SPRÁVA ZÁKLADNÍCH REGISTRŮ

Síťová konektivita ISZR

Verze 1.16

Dostupnost ISZR

ISZR je umístěn v síti KIVS. ISZR je publikován do KIVS a do Internetu. ISZR je dostupný na následujících adresách:

- Testovací prostředí.
  - Publikační přes Internet (egon-4) https://egon.gov.cz/publikace/
  - Publikační přes KIVS / CMS2 (egon-4) https://pub.egon.cms2.cz/publikace/
  - Editační přes Internet (egon-5) https://edit.egon.gov.cz/editace/
  - Editační přes KIVS / CMS2 (egon-5) https://edit.egon.cms2.cz/editace/
- Produkční prostředí.
  - KIVS / CMS2 (egon-7) https://iszr.cms2.cz/prod
  - Internet (egon-7) https://iszr.gov.cz/prod

Připojení k ISZR

Každý správce AISu si musí **sám** u nějakého operátora zajistit připojení do té sítě, přes kterou chce k ISZR přistupovat, tj. buď připojení do Internetu, nebo přípojení do KIVS (a CMS).

Každý správce nějakého AISu si musí pro připojení jím spravovaných AISů k vnějšímu rozhraní ISZR zajistit minimálně jednu pevnou (tj. ne dynamicky přidělovanou) IP adresu. Maximálně může použít 4 pevné IP adresy.

Správce AISu **musí** v žádosti o připojení AISu k ISZR uvést 1-4 IP adresy, které bude AIS pro komunikaci s ISZR používat. Může jít o libovolnou kombinaci IP adres KIVS a Internet.

SZR zajistí u provozovatele CMS zřízení prostupů na firewallech CMS, umožňujících přístup z uvedených IP adres ke službám ISZR.

ISZR navazuje spojení s AISy ze stejných IP adres, na jakých je ISZR dostupný pro AISy. To dělá v případě asynchronních služeb v aktivním režimu.

Komunikace mezi AIS a ISZR probíhá vždy protokolem https (http over SSL), tedy šifrovaně. To je vynuceno na straně ISZR, ať ISZR vystupuje z hlediska navazování spojení v roli klienta nebo serveru.

IP adresy

Pro komunikaci AIS s ISZR je možné používat pouze adresy IPv4, tj. nelze použít IPv6.

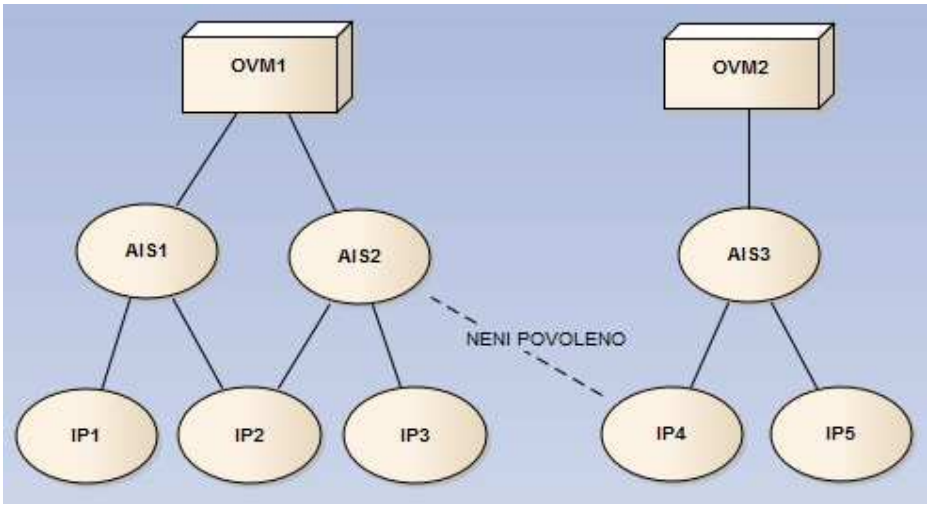
Z Internetu smějí AIS používat pouze IP adresy přidělené poskytovatelům připojení do Internetu pro Českou republiku a pro státy EU. Pokud správce AISu uvede v žádosti o připojení AISu k ISZR adresu přidělenou operátorovi pro jiný stát, bude žádost zamítnuta.

Druhou možností je, že správce AIS uvede v žádosti o připojení AISu k ISZR IP adresu, respektive IP konsolidované adresy CMS.

