifikát pro testovací prostředí).
- Jakmile přijde schválení te žádosti, tak je potřeba ji v RAZR převzít.

- Nasledne jsem podal zadost o produkci, a zase po její akceptaci v RAZRu prevzit.
- Certifikát v RAZRu není spojen s IP adresou. Tzn. při změně/přidání IP adresy AIS není nutné žádat o nový certifikát.
- IP adresa/y do žádosti v RAZR: jde z dokumentu CMS2-12-1 Propojovací bod Subjektu (VFW) - GOV003843, kde je sekce Tabulka 30: Parametry Propojovacího bodu a položka: "PAT pro přístup pro ostatní služby". Na OU máme momentálně u AIS evidovány obě IP adresy jak "PAT pro přístup pro ostatní služby" tak "PAT pro přístup na sdílené služby CMS". Podle osobního komunikace s DIA, může mít jeden AIS až 4 IP adresy, takže nechci řešit, která služba se bude NATovat do které IP adresy. Nemusí se tedy nutně jednat o IP adresu na rozhraní serveru stag-cms.XXX.cz, ale až o nějakou další adresu (pravděpodobně vnější adresu nějakého NAT mechanismu či něčeho podobného).

Jak mají postupovat velké (ne - outsourcované) školy:

Technický postup samotného získání/obnovy certifikátu:

1. Přihlašte se přes ssh na server s aplikací IS/STAG napojenou na CMS.
2. Buďte přihlášení (či se z roota přepněte) na uživatele **tomcat**
3. `cd /opt/tomcat/PORTAL-data/konfigurace`
4. `cp -r iszr_iszr_zal` (záloha adresáře s certifikáty)
5. `mkdir iszr` (vytvoření pokud ještě neexistuje)
6. `cd iszr`
7. `rm *`
8. `wget https://ADRESA_SERVERU/ws/certreq.config`
9. `cat certreq.config` (**zkontrolujte obsah pro jistotu**)
10. `openssl genrsa -aes256 -passout "pass:changeit" -out Private.key 3072` (Generování klíčového páru)
11. `openssl req -new -key Private.key -out My.csr -sha256 -config certreq.config -passin "pass:changeit"` (Vytvoření žádosti o certifikát)
12. Nyní musíte soubor **My.csr** přes státní informační systém RAZR poslat na DIA pro získání certifikátu - to musíte vy, kdo máte přístup do RAZR.
13. Získáte následně soubor **My.txt**, který nahrajete přes např. SCP sem na server do tohoto adresáře a pokračujete:
14. Z webu DIA (zde: <https://crli.szrcr.cz/dia.html>) si stáhněte dva certifikáty a rovnou si z nich postavte soubor s certificate chainem dle následujícího scriptu. Podle toho, zda jste na produkčním či vývojovém serveru si stáhněte příslušnou alternativu (většina zákazníků má typicky pouze produkční prostředí). Tedy:
 1. **Na produkčním:** { `wget -O - https://crli.szrcr.cz/ISZR_CA.pem & wget -O - https://crli.szrcr.cz/RootCA.pem; }` > DIA_chain.pem
 2. **Na testovacím:** { `wget -O - https://crli.szrcr.cz/ISZR_CA_TEST.pem & wget -O - https://crli.szrcr.cz/RootCA_TEST.pem; }` > DIA_chain.pem
15. Spojení certifikátu se soukromým klíčem: `openssl pkcs12 -export -in My.txt -inkey Private.key -out ais.pfx -certfile DIA_chain.pem -passout "pass:changeit" -passin "pass:changeit"`
16. Následně proveďte "tomcat restart"

POZOR, soubor ais.pfx musí být ochráněn heslem, nesmí být hesla (java implementace pak z něj odmítne načíst klienstský certifikát). Doporučené defaultní heslo je "changeit":

Příprava a konfigurace V IS/STAG

Nastavte hodnoty těchto parametrů IS/STAG:

- **ISZR_OVM** - Číslo školy jako organizace OVM - typicky je to IČO školy. (např. pro ZČU je hodnota "49777513").
- **ISZR_AIS** - Číslo IS/STAG jako AIS (agendový inf. systém) jak jej evidují v ISZR. Pod jakým číslem tedy je evidován Váš IS/STAG jako AIS ve státních agendách.

