

# DIGITÁLNÍ A INFORMAČNÍ AGENTURA\_

Export z Národní architektury eGovernmentu ČR

## Obsah

|                                                                        |                 |
|------------------------------------------------------------------------|-----------------|
| <b>Komunikační infrastruktura veřejné správy .....</b>                 | <b>3</b>        |
| <i><b>Popis Komunikační infrastruktury veřejné správy .....</b></i>    | <i><b>3</b></i> |
| <i><b>Pravidla Komunikační infrastruktury veřejné správy .....</b></i> | <i><b>4</b></i> |

# Komunikační infrastruktura veřejné správy

## Popis Komunikační infrastruktury veřejné správy

KIVS/CMS je centrální funkční celek, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy a samosprávy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy a samosprávy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. Skládá se ze 2 hlavních složek, jednak **Centrálního místa služeb (CMS)** a následně sítí, které jsou s ním propojeny (KIVS). Pro účely tohoto popisu se bere CMS/KIVS jako jeden celek, tedy samostatná a oddělená infrastruktura sloužící pro síťové a bezpečné propojení eGovernmentu.

KIVS jako samostatný pojem je také používán jako specifická možnost připojení do CMS. Při používání CMS/KIVS se myslí celek, který obsahuje obecně jakýkoliv způsob připojení, viz dále.

KIVS/CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

OVS přistupuje ke službám CMS pomocí portálu CMS na adrese <https://www.cms2.cz/>. Adresa portálu je dostupná pouze z vnitřní sítě KIVS/CMS, tedy až poté, kdy je OVS připojeno jednou z možných variant níže. Pokud se na adresu přistupuje mimo vnitřní síť KIVS/CMS, dostane se uživatel pouze na [stránku MVČR](#).

OVS a SPUÚ se připojují ke službám CMS výhradně jedním ze čtyř možných způsobů:

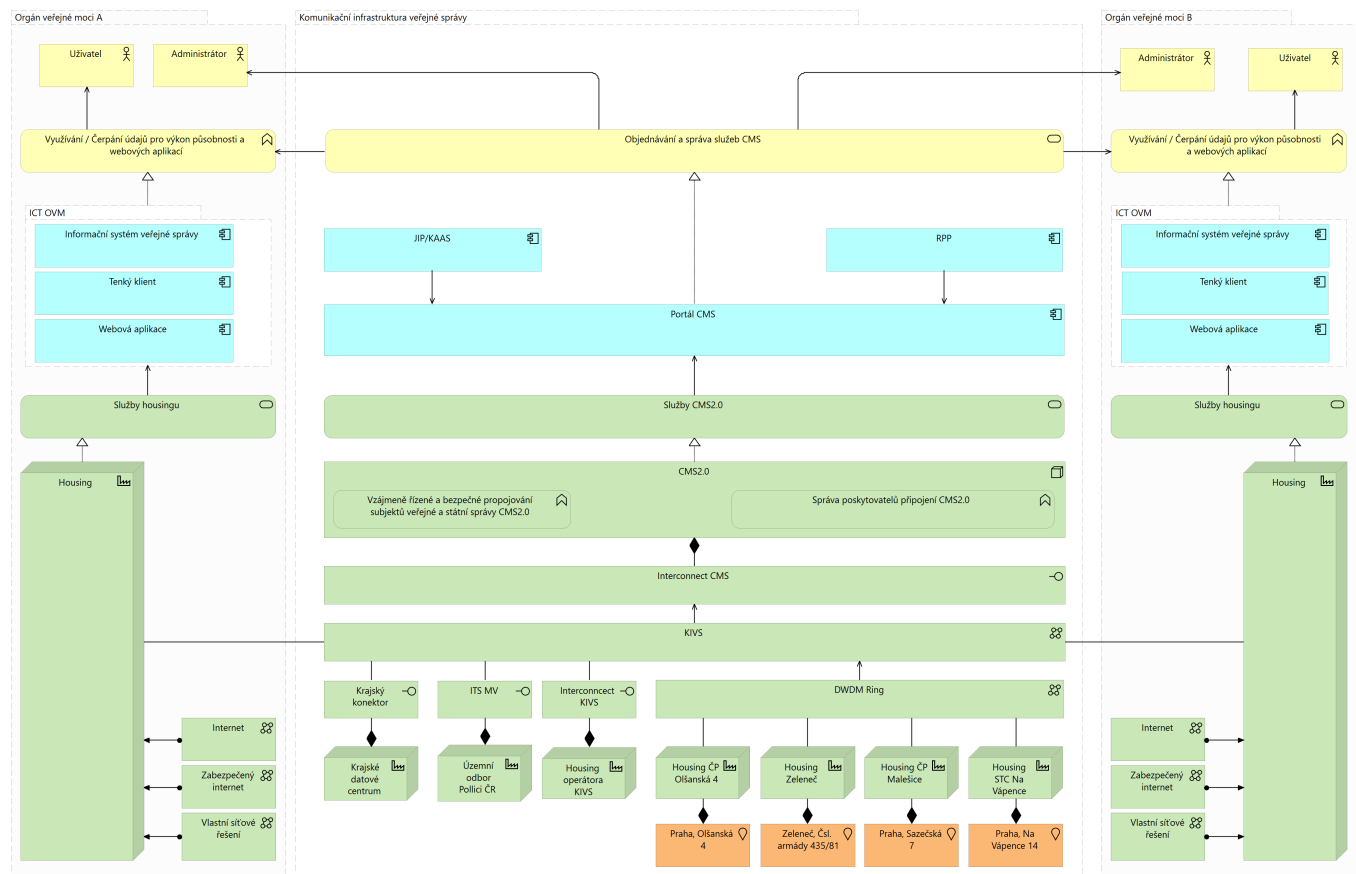
1. Prostřednictvím Krajských sítí (aktuálně v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím [metropolitních sítí](#) připojených např. na [Integrovanou telekomunikační síť \(ITS\) MVČR](#).
3. Prostřednictvím Komunikační infrastruktury veřejné správy (KIVS) s využitím [komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra](#).
4. Prostřednictvím veřejného internetu, a to přes zabezpečený tunel VPN SSL nebo VPN IPSec.

