DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Communication infrastructure of public administration

Description of the Public Administration Communication Infrastructure

KIVS/CMS is a central functional unit whose primary purpose is to provide a controlled and registered connection of information systems of state and local government entities to services (applications) provided by information systems of other state and local government entities with defined security and SLA parameters, i.e. access to eGovernment services. It consists of 2 main components, on the one hand **Central Point of Service (CMS)** and then the networks that are connected to it (KIVS). For the purpose of this description, the CMS/KIVS is taken as a single entity, i.e. a separate and distinct infrastructure serving the networking and secure interconnection of eGovernment.

KIVS as a separate term is also used as a specific connectivity option to the CMS. When using CMS/KIVS, it refers to the whole, which generally includes any connection method, see below.

KIVS/CMS, as a private public administration network, uses dedicated or leased network resources to securely connect public administration officials (OVS) working in public administration agencies to their remote agency information systems, to securely network agency systems to each other, and to securely connect individual OVS to the Internet.

The OVS accesses CMS services via the CMS portal at https://www.cms2.cz/. The portal address is only accessible from the internal KIVS/CMS network, i.e. only after the VCS is connected by one of the options below. If the address is accessed from outside the internal KIVS/CMS network, the user will only reach the MRC website.

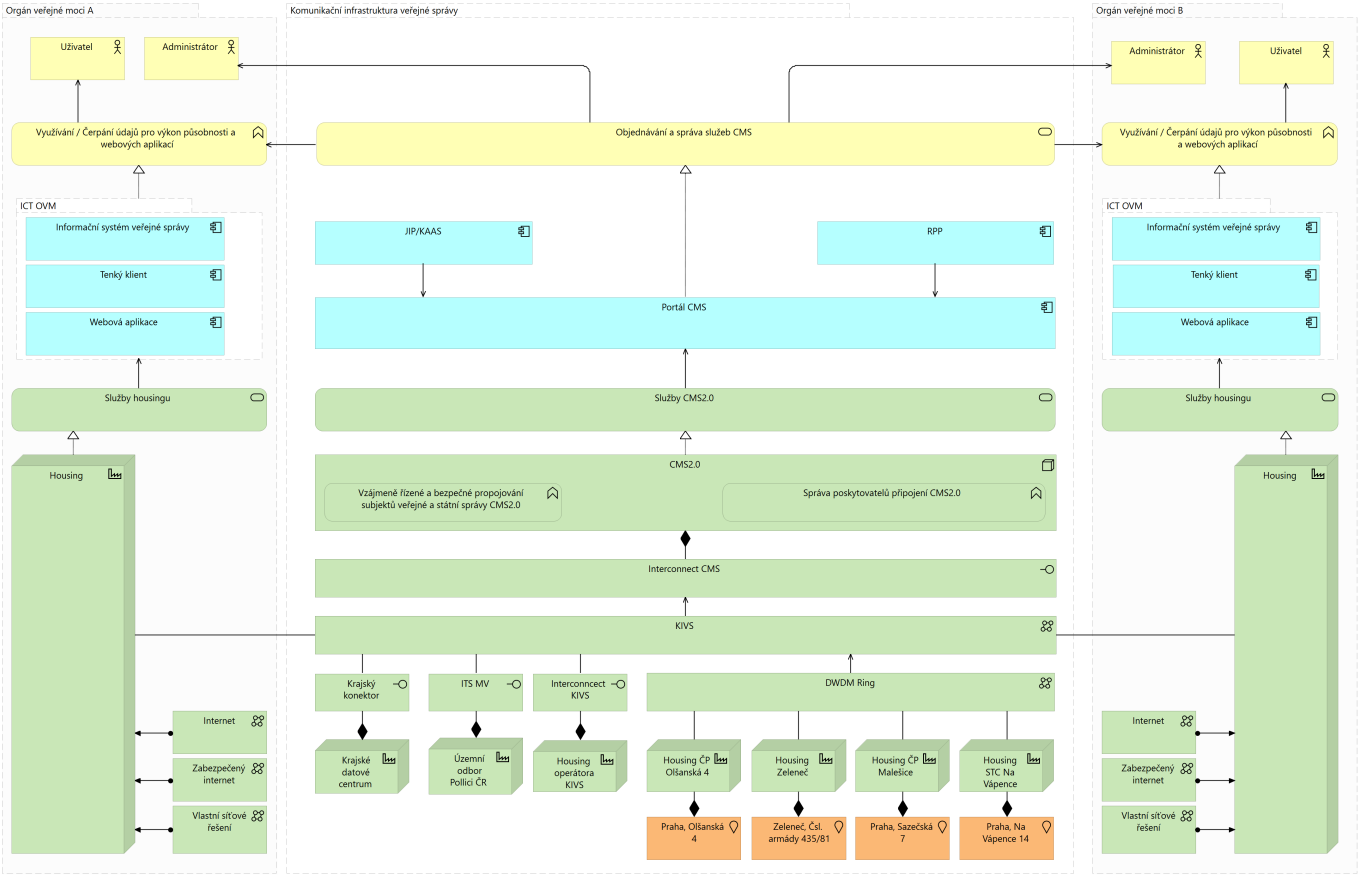
OVS and SPUUs access eGovernment services, such as [en:nap:propojeny_datovy_fond|connected data pool,]] exclusively through the CMS in one of the four possible ways:

1. Through the Regional Networks (currently in the Vysočina, Pilsen, Karlovy Vary, Zlín and partly Pardubice regions + more if built).
2. Through metropolitan networks connected e.g. to the Integrated Telecommunication Network (ITS) of the MVČR.
3. Through the Communication Infrastructure of Public Administration (CIPA) using commercial offers competed through the Ministry of the Interior.
4. Via the public Internet, via a secure VPN SSL or VPN IPSec tunnel.

If the Authority wishes to use the KIVS, i.e. to compete through the central contracting authority of the Ministry of the Interior, it is necessary to define the requirements in accordance with catalogue sheets and then implement the purchase in the dynamic purchasing system. CMS services can also be used via National Data Centres.

Only variants 1 to 3 are admissible for the Public Procurement Service (PPA), so that communication between the PPAs is conducted exclusively via the KIVS/CMS, i.e. the individual PPAs are obliged to access the Public Administration Information Systems (PIS) only via the KIVS/CMS.

View of CMS/CIVS



Public Administration Communication Infrastructure Rules

Act 365/2000 Coll. as amended, introduced the obligation to publish ISVS services to individual users via the Central Service Point (also known as CMS). Combined with the Communication Infrastructure of Public Administration (also referred to as CIVS), it establishes a secure, Internet-separated communication infrastructure providing for individual public administration bodies:

- Secure and reliable access to the application services of the individual ISVS
- Secure and reliable publication of application services of individual ISVS
- Secure access to the Internet
- Secure access to postal services on the Internet
- Provides a secure network environment to ensure interoperability within the EU
- Enables secure access to ISVS application services intended for VS end clients from the Internet

Objective:

- To publish in a secure manner via CMS/KIVS all application services of centralised ISVS while ensuring secure access of individual VCS to these services in the exercise of their competences.
- Enable secure access to the application services of the ISVS intended for the VS end clients from the Internet.
- Ensure a secure network environment to ensure interoperability within the EU

OVS accesses CMS services through the CMS portal at https://www.cms2.cz/. The portal address is only accessible from the internal KIVS/ CMS network, i.e. only after the OVS is connected by one of the possible options below. If the address is accessed from outside the internal KIVS/CMS network, the user will only reach the MRC website. The Central Service Point, as a part of the public administration communication infrastructure, is a system whose primary purpose is to provide a controlled and registered connection of information systems of public administration entities to services (applications) provided by information systems of other public administration entities with defined security and SLA parameters, i.e. access to eGovernment services.

CMS can thus be called a private network for the performance of public administration on the territory of the state.