- **ISZR_OSOBA_NAVIC_DNI** - [nepovinné, default=30] - Počet dní, než systém osobu v ISZR odregistruje poté, co osoba přestane být v IS/STAG "živá".
- **ISZR_AKTIVNI** - Tímto parametrem se celé propojení zapíná - buď částečně a nebo kompletně. Možné hodnoty jsou:
 - **N** (nebo nenastaveno) - propojení na ISZR není aktivní, **neprobíhají** žádné pravidelné joby, synchronizace, komunikace s ISZR, přenosy osobních údajů, nejsou hlídány změny položek osobních údajů v tabulkách
 - **A** - propojení na ISZR je kompletně aktivní, probíhají všechny zde popsané procesy, joby, operace, přenosy a synchronizace.
 - (13.6.2024): Do tabulek sa osobními údaji přeneseme z ISZR: Jméno, příjmení, datum narození, pohlaví, rodinný stav, stát občanství, stát a místo narození, rodné příjmení (v IS/STAG nastavujeme pouze pokud se liší od příjmení)
 - **POZOR, aktuálně neaktualizujeme: trvalou adresu, doručovací adresu, datovou schránku. Budeme zákazníky kontaktovat s návrhy řešení.**
 - **C** - propojení na ISZR je aktivní, ale ne zcela kompletně. Probíhá vše jako když je zapnuto kompletně (A), ale neprobíhá přenos osobních údajů získaných z ISZR do tabulek s osobními údaji IS/STAG (tedy do OSOBY, PR_UCHAZECI, ...). Určeno pro postupné nasazení do produkce, viz popis níže.

Následující věc zařídíme my při přípravě implementace, uvádím to zde pro úplnost: V konfiguračním souboru ws-config.properties na serveru stag-cms.SKOLA.cz musí být hodnota nastavena takto:

```
spring.profiles.active = cms,iszr
```

pro zapnutí modulů CMS a ISZR. Pozor, žádné jiné hodnoty v tomto případě na této řádce nesmějí být!

OTESTOVÁNÍ fungování v IS/STAG

Předpokladem pro otestování je tedy Vaše domněnka, že máte správně získaný certifikát pro AIS a ten máte do modulu nakonfigurovaný a modul spuštěný. Modul sám o sobě obsahuje "self-test", který zkouší volání jedné WS ISZR API (zkouší volat službu OrgCtiZmenyAifo s "prázdnými" parametry, jen aby ověřil, že ISZR akceptuje náš certifikát) a publikuje výsledek na endpointu na který koukají monitorovací softwary. Tento self-test dělá vždy pouze 1x po spuštění aplikace při první potřebě) a pak již zobrazuje pouze výsledek toho prvního volání (abychom nevytěžovali a neprovokovali ISZR divnými voláními). Výsledek testu lze zjistit prohlédnutím URL v prohlížeči:

```
https://_SERVER_NAME_/PortalUpdaterClient/monitor?type=ServerState
```

Zmíněný test potřebuje ke svému fungování mít nastavené parametry ISZR_OVM a ISZR_AIS, ale není nutné mít jakkoliv zapnutý parametr ISZR_AKTIVNI - tedy funguje ještě předtím, než to začnete "rozjíždět".