Správce AISu je odpovědný za to, že AIS používá pro KIVS i Internet pouze takové IP adresy, které je správce oprávněn používat. SZR vyžaduje, aby správci AIS registrovali všechny IP adresy, které AIS používají.

SZR dále požaduje, aby každý správce používal pro AISy, které spravuje, IP adresy, které pro komunikaci s ISZR nesdílí s AISy spravovanými jiným správci. SZR umožní pro určitou IP adresu přístup k ISZR pouze pro prvního správce, který ji uvede v žádosti o připojení AISu k ISZR. Pokud ji uvede v žádosti později nějaký jiný správce, SZR tuto žádost o připojení AISu k ISZR zamítne. SZR neřeší oprávněnost správců AIS používat určité IP adresy.

Pravidlo tedy je, že pro AISy téhož správce je možné pro komunikaci s ISZR používat stejné IP adresy. Pro AISy různých správců musí být použity různé IP adresy. Schématicky je to znázorněno na následujícím obrázku.



Hlavním důvodem tohoto požadavku je, že SZR nedokáže ve většině situací na síťové úrovni identifikovat jednotlivé AISy komunikující na stejné IP adrese. To představuje bezpečnostní riziko typu „není určen odpovědný subjekt“. SZR jako kompromis povolila sdílení IP adres mezi AISy téhož správce, aby subjekt, který spravuje více AISů, vystačil s menším počtem IP adres. Správci AISů ale musí akceptovat fakt, že pokud SZR zakáže přístup k ISZR z nějaké IP adresy, týká se zákaz všech AISů, které tuto adresu používají.

Dalším důvodem požadavku je bezpečnost při vracení odpovědí AISům pomocí asynchronních volání v aktivním režimu. U nich naváže ISZR spojení na IP adresu a TCP port 443. Pokud na tomto portu na příslušné adrese poslouchá více AISů, musí být pečlivě nakonfigurováno, který AIS data dostane. To, že je dostane jiný AIS, než má, představuje bezpečnostní riziko. SZR toto riziko akceptuje pouze za předpokladu, že je jasně určen jeden subjekt, který zodpovídá za všechny AISy, které na IP adrese mohou poslouchat.

Mezi IP adresami uvedenými v žádosti o připojení AISu k ISZR se nesmí vyskytnout privátní IP adresy s výjimkou adres z konsolidovaných rozsahů CMS.

Privátní IP adresy se mohou vyskytovat pouze v privátních sítích. To jsou takové, které nekomunikují s jinými sítěmi, nebo s nimi komunikují po patřičných dohodách provozovatelů o technické konfiguraci obou sítí. Jednou z vlastností těchto adres je, že ty samé adresy se mohou vyskytovat v privátních sítích různých subjektů. To mj. znemožňuje jejich použití ve veřejných sítích typu Internet.

KIVS takové rozsahy privátních IP adres používá. KIVS je neveřejná síť a její správce zajišťuje správu společného adresového prostoru, aby nedocházelo ke kolizím v adresách při vzájemné komunikaci subjektů připojených do KIVS.

V případě, že lokální síť, ve které je AIS umístěn, používá privátní IP adresy, je nutné v žádostech o připojení AISů k ISZR uvádět jednu z následujících adres:

- V případě připojení přes Internet veřejnou IP adresu, kterou přidělil poskytovatel připojení do Internetu.
- V případě připojení přes KIVS tzv. konsolidovanou IP adresu CMS, kterou přidělil provozovatel CMS.

V obou případech musí jít o adresu, která je na vnější straně připojení AIS k Internetu, respektive o konsolidovanou adresu CMS.

Přidělenou konsolidovanou adresu AISu zjistí správce AISu dotazem na provozovatele CMS, kterým je NAKIT, s.p..

SZR nezkoumá dosažitelnost příslušné adresy z hlediska ISZR. Pokud AIS použije nějakou asynchronní eGON službu v aktivním režimu, AIS mu odpověď pošle na zadanou adresu. Příslušný správce AISu (nebo pověřený provozovatel) musí zajistit dosažitelnost IP adresy z Intenetu, respektive z KIVS. A dále musí zajistit, že AIS se na této adrese autentizuje správným certifikátem a je schopen odpověď na asynchronní dotaz přijmout (tj. SSL spojení na příslušnou adresu je obslouženo správným AISem).