



## Síťová konektivita ISZR

Verze 1.6

### Dostupnost ISZR

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

- Testovací prostředí.
  - Publikace přes Internet (egon-4) <https://egon.gov.cz/publikace/>
  - Publikace přes KIVS (egon-4) <https://pub.egon.cms/publikace/>
  - Editační přes Internet (egon-5) <https://edit.egon.gov.cz/editace/>
  - Editační přes KIVS (egon-5) <https://edit.egon.cms/editace/>
- Produkční prostředí.
  - KIVS (egon-7) <https://iszr.cms/prod>
  - Internet (egon-7) <https://iszr.gov.cz/prod>

### Připojení k ISZR

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

Každý OVM v roli 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 pevné IP adresy, které bude AIS pro komunikaci s ISZR používat. Může jít o libovolnou kombinaci IP adres KIVS a Internet. U každé adresy musí uvést, zda bude používána pouze pro synchronní služby a asynchronní služby v pasivním režimu, nebo také pro asynchronní služby v aktivním režimu.

SZR zajistí u provozovatele KIVS zřízení prostupů na jeho firewallech. Pokud jsou pro adresu požadovány asynchronní služby v aktivním režimu, je prostup na firewallu pro příslušnou adresu obousměrný. Pokud ne, je prostup pouze ve směru od AISu k ISZR.

ISZR navazuje spojení s AISy ze stejných IP adres, na jakých je ISZR dostupný pro AISy.

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. 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 adresy KIVS.

Správce AISu (tj. OVM) je odpovědný za to, že AIS používá pro KIVS i Internet pouze takové IP adresy, které je OVM oprávněn používat. Z bezpečnostních a správních důvodů SZR požaduje, aby každý OVM používal pro AISy, které spravuje, IP adresy, které pro komunikaci s ISZR nesdílí s AISy spravovanými jiným OVM. SZR umožní pro určitou IP adresu přístup k ISZR pouze pro první OVM, který ji uvede v žádosti o připojení AISu k ISZR. Pokud ji uvede v žádosti později nějaký jiný OVM,



SZR tuto žádost o připojení AISu k ISZR zamítne. SZR neřeší oprávněnost OVM 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.

AISy pak mohou být používány dalšími OVM, kterým správce povolí přístup k AISu. AIS musí být napsaný tak, že v hlavičkách žádostí o webové služby posílá identifikaci toho OVM, který AIS aktuálně používá.

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

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 údržbu 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 AISu 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 KIVS, kterou přidělil poskytovatel připojení do KIVS.

V obou případech musí jít o adresu, která je na vnější straně připojení AIS k Internetu, respektive ke KIVS. Tj. nemůže jít o adresu, na kterou AIS posílá svůj provoz na router, nýbrž o adresu, ze které odchází provoz do příslušné sítě ze zařízení, které je poslední v článku propojení AIS - Internet, respektive AIS - KIVS. Stručně řečeno, musí jít o adresu routovatelnou v rámci příslušné sítě.

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 Internetu nebo 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 obsluženo správným AISem).