Pokud test vrací OK, můžete přepnout parametr ISZR_AKTIVNI na chvíli na hodnotu C a zkusit dohledání osoby v ISZR: Aktuálně lze propojení vyzkoušet "technicky v TOADu" přímo v databázi IS/STAG. Například pro dohledání osoby v základních registrech podle jména, příjmení a data narození spusťte v TOADu (pod uživatelem s rolí administrátor) takto:

```
select nvl(vyменik.pg_esb.send_xml_to_esb_sync('ISZR', 'VyhledejOsobu',
xmltype('<root><jmeno>JMENO</jmeno><prijmeni>PRIJMENI</prijmeni><datumNarozeni>1980-01-
```

```
30</datumNarozeni></root>') ),  
xmltype('<TEST>CHYBA VRATIL NULL</TEST>')).getStringVal() from dual;
```

JMENO a PRIJMENI si nahradte konkrétními hodnotami (s diakritikou), datum narození doplňte taktéž. Mělo by to vrátit XML s následující strukturou (příklad):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>  
<ImportedOsobniUdaje>  
<admildnoTrvala>24111596</admildnoTrvala>  
<aifo>aajls4jcXvbRjY145Q34SnU=</aifo>  
<datovaSchranka>f5t8111</datovaSchranka>  
<datumNarozeni>1982-00-00</datumNarozeni>  
<jmeno>Lukáš</jmeno>  
<mistoNarozeni>Plzeň</mistoNarozeni>  
<obcanstvi>203</obcanstvi>  
<pohlavi>M</pohlavi>  
<prijmeni>Valenta</prijmeni>  
<rodnePrijmeni>Valenta</rodnePrijmeni>  
<statIdnoNarozeni>203</statIdnoNarozeni>  
<timestamp>1718269920576</timestamp>  
</ImportedOsobniUdaje>
```

Tím ověříte, že celé napojení funguje. Nezapoměňte případně vypnout parametr ISZR_AKTIVNI na hodnotu N, aby se vám v noci už nerozjelo velké ztotožňování, pokud ještě nechcete.

Následné zaintegrovaní do procesů uvnitř IS/STAG je popsáno níže.

POPIS fungování v IS/STAG - detailní technický popis

Zde bude postupně dopsáno, jak přesně napojení na státní registry v IS/STAG funguje, kdy a co se vůči státnímu systému dělá a tak dále. Tato kapitola je "programátorská dokumentace", k nahlédnutí správcům systému, ale berte to prosím primárně tak, že není určena adminům a nebude mít strukturu/formality a nemusí být aktuální. **Tato kapitola je pro zákazníky informativní a bez záruky.**

Evidence toho, jaké vůbec osoby máme vůči státu nějak řešit

Uvnitř systému je několik tabulek evidujících osoby, ty jsou vždy dle kontextu dané tabulky v nějakém stavu co se týče toho, zda jsou "živé / aktuální". Např. již 10 let skončené studium má u sebe osobu, kterou určitě vůči ISZR nechceme řešit. Nad našimi interními tabulkami jsou postavena VIEW, která vybírají ze svých zdrojových tabulek ty záznamy, které jsou dle domluvené logiky v aktuální okamžik "aktivní" a máme je mít vůči ISZR nějak identifikované / zaháčkované. Ta VIEW mají před názvem tabulky prefix **VISZR_**:

- **VISZR_OSOBY** - mají studium S nebo P nebo jakékoliv budoucí studium. A nebo od konce posledního studia uteklo méně než "parametr ISZR_OSOBA_NAVIC_DNI (default 30)" dní a nejsou anonymizovaní.
- **VISZR_PR_UCHAZECI** - mají nějaké aktuální přijímací řízení (parametr PR_KONEC_PRIJIMACIHO_RIZENI nebo 30. září) nebo je ten záznam mladší než 7 dní (abych tam aktuální na chvíli měl) a nejsou anonymizovaní.