Connecting to CMS

KIVS/CMS, as a private public administration network, uses dedicated or leased network resources to securely connect public administration officials (OVS) working in public administration agencies to their remote agency information systems, to securely network agency systems to each other, and to securely connect individual OVS to the Internet.

OVS and SPUUs access eGovernment services, such as [en:nap:propojeny_datovy_fond|connected data pool,]] exclusively through the CMS in one of the four possible ways:

1. Through the Regional Networks (currently in the Vysočina, Pilsen, Karlovy Vary, Zlín and partly Pardubice regions + more if built).
2. Through metropolitan networks connected e.g. to the Integrated Telecommunication Network (ITS) of the MVČR.
3. Through the Communication Infrastructure of Public Administration (CIPA) using commercial offers competed through the Ministry of the Interior.
4. Via the public Internet, via a secure VPN SSL or VPN IPSec tunnel.

If the Authority wishes to use the KIVS, i.e. to compete through the central contracting authority of the Ministry of the Interior, it is necessary to define the requirements in accordance with catalogue sheets and then implement the purchase in the dynamic purchasing system. CMS services can also be used via National Data Centres.

Only variants 1 to 3 are admissible for the Public Procurement Service (PPA), so that communication between the PPAs is conducted exclusively via the KIVS/CMS, i.e. the individual PPAs are obliged to access the Public Administration Information Systems (PIS) only via the KIVS/CMS.

IPsec and its pitfalls

Although only KIVS connections are allowed for OSS, there are offices using IPsec connections, but this is not suitable for critical services and office functions. This connection is not suitable for e.g. the CDBP system (system for collecting applications for the issue of an ID card or travel document of a citizen of the Czech Republic), where the following risks may occur:

1. Connections made via cryptographic means over the public Internet are not suitable as the primary means of accessing services that are intended to be guaranteed to be functional and available. The CDBP system is conceptually based on the assumption of operation on a dedicated network, which is completely separate from normal Internet traffic, and its level of security corresponds to this.
2. The following cannot be sufficiently guaranteed for connections made via the public Internet:
    - the availability requirement, as the Internet is not a guaranteed transmission environment with defined SLAs,
    - throughput requirement, because the CDBP system uses a "heavy" client with remote administration at the ORP; therefore, communication in both directions (CDBP system centre - ORP and ORP - CDBP system centre) is necessary for installing new versions of the application using "packages" of approx. 500 MB/PC and for downloading logs from the PC of approx. 100 MB/PC,
    - the requirement for the WoL protocol, which allows remote "wake-up" of individual workstations of the CDBP System without operator intervention, is necessary for the distribution of new software versions, downloading logs or other activities related to the operation of the CDBP System.
3. On the basis of the above, there is a real risk, if IPsec is used, of connection failures when making applications for ID cards and passports, which may lead to slowdowns or complete unavailability of CDBP System workstations. In the event that, as a result of the use of IPsec, it would not be possible to

remotely install updates on CDBP System endpoints, it would be necessary for a technician to carry out the installation on a call-out basis, which would have to be paid for by the Authority.

CMS, Description of Covered Services

The Department of the Chief Architect of eGovernment and the Ministry of the Interior, within their respective competences, require individual ISVS administrators to publish ISVS services within the Central Point of Service - CMS (service CMS2 -02, CMS2 -04).

Individual users of ISVS at the level of state and local government consume the services of these systems or access ISVS exclusively via CMS (service CMS2 -03).

Service CMS2 - 02 - Application publication

Parameter name	Explanation
Service Code	CMS2-02
Service Name	Application Publication
Service Description	The service creates an environment for publishing an OVM information system application service. The service variants vary according to the target environment. The possible variants are: 1. to the Internet 2. to the CMS network 3. to the TESTA-ng network 4. to the Extranet

The application service can be hosted in the infrastructure of the institution or in the infrastructure of the National Data Centre (NDC). An application service may be published to multiple environments simultaneously. The application service is published on defined protocols and ports.|

When an application is published to the Internet, public IP addresses from the CMS space are assigned to the application. Access to the published service may be restricted to defined source IP addresses.