OVS čerpají služby eGovernmentu, jako např. [propojený datový fond](#), výhradně přes CMS. Pro čerpání služeb z CMS jsou pro OVS, **s výjimkou obcí I. typu**, přípustné pouze varianty 1 až 3 výše. Komunikace mezi jednotlivými OVS je vedena výhradně prostřednictvím KIVS/CMS, tzn. jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

**Obce I. typu** mají povolený způsob čerpání služeb CMS, a tedy i publikovaných služeb eGovernmentu (jako například [CzechPOINT](#), služby [základních registrů](#), atd.), prostřednictvím veřejného internetu, pokud jsou tyto služby publikovány do veřejného internetu s využitím služeb CMS.

Pokud chce úřad využít KIVS, tj. soutěž přes centrálního zadavatele Ministerstvo vnitra, je nutné definovat požadavky dle [katalogových listů](#) a následně zrealizovat nákup v dynamickém nákupním systému. Služby CMS lze čerpat také prostřednictvím [Národních datových center](#).

## Pohled na CMS/KIVS



## Pravidla Komunikační infrastruktury veřejné správy

Zákon 365/2000 sb. v aktuálním znění, zavedl povinnost publikovat služby ISVS jednotlivým uživatelům prostřednictvím Centrálního místa služeb (také jako CMS). V kombinaci s komunikační infrastrukturou veřejné správy (také jako KIVS) zavádí pro jednotlivé orgány veřejné správy bezpečnou, od internetu oddělenou, komunikační infrastrukturu poskytující pro jednotlivé orgány veřejné správy:

- Bezpečný a spolehlivý přístup k aplikačním službám jednotlivých ISVS
- Bezpečnou a spolehlivou publikaci aplikačních služeb jednotlivých ISVS
- Bezpečný přístup do internetu
- Bezpečný přístup k poštovním službám v internetu
- Zabezpečuje bezpečné síťové prostředí pro zajištění interoperability v rámci EU
- Umožňuje bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě internet

Cílem je:

- Publikovat bezpečným způsobem přes CMS/KIVS všechny aplikační služby centralizovaných ISVS se současným zajištěním bezpečného přístupu jednotlivých OVS k těmto službám při výkonu jejich působnosti.
- Umožnit bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě internet
- Zabezpečit bezpečné síťové prostředí pro zajištění interoperability v rámci EU

OVS přistupuje ke službám CMS pomocí portálu CMS na adrese <https://www.cms2.cz/>. Adresa portálu je dostupná pouze z vnitřní sítě KIVS/ CMS, tedy až poté, kdy je OVS připojeno jednou z možných variant níže. Pokud se na adresu přistupuje mimo vnitřní síť KIVS/CMS, dostane se uživatel pouze na [stránku MVČR](#). Centrální místo služeb, jakožto součást komunikační infrastruktury veřejné správy, je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu.

CMS tak můžeme nazvat privátní sítí pro výkon veřejné správy na území státu.

## Připojení k CMS

CMS/KIVS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

OVS a SPUÚ se připojují ke službám CMS výhradně jedním ze čtyř možných způsobů:

1. Prostřednictvím Krajských sítí (aktuálně v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím [metropolitních sítí](#) připojených např. na [Integrovanou telekomunikační síť \(ITS\) MVČR](#).
3. Prostřednictvím Komunikační infrastruktury veřejné správy (KIVS) s využitím [komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra](#).
4. Prostřednictvím veřejného internetu, a to přes zabezpečený tunel VPN SSL nebo VPN IPSec.

OVS čerpají služby eGovernmentu, jako např. [propojený datový fond](#), výhradně přes CMS. Pro čerpání služeb z CMS jsou pro OVS, **s výjimkou obcí I. typu**, přípustné pouze varianty 1 až 3 výše. Komunikace mezi jednotlivými OVS je vedena výhradně prostřednictvím KIVS/CMS, tzn. jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

**Obce I. typu** mají povolený způsob čerpání služeb CMS, a tedy i publikovaných služeb eGovernmentu (jako například [CzechPOINT](#), služby [základních registrů](#), atd.), prostřednictvím veřejného internetu, pokud jsou tyto služby publikovány do veřejného internetu s využitím služeb CMS.

Pokud chce úřad využít KIVS, tj. soutěž přes centrálního zadavatele Ministerstvo vnitra, je nutné definovat požadavky dle [katalogových listů](#) a následně zrealizovat nákup v dynamickém nákupním systému. Služby CMS lze čerpat také prostřednictvím [Národních datových center](#).

## IPsec a jeho úskalí

Ačkoliv jsou pro OVS přípustná jen připojení pomocí KIVS, existují úřady využívající připojení IPsec, který se ovšem nehodí pro kritické služby a funkce úřadování. Nevhodné je toto připojení např. pro systém CDBP (systém sběru žádostí o vydání občanského průkazu nebo cestovního dokladu občana České republiky), kdy mohou nastat následující rizika:

1. Spojení realizovaná prostřednictvím kryptografických prostředků přes veřejný internet nejsou vhodná jako primární způsob čerpání služeb, které mají mít garantovanou funkčnost a dostupnost. Systém CDBP je koncepčně založen na předpokladu provozu na vyhrazené síti, která je zcela oddělena od běžného internetového provozu a tomu odpovídá i úroveň jeho zabezpečení.
2. V rámci spojení realizovaných prostřednictvím veřejného internetu není možné dostatečným způsobem garantovat následující:
  - požadavek na dostupnost, protože internet není zaručeně garantované přenosové prostředí s definovanými SLA,
  - požadavek na propustnost, protože systém CDBP využívá na ORP "těžkého" klienta se vzdálenou správou; nezbytná je tedy komunikace oběma směry (centrum systému CDBP – ORP a ORP – centrum systému CDBP) pro instalaci nových verzí aplikace pomocí "balíčků" o velikosti cca 500 MB/PC a pro stahování logů z PC o velikosti cca 100 MB/PC,
  - požadavek na fungování protokolu WoL, který umožňuje dálkové „probouzení“ jednotlivých pracovních stanic systému CDBP bez zásahu obsluhy, je nezbytný z důvodů distribuce nových verzí SW, stahování logů či jiných činností souvisejících s provozem Systému CDBP.
3. Na základě výše uvedeného reálně hrozí, v případě využití IPsec, riziko výpadků spojení při pořizování