- **VISZR_PR_UCHAZECI_WWW** - mají nějaké aktuální přijímací řízení (parametr PR_KONEC_PRIJIMACIHO_RIZENI nebo 30. září) nebo je ten záznam mladší než 7 dní (abych tam aktuální na chvíli měl) a nejsou anonymizovaní.

- **VISZR_STUDENTI_PRIJEZDY_OSOBY** - mají příjezd, který vznikl ne dříve než před "parametr ISZR_OSOBA_NAVIC_DNI (default 30)" dní a nebo je ten záznam mladší než 7 dní (abych tam aktuální na chvíli měl)
- **VISZR_ZF_ZADOSTI** - záznamy, které nejsou starší než parametr ISZR_OSOBA_NAVIC_DNI (default 30)
- **VISZR_EMAIL_KONTO** - záznamy, které nejsou starší než 7 dní. (jen aby nebyly hned po vzniku smazány... pak to převezmou další tabulky)
- **VISZR_VSECHNY_OSOBY - UNION** všech předchozích - rodná čísla filtruje tak, že bere pouze ta, která nejsou pseudorodné kódy (ty mě vůči státu nikdy nezajímají). Jedná se o komplet souhrn osob, které by měly být v ISZR identifikované a "podchycené".

Celé napojení na ISZR je postaveno nad novou tabulkou **ISZR_REGISTR_OSOB**. Tato tabulka obsahuje seznam osob, které by v daný okamžik měly "mít něco společného" s ISZR či jinými registry, obsahuje jednak tyto osoby, jejich aktuální údaje získané od státu, obsahuje i informace o proběhlých ztotožněních (NIA, BankId), informace stažené z ISZR API a obsahuje i "stavy" té osoby - např. stav, který vyžaduje dohledání osoby v ISZR, zaregistrování k notifikacím v ISZR, zrušení notifikací a odebrání osoby a podobně.

Princip fungování je ten, že až na naprosté výjimky (popsané dále) se veškeré "úkoly" pro modul ISZR odehrávají tak, že se nastaví/změní data v této tabulce. Následně dojde k probuzení modulu ISZR na pozadí a ten zjistí, jaké všechny věci má na základě stavu tabulky na práci a postupně je provede.

Primárním klíčem je **ISZRIDNO** - identifikátor osoby z té tabulky. Tento identifikátor byl distribuován do všech našich dalších "tabulek osob" a je-li např. v tabulce OSOBY uveden, tak to znamená, že my s jistotou víme, že "ta osoba v OSOBY je tou osobou v ISZR_REGISTR_OSOB".

Struktura tabulky stručně:

- **ISZRIDNO** - PK
- **AIFO, AIFO_STATIDNO** - AIFO osoby, pokud jej známe. Do budoucna připravena i možnost, že je z jiného státu (aktuálně 203 nebo NULL znamená ČR a nic jiného neumíme)
- **BSI** - BSI osoby, pokud jej známe. Máme-li BSI a nemáme AIFO, modul okamžitě iniciuje konverzi BSI na AIFO přes ISZR a doplňuje údaje o osobě. Samotné BSI přichází pouze z NIA.
- **JMENO, PRIJMENI, RODNE_CISLO, DATUM_NAROZENI, OBCANSTVI_STATIDNO, DATOVA_SCHRANKA, ADMIIDNO_BYDL, ADMIIDNO_PRBY, NAROZENI_STATIDNO, MISTO_NAROZENI, POHLAVI, RODNE_PRIJMENI, RODINNY_STAV** - aktuální údaje osoby zjištěné poslední interakcí s nějakou státní autoritou (BankID, NIA, ISZR API). Obráceně lze použít v případě, že nemáme AIFO, ale známe jméno, příjmení, datum narození, občanství a/nebo rodné číslo - pokud je to vyplněno takto (plus nastaven příznak VYHLEDAT), modul použije ISZR na dohledání osoby (použije jednu ze služeb podle toho, co o osobě známe a zda má české občanství či nikoliv).
- **ISZR_POSLEDNI_VYHLEDANI** - pokud dochází k vyhledávání osoby na straně ISZR (tedy že ještě nemáme AIFO), zde si ukládáme datum a čas posledního pokusu o dohledávání - abychom nehledali donekonečna.