When an application is published to the CMS network, private IP addresses from the CMS space (Consolidated IP addresses) are assigned to the application. The service can be published to all other entities connected to the CMS network (Public Service) or to defined entities and groups of entities (Approved Service). Access to the Approved Service must be requested by accessing entities through the CMS203-1 service.

When an application is published to the TESTA-ng network (EU network), the application is assigned IP addresses from the CR space in the TESTA-ng network. Access to the published service is limited to the defined source IP addresses. The application publishing must be operated in accordance with the operational and security requirements of the EU for the TESTA-ng network.

When publishing an application to the Extranet, private IP addresses from the CMS (Consolidated IP Addresses) space are assigned to the application. The application service is published to an existing extranet (the extranet is created by the CMS Administrator). Access to the application in the extranet is granted to all users who have access to the extranet.

CMS2 Service - 03 - Application Access

Parameter name	Explanation
Service Code	CMS2-03
Service Name	Application Access
Service Description	This service allows you to set up and cancel access to application services. Service variants vary depending on the target environment. The possible variants represent access to: 1. an application on the CMS network 2. an application on the TESTA-ng network 3. an application on the Internet

The service allows to set up, change and cancel subject accesses to the offered application service. Only one application service can be accessed with one request. Connection is allowed from defined IP addresses in the subject's network.|

Access to an application on the CMS network allows an entity to connect to an application service published by another entity through the CMS2-02-2 service on the CMS network. Establishment of access is subject to approval by the owner of the published application service, which is done through the CMS portal.

Access to an application on the TESTA-ng network will allow an entity to connect to an application service published by another EU State on the TESTA-ng network. Connection is allowed on defined protocols and ports. The application access shall be operated in accordance with the EU operational and security requirements for the TESTA-ng network.

Access to the application on the Internet shall allow the subject to connect to the application service published on the Internet on defined protocols and ports. The target application service on the Internet must be defined by specific IP addresses, protocols and ports.

Service CMS2 - 04 - AIS Publication on eGSB/ISSS

Parameter Name	Explanation
Service Code	CMS2-04
Service Name	AIS Publication on eGSB/ISSS
Service Description	The service provides access to the Publishing Agenda Information System (AIS) within CMS and enables network communication with the eGon Service Bus / Shared Service Information System interface.

The service shall provide the publishing AIS operator with network connectivity between eGSB/ISSS (eGON Service Bus / Shared Service Information System, i.e. a shared generic interface service) and the publishing AIS on defined protocols and ports. Private IP addresses from the CMS (Consolidated IP Addresses) space are allocated within the publication.

By default, the communication between eGSB/ISSS and the publishing AIS is synchronous, optionally asynchronous communication can be enabled.

Legal aspects

With the exception of the so-called operational information systems listed in Section 1(4)(a) to (d) of Act No 365/2000 Coll., on public administration information systems (ZoISVS), Section 6g(3) of this Act imposes an obligation on the administrators of ISVS to provide public administration information system services via the CMS. Public administration bodies are obliged to use the electronic communication networks of the CMS by means of Section 6g(4) ZoISVS.

As the services of the so-called reference interface, as defined in § 2(j) of ZoISVS, are published through the CMS, the obligation imposed in § 5(d) of ZoISVS, i.e. the obligation of ISVS administrators to ensure that the links of the ISVS they administer to the ISVS of another administrator are made through the CMS, is also related to the CMS.

In view of the characteristics of the CMS, as well as the legal aspects described above, it may also be added that the use or non-use of the CMS is a relevant factor for assessing the fulfilment of the related legal obligations, in particular the obligations in the field of cyber security or protection of personal data, as well as the obligation of sound and economic management of public funds and the obligation to prevent damage.

CMS, KIVS, Central Point of Service, Public Administration Communication Infrastructure