žádostí o občanské průkazy a cestovní pasy, což může vést ke zpomalení nebo úplné nedostupnosti pracovišť systému CDBP. V případě, že by v důsledku užívání IPsec, nebylo možné dálkově nainstalovat na koncová pracoviště systému CDBP aktualizace, bude nezbytné, aby instalaci provedl technik při výjezdu, který by úřad musel uhradit.

## CMS, popis zahrnutých služeb

Odbor Hlavního architekta eGovernmentu a Ministerstvo vnitra v rámci svých kompetencí požaduje od jednotlivých správců ISVS, aby služby ISVS publikovaly v rámci Centrálního místa služeb – CMS (služba CMS2 -02, CMS2 -04).

Jednotliví uživatelé ISVS na úrovni státní správy a samosprávy služby těchto systémů konzumují, resp. k ISVS přistupují výhradně prostřednictvím CMS (služba CMS2 -03).

### Služba CMS2 - 02 - Zveřejnění aplikace

| Název parametru | Vysvětlení                                                                                                                                                                                                                      |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kód služby      | CMS2-02                                                                                                                                                                                                                         |
| Název služby    | Zveřejnění aplikace                                                                                                                                                                                                             |
| Popis služby    | Služba vytvoří prostředí pro publikaci aplikační služby informačního systému OVM. Varianty služby se liší podle cílového prostředí. Možné varianty jsou: 1. do sítě Internet 2. do sítě CMS 3. do sítě TESTA-ng 4. do Extranetu |

Aplikační služba může být umístěna v infrastruktuře orgánu nebo v infrastruktuře Národního datového centra (NDC). Aplikační služba může být zveřejněna do více prostředí současně. Aplikační služba je zveřejněna na definovaných protokolech a portech.

Při zveřejnění aplikace do sítě Internet jsou aplikaci přiděleny veřejné IP adresy z prostoru CMS. Přístup ke zveřejněné službě může být omezen na definované zdrojové IP adresy.

Při zveřejnění aplikace do sítě CMS jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Službu je možné zveřejnit pro všechny ostatní subjekty připojené do sítě CMS (Veřejná služba) nebo pro definované subjekty a skupiny subjektů (Schvalovaná služba). O přístup ke Schvalované službě musí přistupující subjekty žádat prostřednictvím služby CMS203-1.

Při zveřejnění aplikace do sítě [TESTA-ng](#) (sít EU)<sup>1)</sup> jsou aplikaci přiděleny IP adresy z prostoru pro ČR v síti [TESTA-ng](#). Přístup ke zveřejněné službě je omezen na definované zdrojové IP adresy. Zveřejnění aplikace musí být provozováno v souladu s provozními a bezpečnostními požadavky EU pro síť [TESTA-ng](#).

Při zveřejnění aplikace do Extranetu jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Aplikační služba je zveřejněna do existujícího extranetu (extranet vytváří Správce CMS). Přístup k aplikaci v extranetu je umožněn všem uživatelům, kteří mají do daného extranetu přístup.

### Služba CMS2 - 03 - Přístup k aplikaci

| Název parametru | Vysvětlení                                                                                                                                                                                                                                 |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kód služby      | CMS2-03                                                                                                                                                                                                                                    |
| Název služby    | Přístup k aplikaci                                                                                                                                                                                                                         |
| Popis služby    | Služba umožňuje zřizovat a rušit přístupy k aplikačním službám. Varianty služby se liší podle cílového prostředí. Možné varianty představují přístup: 1. k aplikaci v síti CMS 2. k aplikaci v síti TESTA-ng 3. k aplikaci v síti Internet |

Služba umožňuje zřizovat, měnit a rušit přístupy subjektu k nabízené aplikační službě. Jednou žádostí lze zřídit přístup právě k jedné aplikační službě. Připojení je povoleno z definovaných IP adres v síti subjektu.