- **ZTOTOZNENI_NIA, ZTOTOZNENI_BANKID, ZTOTOZNENI_ISZR** - V JSON podobě uložená informace o poslední proběhlé interakci s danou autoritou - je tam kdy k tomu došlo a jaké údaje z ní dorazily.
- **ZTOTOZNENO** - datum, kdy byla osoba bezpečně ztotožněna - přes NIA či BankID - tedy víme, že to v tu chvíli byla opravdu ta osoba. Je-li NULL, ztotožněna nebyla.
- **VYHLEDAT** - příznak, zda je třeba danou osobu vyhledat v ISZR - v tom případě je v položkách JMENO, PRIJMENI, RODNE_CISLO, DATUM_NAROZENI, OBCANSTVI_STATIDNO připraveno k vyhledání osoby v ISZR. (příznak je ve formě datumu - určuje okamžik, kdy byl příznak nastaven)
- **ZAREGISTROVANO** - příznak, zda je osoba zaregistrována k příjmu notifikací v ISZR. (příznak je ve formě datumu - určuje okamžik, kdy byla zaregistrována)

- **NOTIFIKOVANO** - příznak, že z ISZR přišla notifikace, že u této osoby se něco změnilo a že si máme stáhnout aktuální data (příznak je ve formě datumu - určuje okamžik, kdy byl příznak nastaven)
- **ODREGISTROVAT** - příznak, zda je třeba osobu odregistrovat od příjmu notifikací v ISZR. (příznak je ve formě datumu - určuje okamžik, kdy byl příznak nastaven)

Jak dochází k udržování obsahu tabulky ISZR_REGISTR_OSOB - o to se stará procedura **PR_ISZR_SPOJENI_OSOB**. Lze ji volat buď bez parametrů - pak provede kompletní občerstvení všech osob (toto se děje 1x denně a je to voláno z jobu v Javě uvnitř modulu ISZR) - a nebo s parametrem s jedním ISZRIDNO - pak procedura zařídí občerstvení pouze daného záznamu (to se používá vždy poté, když dojde ke změně dat dané osoby). Procedura zařizuje následující věci:

- Kopie ISZRIDNO z tabulky EMAIL_KONTO do navázaných tabulek (došlo-li ke ztotožnění uchazeče a podobně, ať se to dostane až do všech navázaných záznamů o osobě)
- Vložení všech osob z **VISZR_VSECHNY_OSOBY** do **ISZR_REGISTR_OSOB**, které tam ještě nejsou a mají tam být - vloží se s příznakem VYHLEDAT a známými osobními údaji, abychom je pak v ISZR hledali.
- Opačný proces - odebrání všech záznamů z **ISZR_REGISTR_OSOB** (starších než 7 dní), které už nejsou v **VISZR_VSECHNY_OSOBY** - jsou-li zaregistrované k notifikování, tak je jen označím k odebrání notifikace. Jsou-li již odregistrovány, smažu je z tabulky.
- Šíříme ISZRIDNO směrem z **ISZR_REGISTR_OSOB** do všech tabulek s osobami uvnitř IS/STAG (OSOBY, PR_UCHAZECI, ...) - hledáme shodu nejprve podle rodného čísla a poté podle kombinace jméno+příjmení+datum narození+občanství. Pokud se nám tedy v registru osob objeví někdo, koho už někde jinde v IS/STAG evidujeme, tak se nám k němu dostane ISZRIDNO. Děje se to ale pouze u "aktivních" záznamů, tj. těch, které nám vrací ta VIEW VISZR_. Na různé "staré" záznamy tedy nesažeme.
