Kontrola oprávnění do AIS přes RPP

Verze	Datum	Autor	Poznámka
0.01	4.9.2024	ARICOMA	Vznik
0.02	16.10.2024	ARICOMA	Doplnění pro AISEO
0.03	14.1.2025	ARICOMA/DIA	Doplnění pro AISC

1. Úvod

Oprávněním do AIS se rozumí oprávnění na položky z AISEO, AISC, AISEOP a AISECD.

2. Stávající stav

Kontrola oprávnění probíhá ve stejném režimu pro všechny ZR i pro všechny nastavené AIS. Tento režim je při chybějícím oprávnění zalogovat a volání nepovolit.

Konfiguračně lze ovlivnit to, zda je nebo není konkrétní AIS do kontroly zařazen. Lze tedy do kontroly postupně zahrnovat jednotlivé AISy.

Pro žadatele lze nastavovat výjimky na OVM, Agendu a AIS, toto nastavení se opět aplikuje globálně na všechny ZR a všechny nastavené AIS.

3. Cíl

Zapnutí kontroly oprávnění na položky konkrétního AIS nezávisle na tom, jak je nastavena kontrola oprávnění na ZR a řízení výjimek taktéž pro konkrétní AIS.

4. Řešení

Je nutné provést úpravy ISZR.

4.1 Rozšíření ISZR

Konfigurace režimu ISZR pro chování dle oprávnění RPP pro AIS

Vytvořit samostatné konfigurace režimu pro řízení jednotlivých AIS:

- AISEO – chybějící oprávnění:
  - nevyhodnocovat
  - logovat a povolit
  - logovat a nepovolit
  - nepovolit
- AISC – chybějící oprávnění – viz výše AISEO
- AISEOP – chybějící oprávnění – viz výše AISEO
- AISECD – chybějící oprávnění – viz výše AISEO

Podle nastavení režimu ISZR pro chování dle AIS:

- Nevyhodnocovat – volání JE předáno do AIS. ISZR neloguje.

- Logovat a povolit – volání JE předáno do AIS, v případě chybějících oprávnění je v ISZR zalogováno.
- Logovat a nepovolit – volání NENÍ předáno do AIS, v případě chybějících oprávnění je v ISZR zalogováno.
- Nepovolit – volání NENÍ předáno do AIS. ISZR neloguje.

Výjimky

Bude možné nastavovat výjimky na jednotlivé AIS. Režim vyhodnocení výjimek bude AND pro atributy žadatele Agenda, OVM a Ais.

Jde o změny ISZR, všechno se provádí v konfiguraci ISZR.

Kdo provádí: technicky zřejmě provoz ISZR, na základě čeho: pokynu DIA.

Kdo je zodpovědný za výdej:

- po dobu vyhodnocování: AIS
- po ostrém spuštění: AIS, RPP a ISZR.

AIS je zodpovědný za to, že vydá pouze položky, o které se žádá.

ISZR je zodpovědné za to, že nepovolí volaní AIS v případě, že žadatel požaduje položky, na které nemá oprávnění v RPP.

RPP je zodpovědné za to, že poskytuje data k vyhodnocení oprávnění.

Tzn v evidenci AIS v ISZR budou doplněna nastavení „Výjimka AISEO“, „Výjimka AISEOP“, „Výjimka AISECD“ a „Výjimka AISC“

Obdobně bude přidáno nastavení výjimek pro OVM a Agendu.

Pokud bude při volání aplikována výjimka, bude toto nastavení zalogováno (pro režim ISZR s povoleným logováním).

Vyhodnocení odpovědi AIS

Toto vyhodnocení je relevantní pro nastavení v režimu „logovat a povolit“.

V případě, kdy bude volání předáno do AIS, je možné vyhodnotit odpověď AIS. Do logu budou zahrnuty nekonzistentní stavy, kdy ISZR dle RPP vyhodnotilo oprávnění jinak než AIS a tento stav lze detekovat (viz níže kapitola AIS).

- ISZR by podle RPP volání nepovolilo, AIS nevrátil výsledek, ze kterého lze detekovat nepovolení.
- ISZR by podle RPP volání povolilo, AIS vrátil výsledek, ze kterého lze detekovat nepovolení.

Výstupy z logování

Pokud je ISZR v režimu logování, pak jsou výstupy z logu dostupné pro DIA dosavadním způsobem, logy budou rozšířeny o informace z výsledku vyhodnocení na úrovni AIS.

5. AIS

Níže je popsáno chování AIS v případě pokusu přístup na položku, ke které AIS interně nepovoluje přístup (chování na testovacím prostředí 5.9.2024).

5.1 Chování AISEO

AISEO u služeb V2 nepodporuje předání seznamu údajů. Volání skončí chybou, pouze pokud žadatel nemá žádná oprávnění.

Lze částečně vyhodnotit konzistenci RPP a AIS.

- Lze detekovat stav, kdy v RPP není oprávnění na požadovanou položku (uživatel musí upravit zasílaný SeznamUdaju).
- Lze detekovat stav, kdy podle RPP není žádné oprávnění a přesto AISEO vydá nějaká data (uživatel musí ověřit oprávnění vedená v RPP).
- Lze detekovat stav, kdy podle RPP existuje nějaké oprávnění a přesto AISEO zamítne (DIA musí zajistit prověření, zda jde o chybu v datech RPP nebo o chybu v nastavení AISEO).

Pro detailnější vyhodnocení by bylo nezbytné logovat všechny odpovědi AISEO, v ideálním případě anonymizovaně, a tyto následně vyhodnocovat.

Detailnější vyhodnocování by mělo výkonnostní dopady v průběhu zpracování eGON služby:

- Výpočetní při anonymizaci před uložením logu.
- Kapacitní a výkonnostní při ukládání na úložiště.

Následné vyhodnocení by bylo možné provádět dávkově bez vlivu na provoz ISZR.

Vyhodnocení by spočívalo v ověření, zda se v odpovědi vyskytují pouze elementy odpovídající oprávněním dle RPP (dle mapovací tabulky).

Následné vyhodnocení nemůže detekovat rozdíly mezi případy, kdy není položka z AISEO vydána z důvodu chybějících oprávnění v AISEO a případy, kdy není položka v AISEO evidována a z toho důvodu se vůbec nevydá na výstup.

5.2 AISEOP

AISEOP v případě požadavku na položku, na kterou nevede interní oprávnění vrací CHYBA / SPECIFIKACE V POPISU / Nemate prava na pozadovana data.

Lze vyhodnocovat konzistenci RPP a AISEOP.

5.3 AISECD

AISECD v případě požadavku na položku, na kterou nevede interní oprávnění vrací CHYBA / SPECIFIKACE V POPISU / Nemate prava na pozadovana data.

Lze vyhodnocovat konzistenci RPP a AISECD.

5.4 AISC

AISC v případě požadavku na položku, na kterou nevede interní oprávnění vrací CHYBA / NEPOVOLENY PRISTUP.

Lze vyhodnocovat konzistenci RPP a AISC.