Přístup k aplikaci v síti CMS umožní subjektu připojení k aplikační službě zveřejněné jiným subjektem prostřednictvím služby CMS2-02-1 v síti CMS. Zřízení přístupu je podmíněno souhlasem vlastníka zveřejněné aplikační služby, které probíhá prostřednictvím portálu CMS.

Přístup k aplikaci v síti TESTA-ng umožní subjektu připojení k aplikační službě zveřejněné jiným státem Evropské unie v síti [TESTA-ng](#). Připojení je povoleno na definovaných protokolech a portech. Přístup k aplikaci musí být provozován v souladu s provozními a bezpečnostními požadavky EU pro síť [TESTA-ng](#).

Přístup k aplikaci v síti Internet umožní subjektu připojení k aplikační službě zveřejněné v síti Internet na definovaných protokolech a portech. Cílovou aplikační službu v síti Internet je nutné definovat konkrétními IP adresami, protokoly a porty.

#### Služba CMS2 - 04 - Publikace AIS na eGSB/ISSS

| Název parametru | Vysvětlení                                                                                                                                                                                                |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kód služby      | CMS2-04                                                                                                                                                                                                   |
| Název služby    | Publikace AIS na <a href="#">eGSB/ISSS</a>                                                                                                                                                                |
| Popis služby    | Služba zajišťuje zpřístupnění publikačního agendového informačního systému (AIS) v rámci CMS a povolení síťové komunikace s rozhraním <a href="#">eGon Service Bus / Informační systém sdílené služby</a> |

Služba zajistí provozovateli publikačního agendového informačního systému (AIS) síťovou konektivitu mezi [eGSB/ISSS](#) (eGON Service Bus / Informační systém sdílené služby, tj. sdílená služba obecného rozhraní) a publikačním AIS na definovaných protokolech a portech. V rámci publikace jsou přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy).

Ve výchozím stavu je komunikace mezi [eGSB/ISSS](#) a publikačním AIS synchronní, volitelně lze zprovoznit komunikaci asynchronní.

#### Právní aspekty

S výjimkou tzv. provozních informačních systémů, které jsou uvedeny v § 1 odst. 4 písm. a) až d) zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoiSVS), je § 6g odst. 3 tohoto zákona správcům ISVS uložena povinnost poskytovat služby informačních systémů veřejné správy prostřednictvím CMS. Organům veřejné správy je prostřednictvím § 6g odst. 4 ZoiSVS uložena povinnost využívat sítě elektronických komunikací CMS."

Protože skrze CMS se publikují služby tzv. [referenčního rozhraní](#), definovaného v § 2 písm. j) ZoiSVS, má vztah k CMS i povinnost uložená v § 5 odst. písm. d) ZoiSVS, tj. povinnost správců ISVS zajistit, aby vazby jimi spravovaného ISVS na ISVS jiného správce byly uskutečňovány prostřednictvím CMS.

S ohledem na výše popsané vlastnosti CMS, jakož i s ohledem na výše popsané právní aspekty, lze také dodat, že využívání, popř. nevyužívání CMS je relevantním faktorem pro posuzování plnění souvisejících právních povinností, a to zejména povinností v oblasti kybernetické bezpečnosti nebo ochrany osobních údajů, jakož i povinnosti řádného a hospodárného nakládání s veřejnými finančními prostředky a povinnosti k předcházení vzniku škod.

[CMS](#), [KIVS](#), [Centrální místo služeb](#), [Komunikační infrastruktura veřejné správy](#)

<sup>1)</sup>

Interaktivní mapa TESTA-ng [https://ec.europa.eu/isa2/solutions/testa\\_map\\_en/](https://ec.europa.eu/isa2/solutions/testa_map_en/)

From:

<https://archi.gov.cz/> - **Architektura eGovernmentu ČR**

Permanent link:

[https://archi.gov.cz/nap:komunikacni\\_infrastruktura\\_verejne\\_spravy?rev=1680695318](https://archi.gov.cz/nap:komunikacni_infrastruktura_verejne_spravy?rev=1680695318)

Last update: **2023/04/05 11:48**