- **Tento krok probíhá pouze pokud je parametr ISZR_AKTIVNI nastaven na A:** Šíříme osobní údaje získané z registrů (tedy z **ISZR_REGISTR_OSOB**) do všech tabulek s osobami uvnitř STAGu (OSOBY, PR_UCHAZECI, ...). Jedeme podle ISZRIDNO, z předchozího kroku máme již spojeno vše, co jde. Aktualizujeme pouze ty údaje, které z ISZR známe (ostatní necháváme v tabulkách IS/STAG beze změny). A pozor, u tabulek, které má možnost editovat veřejnost (PR_UCHAZECI_WWW, STUDENTI_PRIJEZDY_OSOBY atd.), se osobní údaje nalévají pouze tehdy, pokud předtím došlo k úspěšnému ztotožnění přihlášení osoby vůči NIA / BankID (tedy aby někdo nemohl předstírat že je někdo jiný a STAG mu nedodal jeho adresu a podobně...). Aktuálně (13.6.2024) aktualizujeme tyto údaje:
 - Jméno, příjmení, datum narození, pohlaví, rodinný stav, stát občanství, stát a místo narození, rodné příjmení (v IS/STAG nastavujeme pouze pokud se liší od příjmení)
 - **POZOR, aktuálně neaktualizujeme: trvalou adresu, doručovací adresu, datovou schránku. Budeme zákazníky kontaktovat s návrhy řešení.**
 - Studenti, kterým je změněn nějaký osobní údaj, obdrží systémovou notifikaci (typ ISZR_UPDATE), kde je jim tento fakt oznámen.

Manipulace s evidovanými osobami - interakce s ISZR atd.

Koncept je tedy ten, že **celý mechanismus nereaguje okamžitě na žádné události v IS/STAG!** Mechanismus umí udržovat stav jako takový a dělá to pravidelně. Volání je řádově na několik desítek vteřin a není tudíž problém to volat jedenkrát i vícekrát denně, bude-li potřeba. Nicméně konkrétní reakci na konkrétní událost ve STAGu lze samozřejmě vynutit velmi snadno, mám na to interně připravené API (například budeme-li chtít okamžitě převádět BSI na AIFO a následně získat údaje, umíme modul na pozadí aktivovat pro konkrétní ISZRIDNO a budeme to mít).

Co konkrétně dělá Java modul ISZR běžící na speciálním serveru napojeném na ISZR - obecně řečeno především plní "příkazy", které dostane na základě stavu dat v tabulce ISZR_REGISTR_OSOB. Konkrétně:

- **Spouští proceduru PR_ISZR_SPOJENI_OSOB** - dle potřeby a dle situace (před akcí, po akci, pro všechny záznamy, pro jeden... prostě zařizuje správné spuštění)

- **U záznamů, které nemají AIFO a mají BSI:** spustí dohledání AIFO dle BSI - služba E226. Po nalezení si zároveň dá za úkol "notifikováno", aby následně přečetl osobní údaje tohoto AIFO.
- **U záznamů, které nemají AIFO a, mají nastaven příznam VYHLEDAT a mají jméno+příjmení a mají (rodné číslo nebo datum narození) a ještě nedošlo k vyhledávání a není to starší než 5 dní:** spustí dohledání AIFO podle kombinace osobních údajů. Podle toho jaké údaje a občanství mám použije jednu ze služeb: E158 (RC), E278 (datum narození), E174 (cizinci). Po dohledání ukládá získané osobní údaje do **ISZR_REGISTR_OSOB**.
 - Při prototypovém nasazení jsme zjistili, že AIS nemá oprávnění na služby E158 a E174, proto byla funkcionality upravena a vyhledáváme výhradně službou E278. V případě, že nelze dohledat jednoznačně podle jméno+příjmení+datum narození a pokud má osoba ve STAGU evidovanou trvalou adresu ve formě adresního místa, jejetě proveden pokus o dohledání i s adresou. To pak typicky již jednoznačně osobu identifikuje.
- **U záznamů, které mají AIFO a nemají ZAREGISTROVANO is not null:** Provede registraci k notifikacím v ISZR k tomuto AIFO - E45.
- **U záznamů, které mají AIFO a mají ODREGISTROVAT is not null:** Provede odregistraci od notifikací v ISZR k tomuto AIFO - E46.
- Jedná-li se o plnou synchronizaci (job, pravidelně), tak **zjištění, zda nás ISZR notifikuje o změnách nějakých AIFO:** Voláno E07 a u AIFO, které nám přijdou nastavení NOTIFIKOVANO na SYSDATE.
- Jedná-li se o plnou synchronizaci (job, pravidelně), tak **zjištění, zda máme nějaká AIFA o kterých si máme stáhnout aktuální data (mají nastaveno NOTIFIKOVANO is not null):** U těchto AIFO zavoláme E277 a načtené osobní údaje uložíme do **ISZR_REGISTR_OSOB**.
- (při plné synchronizaci i na konci pak spouští proceduru **PR_ISZR_SPOJENI_OSOB**, aby se změny distribuovaly do všech tabulek)

Na žádnou z akcí, které dělá ISZR modul na pozadí, žádná aplikace nečeká, akce probíhají na pozadí. Výjimkou je:

- **Kontrola existence rodného čísla v e-přihlášce** - funkcionality (již je implementována, rozjede se se spuštěním ISZR na dané škole), která okamžitě po zadání českého rodného čísla, jména a příjmení provede dohledání této kombinace v ISZR a pokud nenajde, vrátí uchazeči chybu, protože je jistota, že to je špatně. (v případě nedostupnosti ISZR systému - pokud to prostě do 5 vteřin neodpoví tak nebo tak - přihláška blokována není). Zabere to i v případě, že Slovák zadá rodné číslo, o kterém bude tvrdit, že je české...

Ztotožňování osob u NIA, BankId a souvislost s tabulkou ISZR_REGISTR_OSOB

Po vzniku celého zde popsaného modulu bylo lehce přepracováno i již existující napojení na systémy ztotožnění osob - NIA, BankId. Dříve byly ve všech tabulkách osobních údajů připraveny sloupečky, do nichž se ukládaly výsledky ztotožnění jednotlivě do každé tabulky zvlášť. Po nasazení modulu došlo k odebrání těchto sloupeček, místo nich se tam udržuje nově vazba přes ISZRIDNO na tabulku **ISZR_REGISTR_OSOB**, v níž tyto informace jsou centrálně. Protože ale ztotožnění typicky probíhá u uchazečů, kteří jsou v daný okamžik pouze v tabulce EMAIL_KONTO (a nemusí být dokonce ještě ani nikde jinde), muselo dojít k přidání vazby

- Tabulka EMAIL_KONTO.ISZRIDNO na ISZR_REGISTR_OSOB.

Jak tedy probíhá ztotožnění nyní:

- Uživatel je z nějaké naší aplikace (třeba z e-přihlášky) odeslán ke ztotožnění na NIA či BankID, je úspěšně ztotožněn a je vrácen zpět.
- IS/STAG získává příslušné informace z dané autority - BSI v případě NIA či rodné číslo v případě BankID. Plus rovnou další povinné/volitelné osobní údaje.

- IS/STAG zakládá záznam v **ISZR_REGISTR_OSOB** (případně se "nalepí" na již existující a odpovídající záznam) a ukládá tam získané informace. Do příslušných sloupečků ukládá detailní informace o tom, co všechno z dané autority přišlo a kdy. Nastavuje sloupec ZTOTOZNENO na SYSDATE, abychom věděli, že tento člověk byl reálně opravdu ztotožněn (a nikoliv že jsme si ho jen našli přes ISZR)
- Získané ISZRIDNO ukládá do tabulky EMAIL_KONTO k aktuálně přihlášenému uživateli. (z ní se následně při volní procedury PR_ISZR_SPOJENI_OSOB dostává i do dalších tabulek navázaných na toto e-mailové konto)
- E-přihláška si data vezme a připraví uchazeči předvyplněné formuláře tam, kde to jde ... a pokud už je uchazeč uložen, rovnou aktualizuje data v tabulkách PR_UCHAZECI a PR_UCHAZECI_WWW.

Doporučený postup nasazení napojení na ISZR

V okamžiku spuštění produkčního napojení na ISZR dojde k poměrně velké operaci:

- IS/STAG si uvnitř sebe vygeneruje záznamy pro všechny potenciální osoby, které jsou v dané chvíli aktivní - pro představu na ZČU v dubnu 2024 se jednalo o cca 19 000 osob.
- Všechny tyto osoby se pokusí v ISZR (postupně, řízeně) najít, tedy dle jména, příjmení, rodného čísla dohledat jejich AIFO a dotáhnout jejich aktuální údaje, zároveň se registrovat k odběru notifikací o jejich budoucích změnách v ROB.
- A vzápětí by došlo k aktualizaci mnoha a mnoha tisíc osobních údajů evidovaných dosud v IS/STAG ručně - zmíníme především **adresu trvalého bydliště či datovou schránku**.

Aby nedošlo k nečekaným komplikacím právě v důsledku případné změny osobních údajů (sice ukládáme pouze údaje státem evidované a prověřené, ale kdo ví, jaká byla situace dosud a zda nějaká změna prostě nepůsobí nezamýšlené komplikace), připravili jsme možnost provést nasazení postupně:

- Nejprve doporučujeme nastavit parametr **ISZR_AKTIVNI** na hodnotu **C**. Tím se rozjede téměř vše, až na onen "zpětný přenos osobních údajů do základních tabulek osob v IS/STAG".
- STAG si tyto údaje natáhne pouze do tabulky ISZR_REGISTR_OSOB, kde budou "čekat"
- V modulu reportů - portál / IS/STAG / Reporty / uživatelé a konta je pro administrátory připraven report "Osoby s příchozími změnami osobních údajů z ISZR", který si administrátoři spustí a získají seznam toho, "co a komu by se změnilo, z jaké hodnoty na jakou, kdybyste spojení s ISZR spustili kompletně". Plus tento report bude obsahovat seznam osob, které jsou v IS/STAG evidovány, ale u kterých se nepodařilo dohledání v ISZR.
- Vy můžete tyto změny rozeslat například na fakulty či se s nimi nějak vypořádat po svém... uvidíte prostě, co se stane, až uděláte následující bod:
- Parametr **ISZR_AKTIVNI** nastavte na hodnotu **A**. Tím spustíte kompletní funkcionalitu a během příštího běhu příslušného jobu (nejpozději další noc) dojde k přenosu osobních údajů k osobám.

Zkušenosti z prototypového nasazení do provozu na ZČU

- 1.5.2024 nastaven parametr ISZR_AKTIVNI na hodnotu C.
- Vůči ISZR byl proveden pokus o identifikaci celkem 19918 osob (vyhovující kritériím popsaným výše).
- Jednoznačně bylo identifikováno 18903 osob (tj. cca 95%), k těmto osobám jsme získali AIFO.
- U několika osob dojde k opravě jména a příjmení (jen nuance...)
- Aktuálně řešíme, jak přesně budou aktualizovány adresy a datové schránky. Zatím se neaktualizují.



UNIVERZITA
PARDUBICE

Vytvořeno v rámci projektu **C3.Digitalizace činností přímo souvisejících se zajištěním vzdělávací činnosti a administrativních úkonů spojených se studijní agendou**, reg. č. NPO_UPCE_MSMT-16591/2022.

Toto dílo podléhá licenci Creative Commons BY 4.0. Pro zobrazení licenčních podmínek navštivte <https://creativecommons.org/licenses/by-sa/4.0/>.



Financováno
Evropskou unií
NextGenerationEU



Národní
plán
obnovy

MSMT
MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY