Materiál Ministerstva vnitra

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

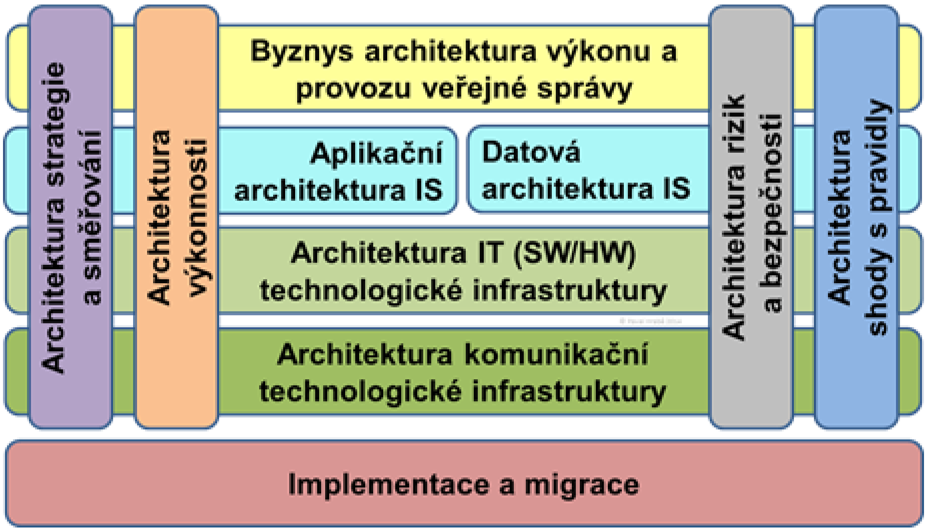
Export z Národní architektury eGovernmentu ČR

Obsah

Authority architecture in the context of public administration and its layers of architecture

This chapter describes the architecture of the office and the public administration of the Czech Republic by each layer of architecture and the incorporation of requirements into the information concept and architecture of the office. This is a different approach to describing the requirements for the use of eGovernment systems and services than in Methods for the use of shared services, functional units and thematic areas of individual offices, where requirements are described in the full breadth (throughout the architecture) of a shared service, functional unit or thematic area.

The composition of this chapter corresponds to National Architecture domains


Architektura strategie a směrování
Architektura výkonnosti
Byznys architektura výkonu a provozu veřejné správy
Aplikační architektura IS
Datová architektura IS
Architektura IT (SW/HW) technologické infrastruktury
Architektura komunikační technologické infrastruktury
Architektura rizik a bezpečnosti
Architektura shody s pravidly
Implementace a migrace

Authority Strategy and Direction Architecture Rules

Incorporating the rules of this architecture layer will describe the Authority's information design.

Alignment with strategic documents, their principles and objectives is essential for the strategy and direction architecture. These documents include:

1. The Digital Czech Republic Strategy and, in particular, the Information Concept of the Czech Republic
2. Information Concept of the Authority
3. National Architectural Plan
4. Strategic Framework for the Development of Public Administration 2014+
5. Concept of client-oriented public administration 2021+
6. Strategy for the development of spatial information infrastructure in the Czech Republic until 2020 (GeoInfoStrategy)

In the model of the authority's own overall architecture, the diagrams of strategic objectives, architectural principles, architectural requirements and constraints, outlined development directions and expected outcomes should serve the practical use in the management of the authority. These should combine in a coherent way objects taken from the overarching strategies, see above, and from the Authority's own strategies and concepts.

The Authority's Performance Architecture Rules

The incorporation of the rules of this architecture layer will be described by the Authority in its information concept.

There are currently no rules for this domain of architecture established by the National Architecture Plan.

Authority's Public Service Performance Business Architecture Rules

The description of centrally provided systems and their services, functional units and thematic areas is described in Description of shared services, functional units and thematic areas of public administration in the Czech Republic.

Rules for individual shared services, functional units and thematic areas are described in Methods for the use of shared services, functional units and thematic areas of individual offices.

The incorporation of the rules of this architecture layer shall be described by the authority in its information concept.

In terms of IT governance, the business architecture is a specification for effective IT support for the performance of public administration. Therefore, the current model of the target state of the authority's business architecture is a mandatory prerequisite and an integral part of the information concept of every authority, public administration body.

Division of public administration processes and functions

In order to decide on options to support the public administration needs of the authority, it is necessary to evaluate and classify all these business needs of the VS from several perspectives.

The head of the IT department of the authority and the technical administrators of the ISVS are obliged, in cooperation with their subject matter administrators, to create and maintain an up-to-date model of the process or functional decomposition of the authority and its diagram, the so-called Business Portfolio/Architecture Map of the authority.

This model must, by the nature of comprehensive IT governance of the Authority, include the identification of all activities (capabilities, processes, functions or services, hereafter represented only by the term function) performed by the organisation, whether they are currently manual or computerised. As part of the means of long-term management of the development of the Authority's IS, all these functions of the Authority must be assessed as to how satisfactorily and effectively they are supported by information technology and to what extent this is intended to be done within the time horizon of the Authority's information concept (5 years). This part of the OVS Information Concept must then include and take into account in particular:

- the decision to consolidate IT support for the business functions of the Authority,

- a decision on the possibility of shared IT support for the Authority's business functions,
- optimisation of the Authority's ICT-supported functions - supplementing and developing the inadequate ICT support for the Authority's functions.

In doing so, it is necessary to view and decide on the identified functions of the Authority from at least the following four perspectives:

1. The aspect of the degree of support of external services for public administration clients.
2. The degree (and potential) of similarity, consistency and centralisation of processes.
3. The extent (and potential) for displacement of functions and the use of shared services in place of individual functions.
4. The aspect of performing the functions of the authority in one's own or others' name and on one's own or others' account.

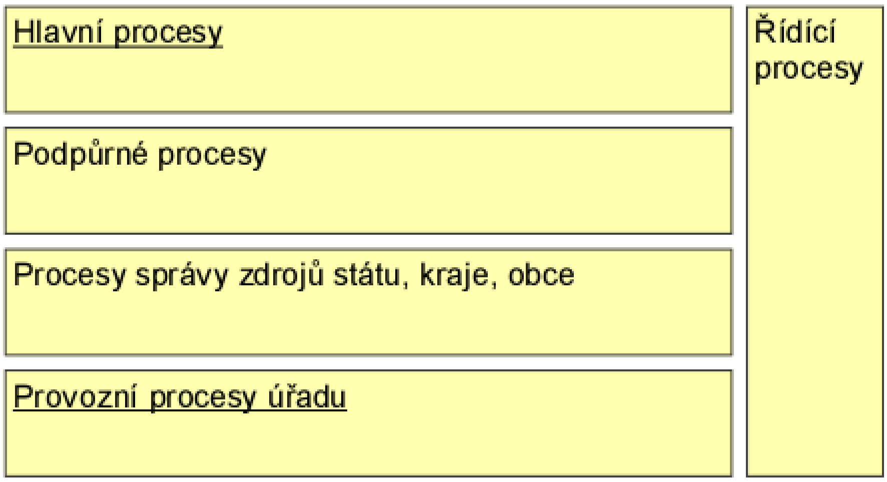
According to all the above-mentioned points of view, the needs of the Authority's functions for application support differ, and it is therefore necessary to distinguish between them and then design the solution for this application support and choose the way of its implementation accordingly. It is important to know these characteristics of the Authority's functions and to manage the development of the Authority's applications accordingly.

Detailed reference models of business architecture, elaborating the rules mentioned here, including their graphical representation, are determined and published by the Department of the Chief Architect of the Ministry of the Interior of the Czech Republic, in cooperation with the eGovernment Department of the Ministry of the Interior of the Czech Republic and organisations representing individual levels of state administration and self-government.

Aspects of the level of support for external services for public administration clients

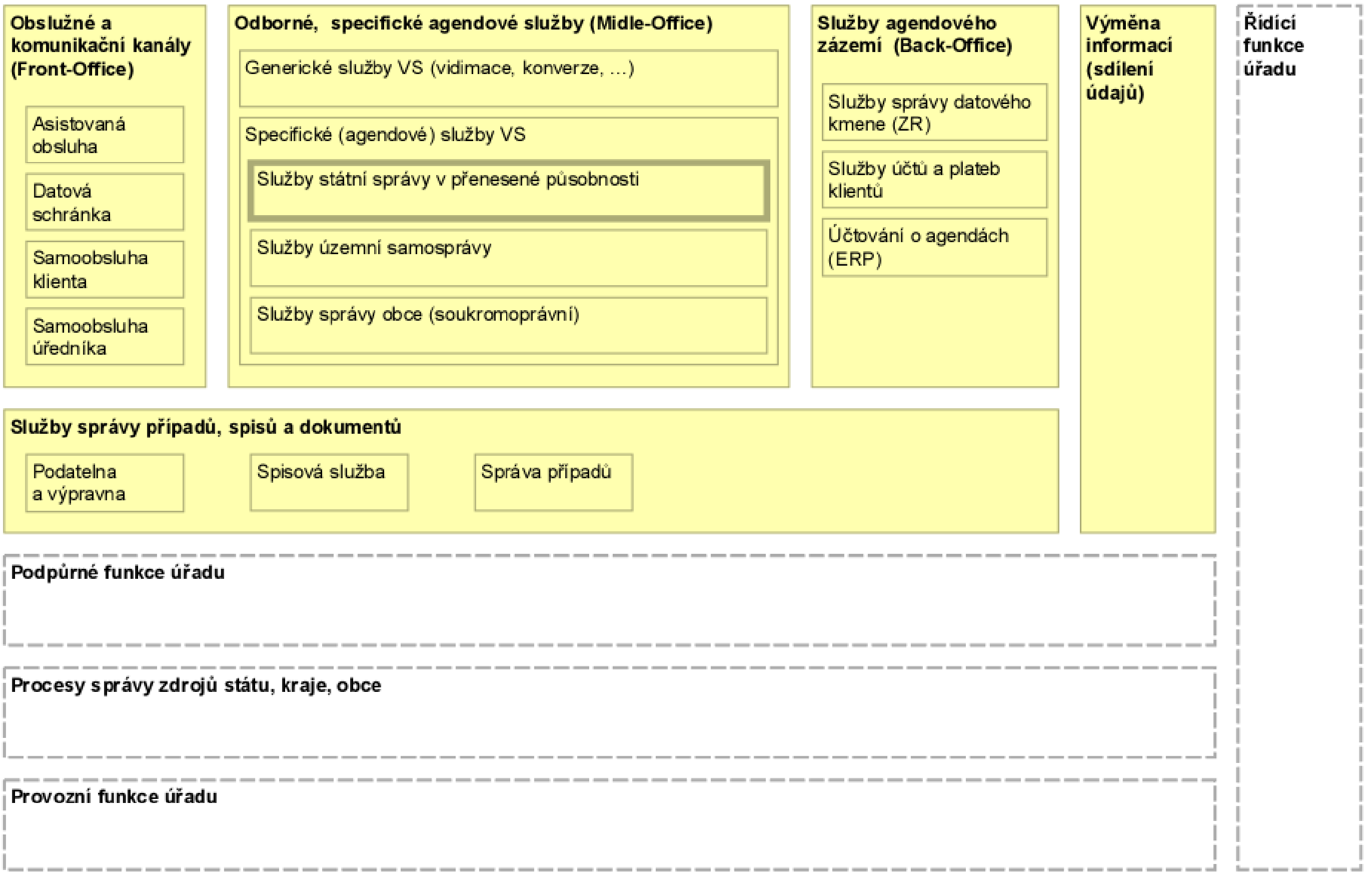
In order to facilitate the modelling of the business layer of the authority architecture, the National Architecture Plan proposes the following Reference Model of the Authority Business Architecture. This divides the Authority's functions into layers according to their "distance" from the provision of services to external clients as follows:

- Core processes, functions of the Authority - performed by the Authority in interaction with an external client or for the performance of a government service to an external client.
- Supporting processes, functions of the authority - performed by the authority as a prerequisite, direct support or follow-up to the individual provision of services to external clients
- Shared resource management functions and processes - performed by the Authority to provide all other prerequisites and resources according to its role and position in public administration, without direct connection to the support of services to its individual external clients.
- Management and development functions - performed by the Authority to enable it to plan, implement, monitor and evaluate the quality and performance of its functions and their further development.
- Operational functions - performed by the Authority as a management of essential resources to ensure its sustainable existence (operations), regardless of its core, support and shared resource functions.



The Authority Business Architecture Reference Model further divides the core functions for performing services mainly to external clients (citizens and representatives of organizations), but also to internal clients (authorities and officials) into:

- Service functions - representing the interaction with clients in all and any service and communication channel, Front-Office (also referred to as FO), targeted as jointly and uniformly as possible, across agencies.
- Specialist functions - representing specialisation in the performance and decision-making of an agenda or operational function, Middle-Office (hereafter also MO). They can be further divided into:
  - Generic public administration professional functions (vidimation, conversion, etc.).
  - Agenda-specific public administration functions
- Common back-office functions - representing functions typically (but not exclusively) performed outside of client interaction, from Back-Office (hereinafter also BO), jointly and uniformly for several (up to all) agencies of the authority.
- File and case management functions - used to manage documents and information linking the various phases (and functional areas) of client case handling (management), both internal and external. All the duties of maintaining proper documents and files in the case management service must not be replaced by case records, which are only for special matters outside established and proper procedures.
- Inter-agency integration and cooperation functions in the delivery of services to clients.


Obslužné a komunikační kanály (Front-Office)
Asistovaná obsluha
Datová schránka
Samoobsluha klienta
Samoobsluha úředníka
Odborné, specifické agendové služby (Midle-Office)
Generické služby VS (vidimace, konverze, ...)
Specifické (agendové) služby VS
Služby státní správy v přenesené působnosti
Služby územní samosprávy
Služby správy obce (soukromoprávní)
Služby agendového zázemí (Back-Office)
Služby správy datového kmene (ZR)
Služby účtů a plateb klientů
Účtování o agendách (ERP)
Výměna informací (sdílení údajů)
Řídící funkce úřadu
Služby správy případů, spisů a dokumentů
Podatelna a výpravna
Spisová služba
Správa případů
Podpůrné funkce úřadu
Procesy správy zdrojů státu, kraje, obce
Provozní funkce úřadu

Aspects of the degree (and potential) of displacement of functions and the use of shared services in place of individual functions

Identified functions in the authority's business architecture model should be considered in terms of the availability of already shared business services or the potential for displacement (outsourcing) to the provider of such shared services - within the authority or local government unit by choice, elsewhere by law or regulation.

In doing so, we distinguish the following possibilities (levels) of sharing on:

- Nationally (statewide) shared services. These are further subdivided at this and all other levels into:
  - external services in support of public administration clients (and, where applicable, OVM) - services for core and support processes
  - internal services in support of authorities and officials - shared resource, management and operational process services
- Shared services of public corporations (budget chapter administrators, regional and local (ORP) territorial corporations)
- Shared services within the office - typically services for the service functions (FO), for the back office (BO) functions, and for the document, file, and case management functions
- Individual (partial, specific, non-shared) functions - typically professional agency functions (MO)

Aspect of performing the functions of the office in one's own name or on behalf of others and on one's own or others' account

As a counterpart to functions handed over to another authority, organisation to perform, there are functions in public administration bodies performed for someone else, i.e. on someone else's behalf, on someone else's account, or both. For all identified functions of the authority it is necessary - always - to assess this aspect as well, i.e. for activities (processes, functions, services) on whose behalf and on whose account they are performed. Typical examples of functions taken over in this way are:

- Performance of public administration services under delegated competence
- Performance of corporate or state shared service centres

Reporting of Authority Agencies in the RPP

The Act 111/2009 Coll. on Basic Registers introduced an unambiguous hierarchy of agencies and agency information systems, together with the indication of both the data that are kept within the agency and the data that the agency is entitled to use in its activities from basic registers and other agencies. The implications for the design of the information systems architecture at all layers of the model are presented within this text.

An agenda is defined by the central administrative authority responsible for the execution of the agenda **in legal terminology**. The description of the data therefore does not use technological terminology but the terminology given in the relevant legal regulation.

The authority operating the agenda can no longer influence the declaration of the agenda, but may, if necessary, request the central administrative authority which declared the agenda to modify it.

The logic of the notification of agendas determines what data is kept in the agenda on the individual subjects/objects of law as defined in the legislative text. Within the adopted notation, the agenda code is denoted by a capital letter A followed by the assigned agenda number. The individual subjects/objects about which data **(contexts)** are kept in the agenda are further numbered consecutively. This is followed by the number of the data within the context.

Thus, for example

- Agenda A998 *Agenda on the conditions of operation of vehicles on roads*
- has the first context listed as 998-1 *Road vehicle*
- which has 998-1-*1 Owner and operator data, if different from the owner, as the first context*

The purpose of this registration is **not a detailed data breakdown** into items in an informational sense, but to determine the data to which the authorisation for use can be related. It is therefore clear that the data 998-1-1 is subsequently broken down into information items (see Act No 56/2001 Coll., on the conditions of operation of vehicles on the road, Section 4(2)(a)).

Each information item must therefore be listed as an additional layer in the notation

998-1-1-1 **Name** of the owner of the road vehicle.

The purpose of this notation, the notification of the agendas in the Register of Rights and Obligations and the subsequent technological specification is to **uniquely separate legal and informational responsibilities.** Thus, when designing a publication via eGSB / ISSS, the administrator of the agenda defines the legal division of contexts and data and the administrator of the respective agenda information system the subsequent informational division of these data. This partitioning then uniquely defines the item in the transmitted data record within the linked data pool and the management of access permissions to that item.

Thus, the Agenda Information System Administrator must work with the Agenda Administrator to report the agenda so that an unambiguous decomposition of the data in context can be performed on a single information item. The definition of these information items is subsequently part of the data interface definition.

The chosen principle avoids confusion of data by name (the name of the vehicle owner is certainly different from the name of the property owner, although both items are named name) and it is necessary to use the above numerical hierarchical notation in the design of all data interfaces.

The agency administrator also determines, when notifying, which data from the basic registers or other agencies it is entitled to use in its activities, and the agency information system administrator then draws on the definition of data items of the individual ISVS that publish data/data to the linked public administration data pool when designing the data interface.

If an agenda is executed through multiple Agenda Information Systems, then the agenda manager must designate the Agenda Information System manager that will bind the decomposition of data into data items, and the other Agenda Information System managers must respect this decomposition.

Breakdown of public administration service and communication channels

The service and communication channels of a public administration authority towards its external clients can be divided from several perspectives for the purpose of their effective management and their IT support, according to:

- Sharing and subjectivity of the operator of the service channel into own, central, delegated, with service providers (third parties) and other
- According to the degree of client involvement in the
  - Self-service or
  - assisted (face-to-face, externally paper or voice but internally fully electronic)
- By relationship to location and agenda into
  - Universal - without local or subject matter jurisdiction,
  - territorial - with local but no subject matter jurisdiction, and
  - agency - with subject matter jurisdiction (of one or more agencies of the same central administrative authority) but without local jurisdiction (historically and, where justified, local jurisdiction).
- According to the medium of communication and means of filing/delivery, in person - by writing a report, in paper form - by post, courier or at the registry office, and in electronic form - by data box, by electronically signed document in the electronic registry or in a specific application of the office (according to specific laws), or by the procedure described on the official board of the office.

The aim is to serve as many client needs as possible in the first level of service, i.e. in universal contact points (also referred to as "UKM") - client centres such as the self-service Client Portal (citizen, entrepreneur, organisation representative and foreigner) in PVS and assisted CzechPOINT. Specialised contact points of the authorities will continue to be available for the necessary individual services.

The starting assumption in the design of the solution should be to make every effort to ensure that the client can find the maximum available information about his/her contacts and procedures with the public administration within the UKM.

However, in the case of assisted contact points (both universal and in territorial or agency OVS), the information on all information on the relationship between the client and the public administration will be mediated by a civil servant, solely on the basis of explicit authorisation by the client. This is the only case where the clerk is allowed to see more than one agenda at the same time, but is only allowed to see status information from notifications, i.e. whether the client should pay attention to the agenda for some right or obligation. Based on such an overview, the client may instruct the clerk to handle each agenda for it one by one.

All actions in the service channels must be adequately recorded and logged in the transaction log of the relevant IS and in the office's filing service.

The public administration office is obliged to ensure full equality of all service channels in the legislation (if it can influence it), in the office processes and in their application support (to the extent according to the legislation in force) and to allow the client to choose between the channels.

The preference for a channel that is more efficient from the point of view of the Authority, i.e. typically an electronic self-service channel, is only possible by increasing its attractiveness for the client, not by regulatory action (regulation, sanctions).

Furthermore, for IT support in the Authority, it follows that at the end of the horizon of the rules of this ICR, currently in 2023, it is valid for all the Authority's agendas that:

- All solutions (legal, business and IT) must be designed to be fully electronic internally and support all service channels (document conversion) externally.
- All contact channels, including specialised ones, will support navigation to the service (service discovery) according to life situations resulting from clients' life events.

Modifications to the legal environment, business processes and functions and IT solutions will be designed to support equality and interconnectedness of service channels (Multichannel) in the long term - i.e. a procedure can be started in any channel, monitored in another and completed in another.

The impact of the Authority's business architecture on its IT support solution options

The nature of the Authority's activities, see the decomposition above, suggests opportunities for sharing and achieving effective application support for those activities.

Where the authority remains legally responsible for a particular activity (agenda, support function) it cannot use shared solutions and even at the level of central eGovernment elements such shared solutions will not be prepared until the legal conditions for this area change.

An example is ERP or a filing service. Here, both the processes and their application support must be owned by each authority, which remains the substantive administrator of these solutions. Therefore, if an authority is the substantive manager of a solution, it retains responsibility for it and should have the power to make an immediate decision on it - it should be a solution under the authority of that authority.

In this case, for such solutions as ERP or eSSL, the OVS can only use shared services at IT technology and platform level, the software solution must be provided to it in a maximum so-called multitenant form (multiple separate tenants) on a common technical infrastructure, so that the individual responsibility of the OVS for the activity and data is maintained.

Rules for the application architecture of the VS Office IS

The description of centrally provided systems and their services, functional units and thematic areas is described in Description of shared services, functional units and thematic areas of public administration of the CR.

Rules for individual shared services, functional units and thematic areas are described in Methods for the use of shared services, functional units and thematic areas of individual offices.

The incorporation of the rules of this architecture layer shall be described by the authority in its information concept.

From the point of view of IT governance, the application architecture is the centre of gravity for the management of effective IT support for the performance of public administration. The development of each authority's information system is done through the development of its application components, in the context of all other application components of the authority and available shared eGovernment application services. Therefore, the current model of the target state of the authority's application architecture is the basis of the information concept of each authority, public administration body.

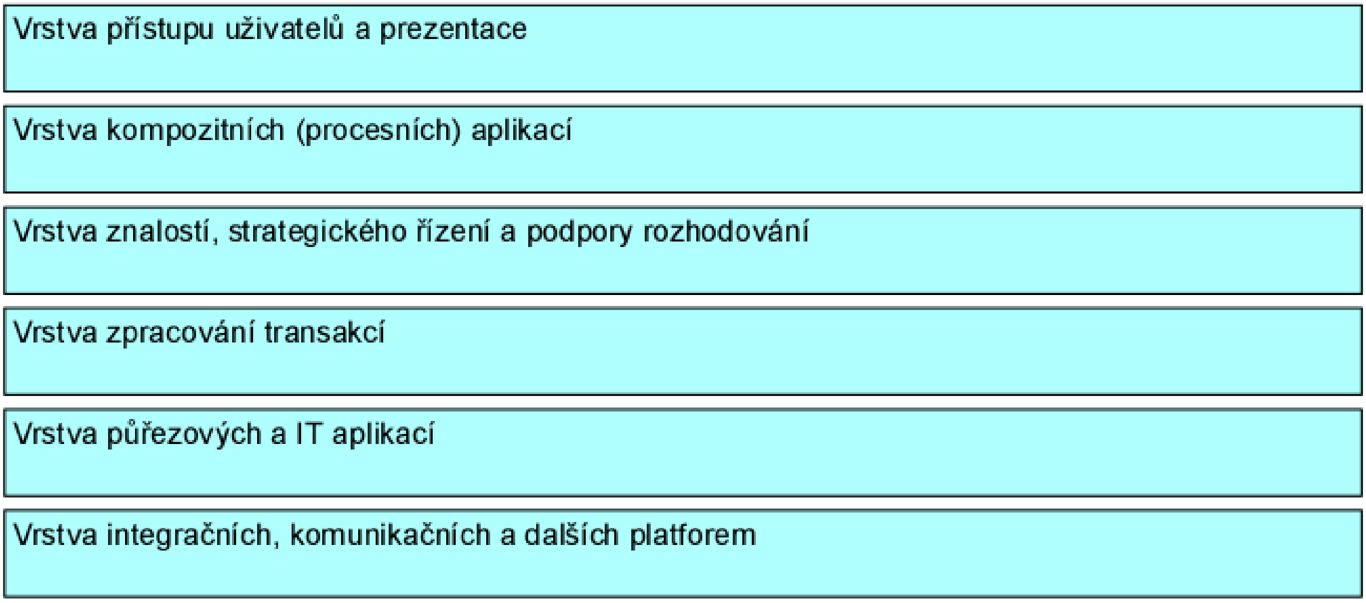
Public administration information systems are used to support the performance of a public administration agenda or agendas. Thus, it must serve as a means for the official to guide him through his official work and to assist him in his official work, to collect and complete the necessary data, to monitor the fulfilment of certain obligations and to offer solutions, but perhaps it should also be able to prepare a draft decision on a given matter. The official should be given a comprehensive tool in the ISVS or AIS that will handle all or at least a significant part of the administration for him/her, so that the official has time to work with the client and to make real administrative decisions where such decisions are needed. In short, the record-keeping role of these IS is changing to a procedural role.

Principles of application classification according to the reference model

Thus, public administration information systems (PIS), as defined by their agency or other laws, usually consist of one or more application components. For the purposes of their management, application components of ISVS and other information systems of the authority can be classified, for example, according to the groups of business functions of the authority they support, according to the degree of sharing of application services and according to the clients of these services, or according to the relationship of the IS to the chain of service of the clients of the public administration.

The authority's CIO and technical administrators of ISVS are required, in cooperation with their subject matter administrators, to create and maintain an up-to-date model of the decomposition of the authority's application components and application functions and its diagram, the so-called Authority Application Portfolio/Architecture Map.

Decision support in managing the life cycle of application components of the VS information systems and at the same time expressing the best practice of their inventory and classification is provided by the so-called Application Architecture Reference Model, which is the basis of the Authority's Application Map.



Vrstva přístupu uživatelů a prezentace

Vrstva kompozitních (procesních) aplikací

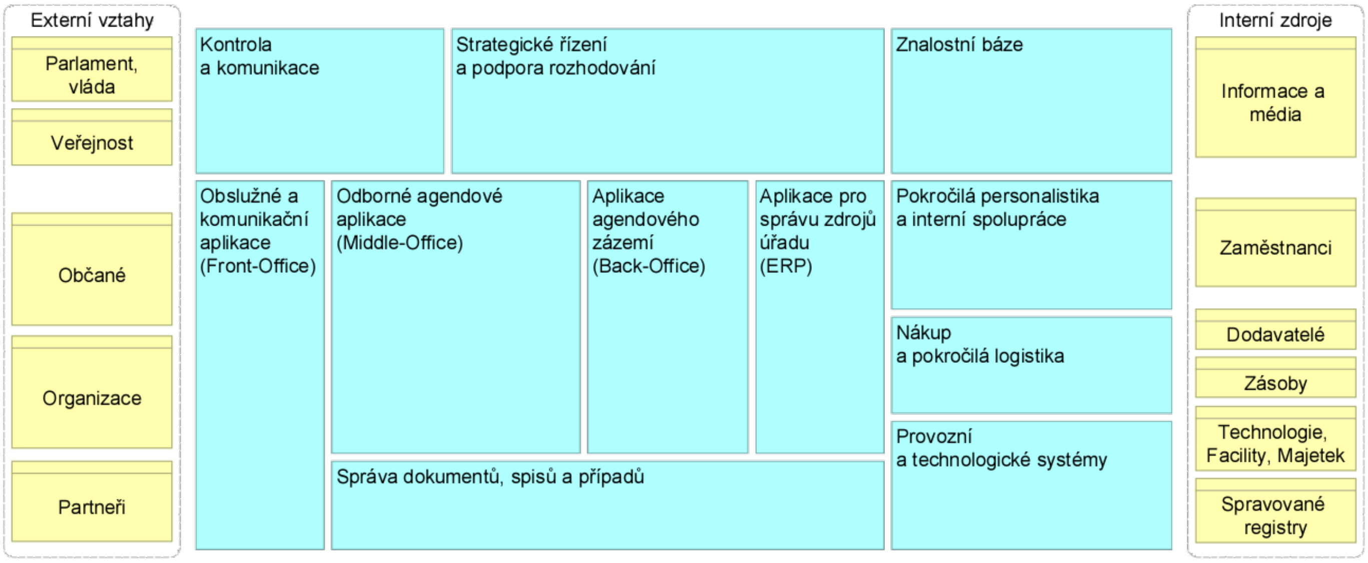
Vrstva znalostí, strategického řízení a podpory rozhodování

Vrstva zpracování transakcí

Vrstva průřezových a IT aplikací

Vrstva integračních, komunikačních a dalších platforem

The division is based on the purpose of the application components from above, starting from the role of user interface and navigation to platforms, completely independent of the types of users and services provided by the Authority. In the application map, this division is applied as layers of vertical dimension.


Externí vztahy
Parlament, vláda
Veřejnost
Občané
Organizace
Partneři
Kontrola a komunikace
Strategické řízení a podpora rozhodování
Znalostní báze
Obslužné a komunikační aplikace (Front-Office)
Odborné agendové aplikace (Middle-Office)
Aplikace agendového zázemí (Back-Office)
Aplikace pro správu zdrojů úřadu (ERP)
Pokročilá personalistika a interní spolupráce
Nákup a pokročilá logistika
Provozní a technologické systémy
Správa dokumentů, spisů a případů
Interní zdroje
Informace a média
Zaměstnanci
Dodavatelé
Zásoby
Technologie, Facility, Majetek
Spravované registry

Further, the division of applications is based on the business logic of the business functions supported, where on the one hand there are functions (services) for external clients, partners and the public, and on the other hand there are functions that support in detail the individual key resources of the authority (knowledge, staff, assets and inventory (and their suppliers), or entrusted registers).

If the law defines for an agency also the IT support for data recording and thus empowers the implementation of an ISMS, it does not imply that this system cannot use some of its components together with other agencies (and agency systems) of the same agency. On the other hand, it is not yet possible, unless explicitly provided for by law, to share application components owned by another authority (or the relevant corporation, i.e. a department, region or ORP) in the ISVS.

This implies a currently feasible requirement to optimize the processes and application portfolio of the authority by using unified or even central shared components of the authority's application portfolio for cross-cutting agency processes (e.g. for customer service at counters, portal self-service, on-site control management, receipt and matching of payments, etc.), transcription of names of persons from countries using a script other than the Latin alphabet) within its office, or central shared application services made available to it by law or regulation at a higher level of government (corporations, central eGovernment).

Where multiple components across agencies are shared in this way within an office, these use not AIFO for external client identification, but preferably some common public client number of the citizen and the organisation within the office's master data system. The AIFO, as a non-public identifier, will only be used when externally exchanging client data within an agency via a back-end integration through the Reference interface of public administration.

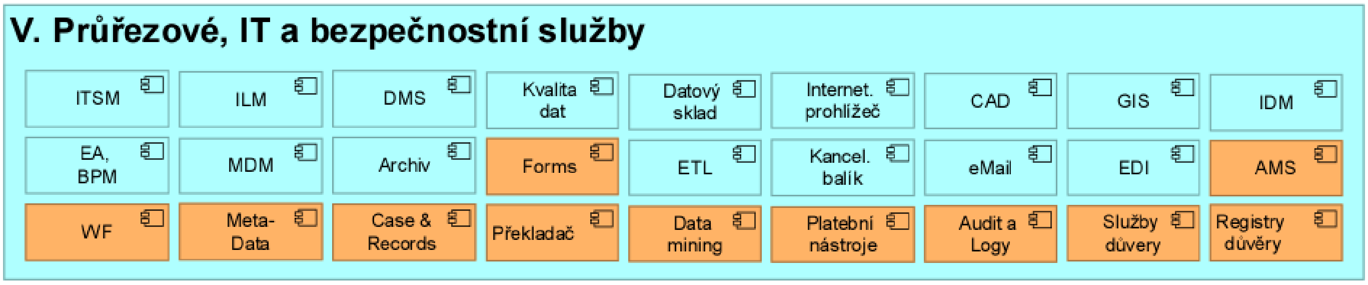
Cross-cutting, IT and security services

The scope and content of applications for service, professional and back-office functions of agendas varies by segment of government. Differences in other categories are minimal, with similar and uniform application functions prevailing.

The content of applications for cross-cutting, IT and security services is presented in the reference model in the form of standard, logical application components. The turquoise components represent the results of generalisation of the authors' previous practice, while the orange components were taken from the EU reference model (EIRA).

It is the responsibility of the Authority's CIO (Technical Administrator) to take into account the similarity of the applications to each other according to their category when deciding whether to consolidate applications or to design application support in categories where it is insufficient or lacking.

A reference model of the application architecture with full details of the classification and with different content of key transactional components for different segments of the public administration (e.g. health, insurance agendas, subsidy agendas, network infrastructure management, etc.) will be released in the following versions NAP.



V. Průřezové, IT a bezpečnostní služby

ITSM	ILM	DMS	Kvalita dat	Datový sklad	Internet. prohlížeč	CAD	GIS	IDM
EA, BPM	MDM	Archiv	Forms	ETL	Kancel. balík	eMail	EDI	AMS
WF	Meta-Data	Case & Records	Překladač	Data mining	Platební nástroje	Audit a Logy	Služby důvery	Registry důvěry

Rules for user interfaces and access to information systems

First and foremost, user interfaces of ISVs and operational systems must be ergonomically optimal to best support appropriate user roles and their performance of external and internal government functions.

- The authority must have all its forms primarily in the authenticated zone of the portal and allow pre-filling of data from the PPDF using guaranteed client identity
- Agency and local portals will be expanded from informational to transactional
- Transactional portal content (forms or portal application user interfaces) must be integrated (federated) with PVS - Citizen Portal
- If a legal regulation or the exercise of competence requires proof of identity, proof of identity using electronic identification may only be enabled through a qualified electronic identification system. This identification is currently only provided through the National Identity Scheme

Except in exceptionally justified cases, such as modelling or GIS tools, or when sufficient Internet bandwidth is unavailable, no business logic shall be included in the user interface, but shall be available uniformly from the application servers for all types of AI used (local client, web client, mobile client). The reason for this is to facilitate uniform maintenance of business logic during constant changes (parameterization) of IS functions.

NAP envisages a gradual unification of the appearance and behaviour of the portal applications of central administrative authorities to achieve a uniform user experience of the client. This is especially true once the elementary services of the authorities are accessible by "clicking" from the citizen's portal. For this purpose, the graphic manual of the Ministry of the Interior

The aim is to enable smaller central authorities and local governments to use the SaaS services of the Citizen Portal in PVS instead of building local portals, in the first step for state administration services in delegated competence, and later also for local government services and the economic activity of the municipality. Therefore, this purpose will be the possibility to graphically localize the services in PVS, while maintaining uniform navigation and operating tools.

Rules for service agency applications (FO)

The target service application functions must be uniform and centralized across the office, department (or corporation) and the state so as to provide a good and uniform "experience" and efficient service to the public administration clients, in proportion to the above breakdown of public administration service channels and their support requirements.

This means that service channel applications of the same type, such as an external portal, must be hierarchically federated or fully centralised. Applications of different types, for example, the user interface for the physical counter and for the portal, must be integrated with each other by using a common application logic for communicating with clients, which is not built into either the portal or the counter SW, but just into the common application SW of the service channels, also called CRM, which in public administration means Citizen Relationship Management.

CRM together with communication technologies (web, mail, phone, chat, SMS, DS, etc.) will ensure a unified multichannel service (multichannel, omnichannel).

A substantial part of the agency business logic is drawn and presented by the service channels from the agency-specific (MiddleOffice) systems and from the agency back-office systems (Back-Office).

Rules for Expert (Specific) Agenda Applications (MO)

In all cases where a public service in an agenda is to be provided in a delegated competence or in its own competence across a branch network (territorial deconcentrations - FŘ, OSSZ, District Courts), it is the duty of the central administrative authority reporting this agenda to act as the substantive administrator of its ISVS and to provide for such an agenda a central agenda information system covering the specialist agenda functions (MO) or the back-office functions (BO).

This system must be accessible via the State's network infrastructure at all public administration service points, both agency and universal. It must be capable of integration with local and national application components for client servicing (FO), for local common back-office functions (payments, file management, etc.) (BO) and, in particular, it must be capable of integration with the local filing service, local client accounts and the local EkIS of the office.

The user interface of these central AISs must be sortable and selectable from a single transactional navigation in the central portal of the civil servants (public administration intranet) and (temporarily) in the local intranet of the authority.

For the application architecture of the authority, then, the authority must for a logically centralised AIS either:

1. use this centrally shared application component, i.e. provide the Authority's users with user access to this component via the JIP/KAAS and integrate this component on the Back-Office with other necessarily local Authority components such as the Authority's filing service or customer service management system.
2. (b) Use the Authority's own standardised agency system for this agenda (or multi-agency), integrated on a central shared component, serving as its "fat client" but with full responsibility for its legislative updates.

For both options, there is a binding architectural requirement for both the subject administrator of the central system and the local authority that neither internal staff nor the external client may enter any data twice in the provision of a single service for this agenda.

The aforementioned centralised specialist agenda application must be provided by the administrator (agenda submitter) including a self-service citizen/business customer portal ensuring compliance with the Once Only principle. At the same time, this central application publishes the agenda data registered in the agenda to the PPDF and publishes the public data of the agenda to the VDF as open data.

Rules for Agenda Background Applications (BO)

If an office is active in multiple agencies that all lead to similar agenda background (BO) functions, e.g. file management, fee receipt, benefit payment, etc., it will use a shared solution for these functions (file service, balance sheet accounting, ...) and should gradually unify legislation and processes in these function areas. From a business point of view, it should be borne in mind that, for example, tax administration differs from general administrative procedures in its basic concept, and therefore there will always be situations which, although acceptable for the administrative process, would be completely unacceptable for tax administration. From an

ICT perspective, however, it is about adapting a particular solution to a particular situation/problem - also known as "parameterisation".

The key component of this area from the perspective of both clients and the authority is the component for maintaining the client tribe and their accounts receivable/payable (balance sheet). These components should be central and consistent across agencies in each office.

Shared solutions for the agency back office can be shared not only within the office, but also across the department/corporation or nationally as soon as it is legislatively and technically feasible and available.

The electronic filing system is so fundamental and so specific to the processes of the Office that, although by definition it is an agenda background (BO) tool, a separate category has been created for these systems and the rules for them, see below.

Rules for file service applications, case management and workflow

Different procedural requirements for the management of client cases and files, clearly related to clients (data owned by clients and lent to offices for management) and OVS internal management cases and files (no client links). It is advisable to be aware of these differences and to adapt the links to AISs on the one hand and the links to operational systems (ERP, HR, purchasing, etc.) on the other.

From the point of view of the Archives and Records Management Act, there is a category of 'designated originators' who are obliged to carry out records management in electronic form in electronic records management systems. Thus, despite the differences mentioned in the previous paragraph on links, each designated originator must establish, operate and use an electronic filing system shared by all the agencies and departments of the Office for the registration of all documents, unless it is not worthwhile from the point of view of good administration to use a separate filing system for an agency under the Archives Act. In this case, both (all) records must be integrated in accordance with the National Standard. Similarly, and appropriately, non-designated originator authorities should take a similar and proportionate approach to the above issue with regard to architectural principles.

Where an authority maintains multiple documents for its agencies on the same matter, it is required to record these documents in a 'file'. Therefore, it should then consider a file management function as a common and shared component. Moreover, if more and more agendas are gradually being computerised and automated in their processing as a so-called electronic document workflow, the office should have a single shared component for managing this workflow over electronic documents. The electronic workflow tool should support both basic types of workflow:

- transactional workflow - where a reference to a transaction in progress in an agency or operational IS is passed between staff, together with links to the corresponding documents or files that are attached.
- document workflow - where only the reference to the document or file in the file service is passed between workers, or where the document or file is passed via workflow

The user-client for the workflow should (o) be concurrent (optimally):

- the user interface of the AIS application, the operational system or the file service, depending on the type of workflow, see above
- a common interface accessing the "workflow-inbox" in the Clerk Portal, where links to all ongoing workflows are provided
- an interface to the clerk's mailbox allowing workflows of both types to be handled"

Rules for the knowledge systems category

Knowledge systems in the Authority must be consolidated so that all Authority information and knowledge, except for individual agency performance and classified information, is available for training and service performance support to all Authority staff, with common information retrieval on the Authority's intranet / Clerk Portal..

For information systems that provide information on current, historical and pending legislation, only systems and functions that are not supported by the central eCollection/eLegislation system may be operated in offices.

Identity Management (IDM) Rules

Each office is obliged to consider in its architecture the acquisition of a solution for central management of identities and user permissions (also called IDM (Identity Management) or IAM (Identity & Access Management)) of the office and its integration with the personnel system of the office on the one hand and with the central unified identity space of the civil servants of the Ministry of Justice on the other hand (currently the JIP/KAAS solution).

- Obligation to connect client identification and authentication to a qualified system, which is currently only NIA
- Obligation to link identification, authentication and authorization of officials to JIP/KAAS
- Recommendation to implement a central identity management of the office (IDM), linked for officials to HR (HCM)

Rules for integration platforms

A common problem with ISVS administrators is that these information systems are built as stand-alone blocks that are not properly and correctly linked and integrated with other information systems and components in the office. This needs to be kept in mind when setting up the initial architecture and consistently ensure these integrations, in the form of open and above all described and replaceable interfaces, not as black boxes (peer-to-peer, P2P) on vendor agreement.

Every public administration information system must be integrated with:

- An electronic filing system - for the management of the filing service, or with a separate document register for professional document management and for document-related operations, where the above systems are tools either for the performance of the filing service or for the registration of documents. These systems must then always comply with the National Standard under Act No 499/2004 Coll.
- Operational systems of the IDM and monitoring type
- Auditing and logging systems - to ensure logging of the handling of data recorded in the ISVS, including but not limited to personal data
- Economic information system to ensure financial operations and their recording - for systems for agendas where funds are either paid or received.

The preferred way of integrating applications is to use a standard integration platform (also Enterprise Application Integration, hereinafter also referred to as "EAI", or synonym Enterprise Service Bus, hereinafter also referred to as ESB), which replaces the P2P integration of the authority and provides functions for, in particular, asynchronous integration (not waiting for a confirmation of the entry into the database or a response), queue handling, logging, etc.

Each authority will use its own or shared EAI connected to a central eGSB / ISSS.

In line with the NAP, these rules assume a multi-tier hierarchical structure of integration platforms.

A central integration platform eGSB / ISSS is built for the involvement of authorities in sharing within the interconnected data pool. The authorities preferably connect to it via the corporate integration platforms of the ministries (regions, ORP) or via their own EAI, if they have one.

The corporate EAI serves primarily for internal integration needs within the chapter or public corporation, as an external integration for the department or subdivision office, and as a shared service for subordinate organizations of the corporation for which it is not convenient to build an EAI of their own.

Local integration platforms are built by those authorities for which the investment in their internal and external application integration platform is economically and operationally advantageous due to the frequency and complexity of the interfaces or the volume of messages transmitted.

Rules for systems publishing and using open data

Data recorded in the ISVS for which it is valid shall be published in complete form as open data:

- the obligation to publish in open data form is expressly provided for by law; or
- it is an ISVS the content of which is wholly or partly public and the previous case does not apply. In this case, an assessment must be made as to whether disclosure of the data in this form will result in a disproportionate interference with the right to the protection of personal data or significantly increase the possibility of a breach of the security of the CR; or
- it is data that could be provided on the basis of a request under the regulations governing free access to information (cf. Section 5(7) of the Act on Free Access to Information) and at the same time it is not the case in the previous two cases. In such a case, the data in the form of open data shall be disclosed only to the extent that it could be disclosed if it were the subject of a request under the laws governing free access to information, while an assessment must also be made as to whether disclosure in this form would entail the possibility of undermining the security of the Czech Republic.

Publishing data from ISVS as open data implies an obligation to provide it to all data processing professionals (programmers, data analysts and journalists, scientists, students, etc.) and to the OSS in a form that actively supports its machine processing and replication and, in particular, does not impose any (technical, legal or economic) obstacles to this purpose.

In the case that data in the form of open data are published from the ISVS, the possible legislative requirement to provide public remote access to these data is also fulfilled.

The sharing of public data recorded in the ISVS between public administrations must be ensured through open data in the VDF. The PSC whose data records in the ISVS it manages are primary records must publish them as open data. A VAS that uses these data in the ISVS it manages must retrieve them as open data if they are published as open data.

The same data can only be published as open data once in a public administration. Where data held in an ISVS are transferred to another ISVS for the purpose of collecting data from different PSIs and subsequent publication, the transferred data shall not be published as open data from the first ISVS but only from the second ISVS. The publication shall be ensured by the administrator of the second ISVS. In the case of central application services, the data maintained are provided as open data by the administrator of the central application service and the local authority no longer publishes its relevant data as open data.

Rules for the use of SaaS eGC services

SaaS eGC services can theoretically be used to replace any service on the application layer of the authority's architecture, or the internal implementation of a given service ("function" in terms of the architectural model) can be replaced by a SaaS service. SaaS eGC services will be subject to the same architectural requirements as on-premise ISVs and security requirements corresponding to the security impact assessment level of the ISV.

The practical use of SaaS eGC services is expected to be mainly and firstly in the categories of support systems, filing services and agency background, and in the case of municipalities also in the category of agency applications for self-government.

IS VS Data Architecture Rules

The description of centrally provided systems and their services, functional units and thematic areas is described in Description of shared services, functional units and thematic areas of public administration in the Czech Republic.

Rules for individual shared services, functional units and thematic areas are described in Methods for the use of shared services, functional units and thematic areas of individual offices.

The incorporation of the rules of this architecture layer shall be described by the authority in its information concept.

The IS VS data architecture is formally part of a single layer together with the application architecture. Here they are described separately because of the emphasis on the work and rules for the system and the work and rules for the data/data they work with.

These rules do not currently prescribe any mandatorily standardized individual elements of the public administration data architecture, except for those that are progressively published as part of the CR's reference and agency data.

A fundamental requirement of the information concept is the adoption (application) of a common approach to data architecture for all public administration bodies. The administrator of each information system must know:

- **What** data (data) is present in the public administration information systems that are used to support the agenda
- **Where** this data comes from. i.e., whether it is data generated as part of the agenda activity, obtained from basic registers, agenda sources, used from other agendas, from open data pools, etc.
- **To whom** the data is provided (whether under another agency's data use authorisation or on request)
- **How it ensures the protection** of the data, both in accessing the data and in keeping records (logs) of those accesses and protecting those logs.

Thus, the requirements for changing access to **data** architecture are applicable to all ISVs in the state.

Any ISVS that contains any data holdings is required to provide (the ISVS administrator must):

1. **Reference -** identify all subjects/objects held in the basic registers (natural persons - ROB, legal entities - ROS, address points and other territorial elements - RUIAN) and start receiving notifications of changes to data on these subjects/objects both from the basic registers and from other agency sources.
2. **Unambiguity -** split the data pool into parts
   1. **Reference data** - must be consistent with the basic registers
   2. **Agenda data** - come from editors of basic registers (e.g. Population Register) or other agenda information systems (e.g. Driver Register) within the agenda are only used
   3. **Agency own data** - data created within the agenda (can be further provided to other agendas as agenda data)
3. **Security** - must be ensured both in terms of protection of personal data and security against loss or unauthorised alteration of data

This method of data architecture management must be applied by the Authority not only for individual ISVS but in aggregate for the entire OVS, its Authority and the Corporation.

The Chief Information Officer of the Office and the technical administrators of the ISVS are obliged, in cooperation with their subject matter administrators, to create and maintain an up-to-date model of the basic (conceptual) decomposition of the Office's data and its diagram, the so-called Data Architecture Map of the Office.

Detailed reference models of the data architecture, elaborating the rules mentioned here, including their graphical representation, i.e. the Map, are established and published by the OHA of the Ministry of Interior, in cooperation with the OeG and organisations representing individual levels of state and local government.

Data distribution / classification in public administration

The ICR requires authorities to maintain up-to-date classifications of the basic information (data) objects of the authority's architecture. These identified objects must be classified into the following categories and must be treated in the application architecture in a manner appropriate to their classification.

All the data managed in the IS of the Authority, constitute the so-called **data pool of the Authority**. The basic existential (static, card catalogue) data on subjects (clients, suppliers, employees, etc.) and on public administration objects (registered vehicles, cultural monuments, livestock, property of the authority, etc.) constitute the so-called **data trunk of the authority**, or its master data. On the other hand, data on procedures (operations, actions) with or over public administration objects are called **transaction data of the authority**. Trunk and transactional data are the two most important components of the Authority's data holdings; other categories of data are presented below.

A fundamental requirement of the information concept in terms of classification of data in public administration is the introduction of the concept of **agenda data**. Currently, the concept of reference data is already introduced in the Basic Registers Act (Section 2). An agency data has a similar data quality when it is used, but its quality and guarantee is guaranteed by its provider, which in most cases is agenda notifier. This includes, for example, data relating to drivers, vehicles, education of natural persons, qualifications of natural or legal persons to carry out activities according to the law (doctor, educational institution, accreditation centre, etc.).

Applying the above principles, the data held in the data pool of the public administration information system (agenda), and collectively in the data pool of the authority, can be divided in several respects. The primary aspect is the classification of data objects in terms of responsibility for their validity, see above under **uniqueness.**

In addition, individual data objects in the ISVS and Authority data pool can be classified according to their type (in terms of stability, dynamics or treatment):

- Master data
- Transactional data of individual proceedings in agencies
- Documents
- Spatial data
- Analytical (aggregated, anonymised or otherwise transformed) data
- Signal data (real-time data stream)
- Metadata of spatial data, analytical data, documents and multimedia objects
- Operational and security audit data (logs)
- Parameterization data, control dials (languages, currencies, zip codes, tax types, rate categories, fuel types, vehicle categories, NACE, etc.)
- Program code data (source code in database)

Another fundamental classification of data objects, not only in the data trunk but also in the other data objects mentioned above, is according to the content of personal data:

- Containing personal data

- Containing special categories of personal data (formerly known as sensitive personal data)
- Containing no personal data.

The basic tool for the management of data objects about subjects and objects of law contained in the agenda data trunk is the Register of Rights and Obligations. When declaring an agenda, it is necessary to list the data maintained in the agenda according to Act 111/2009 Coll. on Basic Registers, § 51 (5) (h). These documents are used for the notifiers of other agendas who register a request for the use of these data according to point j) of this provision.

The RPP maintains information on the data provided and used in this way from a legislative point of view, i.e. as specified in the relevant legislation. From a technical usage point of view, the ISVS administrator that provides the data via eGSB / ISSS is then required to publish the corresponding technical regulation as an XML template within the WSDL of the usage regulation of the published services eGSB / ISSS.

Thus, from a technical point of view, the binding prescription is how data is published for use on the Basic Registry Information System and eGSB/ISSS interface. This unifies the reference interface of the public administration and ensures a clear technological presentation of legal concepts in terms of the data transmitted.

At the same time, it is **not** foreseen that data can be exchanged between public administration information systems outside the reference interface.

Rules for codebook data

Anyone providing data in a linked data pool is obliged to publish the associated codebooks as open data in SVDF. These are codebooks that they create as part of their activities, not codebooks used in the maintenance of the data.

Thus, for example, if the Country Codebook (CZEM) is used in the data filling, then the administrator does not publish this codebook, but only states that it uses the codebook published by the Czech Statistical Office.

Therefore, for each codebook it must be known:

- The administrator of the codebook (OVS)
- Place of publication of the codebook and its technical format
- Method of updating the codebook

Dictionaries registered according to the above principles are **binding in the exchange of data between agencies**.

Rules for reference and agency master data

An authority may, or must, use reference and agency tribal data within its local information system for the execution of an agenda. This data may be used on-line when needed by querying the reference interface (ISZR and eGSB/ISSS), or a copy may be stored for subjects and objects maintained within the agenda.

Agenda data:

- It is created in the given agenda by its activity (defined by the relevant law) and the administrator of the agenda is responsible for its correctness - agenda resource - current state
- It is used in other agendas - current status (the agenda is authorised to use data of other agendas in its activity)
- Its use from an agenda source ensures that it is done "officially correctly" similar to the reference data - legislative addition required

Responsibilities in terms of agenda data - intent:

- The administrator (of the agenda) registers the data with the Register of Rights and Obligations as agenda data
- Controller publishes the data within the selected context with a link to the subject/object via eGSB / ISSS
- The administrator publishes changes to the agenda data
- The administrator accepts complaints about the state of the agenda data
- The agenda using the agenda data registers this request in the Rights and Obligations Register
- Agenda uses the data via eGSB/ISSS
- If the agenda stores this data in its data pool, it keeps it in compliance by subscribing changes
- If, during the operation of the agenda, a doubt is detected about the correctness of the data, then it notifies the data controller

How efficiently the reference and agency data from the reference interface is used is critical to the efficiency of the administration. At the same time, it is necessary to ensure architecturally that the performance of the public administration is as resilient as possible to failures of central components.

1. If these data are not used in large quantities within an agenda, then the most efficient and secure use of them is based on online queries at the time of need. The data is then not permanently stored in the agenda data, but only the shape of the data retrieved at the time of the query and in the context of the purpose.
2. If these data are used by the agenda in large quantities, or if there is a risk of delay in the event of unavailability of central systems, then it is efficient to maintain a local copy of the reference and agenda data on the subjects and objects of the agenda for the purposes of its execution. In this case, systematic maintenance of this data is absolutely necessary so that it is **consistent** with the data held in the underlying registers and agenda sources. To this end, it is necessary to use the notification process to change and update the data on the subjects and objects for which the change has been notified.

The principle of notification is fundamentally of the **pull** type and without passing data during notification. Thus, the agenda using the data requests a list of subjects or objects for which the data has changed in the past period (typically one day). It then uses this list to actively query the data source to retrieve data according to its permissions. This ensures that during notifications no data can be passed that the agenda does not have permission to. At the same time, when querying a natural or legal person, an entry is created in the basic registers and the right holder concerned is informed that the agenda has updated the data about him in its data stem.

In case the OVS uses more than one own (local) agency information system and uses reference and agency master data, a local master data management solution must be implemented which, after the initial identification, keeps the agency master data up-to-date by receiving notifications from the PPDF and does not burden the linked data pool with continuous on-line queries. Personal data obtained in this way is stored outside other agency information systems and is only used by individual systems when necessary. This ensures the separation and security of personal data with unquestionable auditing of access to personal data.

Open Data (OD) Rules

The following rules apply to the publication of VS data in the form of open data for the OSS:

- When publishing public information for general public use, the rules set out for Open Data (OD) must be followed.
- When publishing public information intended to be shared between public bodies with each other and for sharing public data between public and private bodies, the rules set out for the Public Data Fund (PDF) must be followed.

In particular, open data must meet the legislative requirements within the meaning of Act 106/1999 Coll. on Freedom of Access to Information, taking into account the Data Protection Act and the GDPR. In addition, the method of publication must fulfil the following conditions, which must be ensured by the OSS publishing the open data:

- Open data must be catalogued in the NKOD in the form of individual datasets.
- The dataset must consist of logically related data, logically organised into records with the same data structure.
- Selected data or entire records that can be published must not be deliberately removed from the dataset.
- The dataset must be provided in the form of one or more downloadable data files from the Web, which we call dataset distribution.
- Dataset distributions may differ from each other only in their data format, not in their content. Each distribution must contain the complete set of records that make up the dataset.
- At least one of the distributions must be provided in an open and machine-readable format within the meaning of the definition of open data under Section 3(11) of Act No.106/1999 Coll. and must:
    - Be provided with terms of use that do not restrict any (legal) use of its content, in particular, they must not prevent commercial use or require user registration.
    - It must be provided without undue hindrance. It is not possible to make access to the distribution conditional on registration, contract, application key, login, etc. Access to the distribution may be restricted to the subject only if and for as long as his behaviour in obtaining the distributed dataset shows signs of a cyber-attack.
    - Must be published according to open formal standards within the meaning of Section 4b(1) of Act No. 106/1999 Coll. on Freedom of Access to Information, published on the Open Data Portal (POD).
- Each distribution in an open and machine-readable format must be accompanied by a logical data schema expressed in an appropriate and commonly used language for describing data schemas, if such a language exists for the format. The logical data schema describes the representation of the data structure of the records constituting the dataset in the appropriate format. A distribution must be valid against its logical data schema.
- The dataset shall be documented in detail, in particular to avoid misinterpretation of its contents as far as possible. In the event that some data or entire records have been removed from the dataset prior to its publication due to the impossibility of publishing them, this must be documented and justified. Where the dataset is an anonymised form, summary or statistic of the source data, the method of anonymisation or creation of the summary or statistic must be documented.
- The content of dataset distributions must be updated according to the frequency declared by the OVM when cataloguing the dataset in the NKOD.
- Only backward compatible changes to the data structure of the records comprising the dataset are permitted. Changes to the data structure must be implemented in the logical data schemas of the distributions.
- In the case of changes that are not backward compatible, a new dataset must be created and the original distribution must no longer be updated.
- For datasets whose distributions are no longer updated, the availability of their distributions must be ensured for the longest possible period of time, but at least 3 years.

Rules for public data holdings data

In addition to the above conditions for open data, a dataset published as open data in the VDF must meet the following additional conditions to ensure usability and confidence in the data in the VDF:

- Elements defined by logical data schemas distributing the dataset whose semantics are significant must be linked to the concepts of the semantic vocabulary of terms in order to harmonize the semantics of the dataset according to the designated OFN published on POD.
- In the case of duplication of published datasets or addition of data by different publishers to the same published entity, links to already published data in the VDF must be added. The obligation to complete the links falls on the publisher who publishes the additional data.
- For each dataset published to the VDF, information about the notification mechanism of changes according to the corresponding OFN listed on the POD shall be provided.
- The OSP publishing the dataset must ensure and guarantee the availability of the dataset distribution in an open and machine-readable format for all OSPs using it in the execution of their agendas.

- The administrator of the ISVS from which the dataset is obtained is responsible for the factual correctness of the content of the dataset. This means that it is responsible for:
    - the accuracy of the individual records making up the dataset and the individual data that make up the dataset,
    - the timeliness of the published datasets,
    - the regular updating of datasets,
    - forwarding notifications of updates to the notification HUB.

Analytical Data Rules

Any agency that by law maintains primary individual record data on subjects or objects of law in its agency systems may create anonymized statistical data from that data for agency management and other public use.

The anonymised statistical data shall be sortable according to all parameters (keys) which are not specifically protected data and do not give rise to the possibility of profiling.

Statistical data may be produced with an appropriate period according to the nature of the data recorded in the primary register (day, week, month, quarter, year). Data which cannot otherwise be published for reasons of data protection will be published as statistical data after the necessary adjustments (e.g. aggregation) have been made. Statistical data shall be produced in such a way as to preserve the information value of the original data as far as possible.

Statistical data produced in this way must be published as open data and may also be published on the Authority's portal as visually readable data.

Authorities whose specific agency laws do not foresee the production of statistical data and its use for the management and optimisation of the performance of the agenda and for publication as open data must seek appropriate legislation.

Statistical data of the same (or very similar content) can only be created once in the public administration, therefore the administrator of the agenda information system of the primary register of the relevant subject or object of law and the relevant data is responsible for this.

The statistical data that the authorities now legally mandated to collect such statistical data may obtain from their primary records may not be duplicated by collection from the subjects.

Spatial Data Rules

Any agency information system managing spatial data that may be shared within a linked public administration data pool must:

- Be described in terms of content up to the level of data elements in the public administration information system up to the level of data elements. The data element corresponds to the spatial data class in geographic information systems.
- Publish spatial data sharing services
- Spatial data elements that are related, similar or identical to RUIAN elements shall contain the RUIAN element identifier (e.g. digital technical map buildings, address locations of properties affected by the agenda, etc.).

Hierarchy of data use obligations according to their binding nature

1. Linked data pool
    1. Reference data from basic registers (using [ISZR services])
    2. Data published by the agencies and their AISs (used eGSB / ISSS)

2. Public Data Pool
    1. Public registers and lists published in a way that allows remote access)
    2. Open data from ISVS published and with metadata written in NKOD)

IS VS technology/platform architecture rules

> The description of centrally provided systems and their services, functional units and thematic areas is described in Description of shared services, functional units and thematic areas of public administration of the Czech Republic.
>
> Rules for individual shared services, functional units and thematic areas are described in Methods for the use of shared services, functional units and thematic areas of individual offices.
>
> The incorporation of the rules of this architecture layer shall be described by the authority in its information concept.

IT Technology Architecture Classification

The IT technology architecture (also referred to as "platform architecture") is the layer dealing with the technologies that support applications, systems and, in general, elements from the application architecture with their functionalities and services. The areas of platform architecture can be divided into:

1. Computing power,
2. Data storage,
3. Endpoint devices (Firewall, Switch, generally active elements).

On-Premise Architecture Design and Utilization Rules

All IT technology, with the exception of internal users' end-user input/output devices, must be housed and operated in dedicated facilities, also called server rooms or data centers, conforming to established standards.

Standards for server rooms and data centres will be issued by the MoI in cooperation with public administration security organisations and professional IT organisations.

According to the ICRC, the occurrence of so-called grey IT, i.e. applications and platform software and HW, acquired or located or used in the professional units of the OSS without compliance with the central oversight (governance) of the authority's IT unit, is unacceptable.

If it is uneconomical or technically or staff-wise impossible for some small authorities to comply with these rules, the only option is to entrust their IT solutions to the care of other public administration organisations where the rules will be complied with and use IT support for their public administration processes as a service.

Rules for the use of PaaS and IaaS eGC services

PaaS and IaaS eGC services can be used to replace any service at the technology layer of the authority's architecture, or the internal implementation of a given service ("function" in terms of the architectural model) can be replaced by a PaaS or IaaS service. PaaS and IaaS eGC services will be subject to at least the same architectural requirements as on-premise platforms. For eGC services and on-premise, the security requirements corresponding to the security impact assessment level of the ISVs using these platforms shall be the same.

The practical use of PaaS and IaaS services is expected mainly in the form of groups of services corresponding to the operational platform of a specific ISVS or operational information system, or a clearly defined part of it (e.g. web front-end), either at the level of a fully managed technology platform including OS management (PaaS) or at the level of virtualised computing and disk resources (IaaS), which the Authority will manage in-house or using third party services. From an eGC perspective, the use of PaaS services is preferred to achieve a higher level of efficiency.

Another example of the use of PaaS services is the use of fully managed database or application server platforms, including the provision of software licences.

Rules for Active - Active mode of individual compute nodes

If compute platforms are built in Active - Active mode it is essential to have a minimum of 3 sites provisioned, with 2 sites for the compute platforms themselves and a third site to house the technologies that monitor the remaining sites and decide their behaviour.

IS VS Physical and Communication Infrastructure Rules

The description of centrally provided systems and their services, functional units and thematic areas is described in Description of shared services, functional units and thematic areas of public administration of the CR.

Rules for individual shared services, functional units and thematic areas are described in Methods for the use of shared services, functional units and thematic areas of individual offices.

The incorporation of the rules of this architecture layer shall be described by the authority in its information concept.

KIVS/CMS is a system whose primary purpose is to provide controlled and registered interconnection 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. KIVS/CMS can thus be called a private network for the performance of public administration on the territory of the state. KIVS/CMS as a private network of public administration uses dedicated or leased network resources for secure interconnection of public administration officials (OVS) working in public administration agencies with their remote agency information systems, for secure network interconnection of agency systems with each other and for secure access of individual OVS to the Internet.

OVS and SPUUs access eGovernment services, such as connected-data-fund, exclusively via CMS in one of four possible ways:

1. Through the Regional Networks (currently in the Vysočina, Pilsen, Karlovy Vary, Zlín and partly Pardubice regions + others 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 (KIVS) 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 (ISVS) only via the KIVS/CMS.

With the exception of the so-called operational information systems, which are 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 through 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.

Specific rules for office architecture

Rules for architecture according to the size and capabilities of the authorities

For Type 1 and Type 2 municipalities, the vision for the architecture of public administration is as follows:

The IT architecture of a Type 1 and Type 2 municipality (up to a certain size, see below) consists only of end-user devices, the network infrastructure is provided by the county as a shared service, the application services for the state administration in delegated competence are provided by the reporting agencies, and the application services for the local government competence are provided by the higher level of local government (ORP, county) as a shared service.

The concept for local government is thus based on the following principles:

1. The NAP is binding for all local government entities that have more than 10 facilities.
2. Information systems for activities and agendas under delegated competence are taken over in full from central authorities. Each local authority is responsible for its own activities.
3. Entities with less than 10 devices purchase only user HW and SW, i.e. these end devices, SW products for the performance of public administration are provided as a service by the entities in whose administrative district they are located.

Rules for architecture according to the position of the authority in the structure of the Czech Government and its relation to shared services

Authorities, responsible by law as subject matter administrators of shared elements of eGovernment services, consider these elements entrusted to them as an integral part of their authority's architecture. In addition to the overall architecture of their offices, they also model the architecture models of these entrusted shared elements independently, even at the level of detail of the so-called solution architecture. These authorities also model so-called extended models for these elements, i.e. models that also include type (logical) architecture elements on the side of the type (typical) consumers of their shared services.

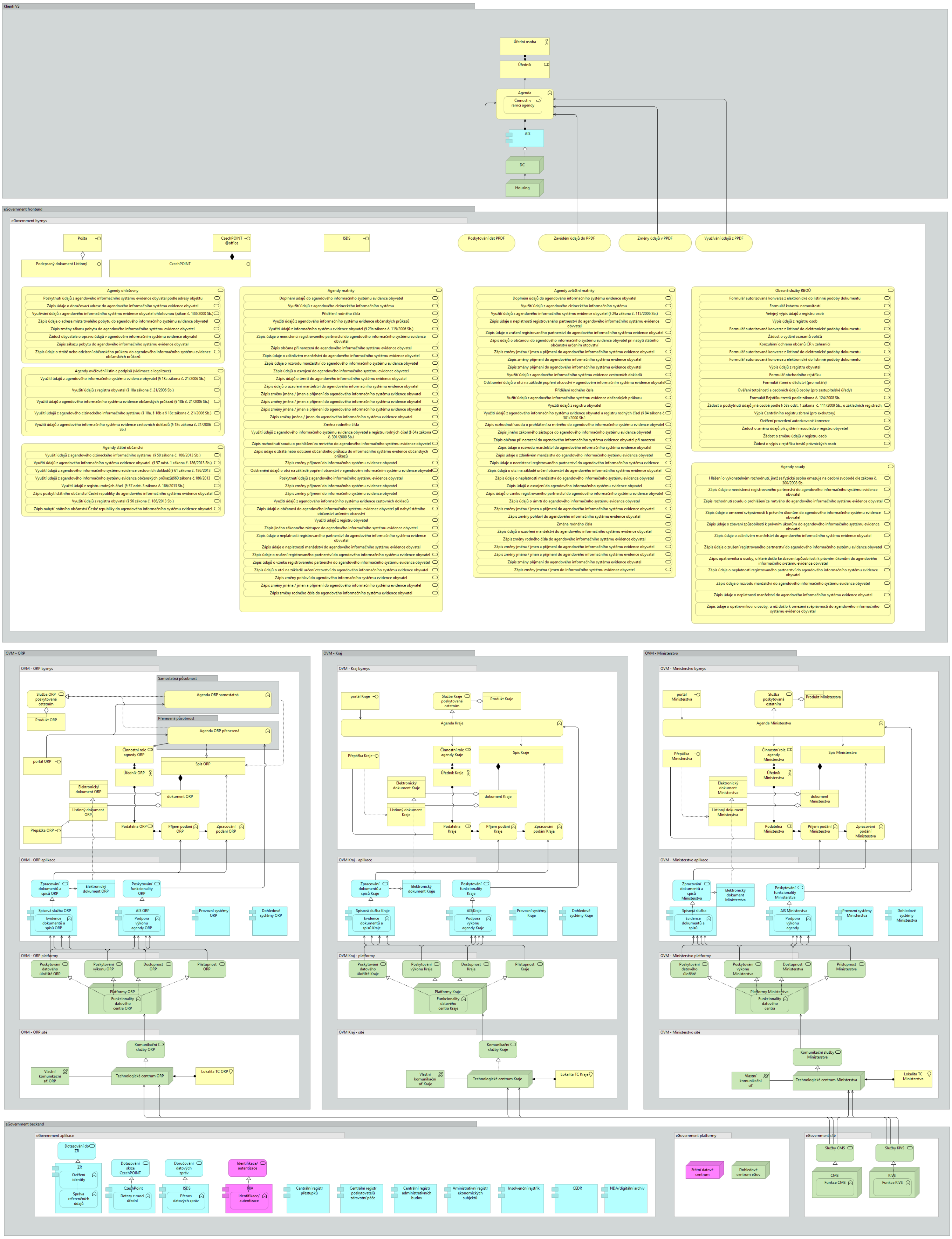
The authorities using the services of the shared eGovernment elements do not model these information systems as active elements (application and technology components and interfaces) in any case - they do not have them within their scope of responsibility, but exclusively as services (business, application or technology and infrastructure - depending on the need for expression) and interfaces of their own components to these systems.

Authorities responsible for implementing and operating central registries and AIS for services under delegated responsibility, model their authority architecture to include these systems as a matter of course. At the same time, they are also obliged to create and maintain so-called extended models, i.e. models that also include type (logical) architecture elements on the side of the type (typical) subscribers of their shared services, showing all the necessary context (e.g. integration of the central AIS to the local eSSL and EkIS).

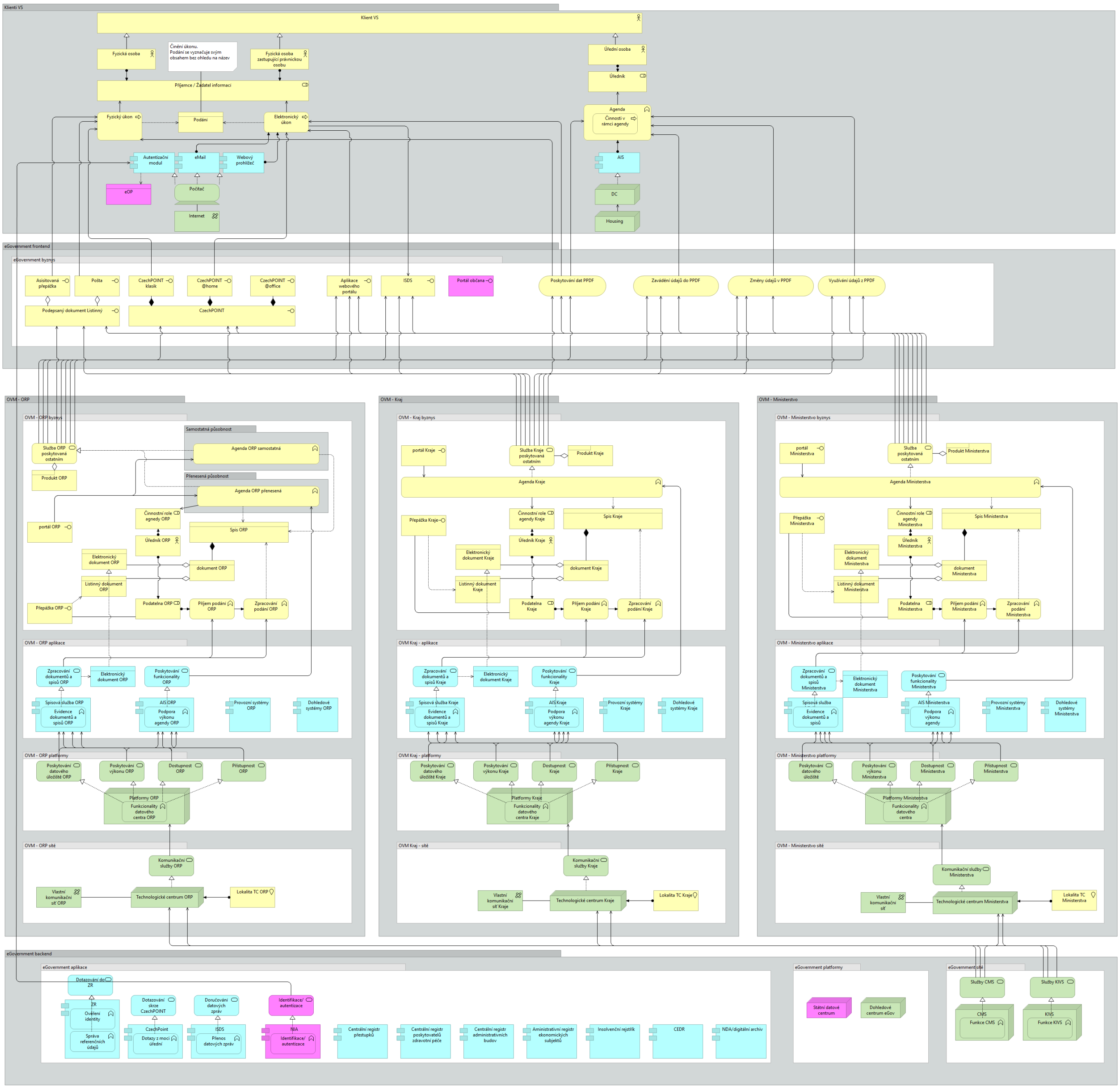
The authorities using these central AIS for services under delegated responsibility do not model these as active elements in their authority architectures (they do not have them under their responsibility), but as services of these systems and interfaces of their own components to these systems.

Views of the overall composition of the public administration architecture

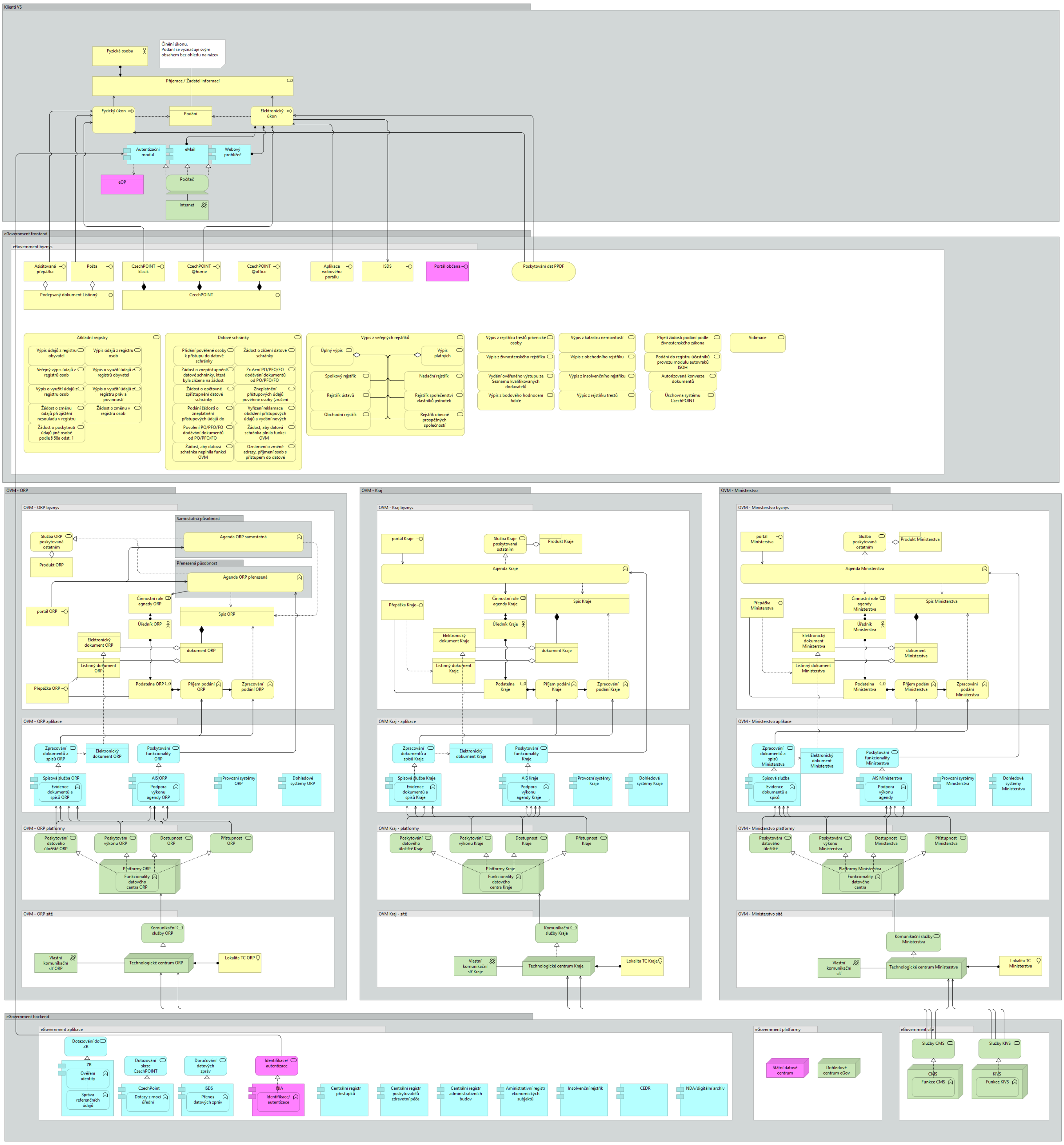
Clerk's view


Klienti VS
Úřední osoba
Úředník
Agenda
Činnosti v rámci agendy
AIS
DC
Housing
eGovernment frontend
eGovernment byznys
Pošta
CzechPOINT @office
ISDS
Poskytování dat PPDF
Zavádění údajů do PPDF
Změny údajů v PPDF
Využívání údajů z PPDF
Podepsaný dokument Listinný
CzechPOINT
Agendy ohlašovny
Poskytnutí údajů z agendového informačního systému evidence obyvatel podle adresy objektu
Zápis údaje o doručovací adrese do agendového informačního systému evidence obyvatel
Využívání údajů z agendového informačního systému evidence obyvatel ohlašovnou (zákon č. 133/2000 Sb.)
Zápis údaje o adrese místa trvalého pobytu do agendového informačního systému evidence obyvatel
Zápis změny zákazu pobytu do agendového informačního systému evidence obyvatel
Žádost obyvatele o opravu údajů v agendovém informačním systému evidence obyvatel
Zápis zákazu pobytu do agendového informačního systému evidence obyvatel
Zápis údaje o ztrátě nebo odcizení občanského průkazu do agendového informačního systému evidence občanských průkazů
Agendy ověřování listin a podpisů (vidimace a legalizace)
Využití údajů z agendového informačního systému evidence obyvatel (§ 18a zákona č. 21/2006 Sb.)
Využití údajů z registru obyvatel (§ 18a zákona č. 21/2006 Sb.)
Využití údajů z agendového informačního systému evidence občanských průkazů (§ 18b č. 21/2006 Sb.)
Využití údajů z agendového cizineckého informačního systému (§ 18a, § 18b a § 18c zákona č. 21/2006 Sb.)
Využití údajů z agendového informačního systému evidence cestovních dokladů (§ 18c zákona č. 21/2006 Sb.)
Agendy státní občanství
Využití údajů z agendového cizineckého informačního systému (§ 58 zákona č. 186/2013 Sb.)
Využití údajů z agendového informačního systému evidence obyvatel (§ 57 odst. 1 zákona č. 186/2013 Sb.)
Využití údajů z agendového informačního systému evidence cestovních dokladů(§ 61 zákona č. 186/2013
Využití údajů z agendového informačního systému evidence občanských průkazů(§60 zákona č.186/2013
Využití údajů z registru rodných čísel (§ 57 odst. 3 zákona č. 186/2013 Sb.)
Zápis pozbytí státního občanství České republiky do agendového informačního systému evidence obyvatel
Využití údajů z registru obyvatel (§ 56 zákona č. 186/2013 Sb.)
Zápis nabytí státního občanství České republiky do agendového informačního systému evidence obyvatel
Agendy matriky
Doplnění údajů do agendového informačního systému evidence obyvatel
Využití údajů z agendového cizineckého informačního systému
Přidělení rodného čísla
Využití údajů z agendového informačního systému evidence občanských průkazů
Využití údajů z informačního systému evidence obyvatel (§ 29a zákona č. 115/2006 Sb.)
Zápis údaje o neexistenci registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis občana při narození do agendového informačního systému evidence obyvatel
Zápis údaje o zdánlivém manželství do agendového informačního systému evidence obyvatel
Zápis údaje o rozvodu manželství do agendového informačního systému evidence obyvatel
Zápis údajů o osvojení do agendového informačního systému evidence obyvatel
Zápis údajů o úmrtí do agendového informačního systému evidence obyvatel
Zápis údajů o uzavření manželství do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen do agendového informačního systému evidence obyvatel
Změna rodného čísla
Využití údajů z agendového informačního systému evidence obyvatel a registru rodných čísel (§ 84a zákona č. 301/2000 Sb.)
Zápis rozhodnutí soudu o prohlášení za mrtvého do agendového informačního systému evidence obyvatel
Zápis údaje o ztrátě nebo odcizení občanského průkazu do informačního systému evidence občanských průkazů
Zápis změny příjmení do informačního systému evidence obyvatel
Odstranění údajů o otci na základě popření otcovství v agendovém informačním systému evidence obyvatel
Poskytnutí údajů z agendového informačního systému evidence obyvatel
Zápis změny příjmení do informačního systému evidence obyvatel
Zápis změny příjmení do informačního systému evidence obyvatel
Využití údajů z agendového informačního systému evidence cestovních dokladů
Zápis údajů o občanovi do agendového informačního systému evidence obyvatel při nabytí státního občanství určením otcovství
Využití údajů z registru obyvatel
Zápis jiného zákonného zástupce do agendového informačního systému evidence obyvatel
Zápis údaje o neplatnosti registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údaje o neplatnosti manželství do agendového informačního systému evidence obyvatel
Zápis údaje o zrušení registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údajů o vzniku registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údajů o otci na základě určení otcovství do agendového informačního systému evidence obyvatel
Zápis změny pohlaví do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny rodného čísla do agendového informačního systému evidence obyvatel
Agendy zvláštní matriky
Doplnění údajů do agendového informačního systému evidence obyvatel
Využití údajů z agendového cizineckého informačního systému
Využití údajů z agendového informačního systému evidence obyvatel (§ 29a zákona č. 115/2006 Sb.)
Zápis údaje o neplatnosti registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údaje o zrušení registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údajů o občanovi do agendového informačního systému evidence obyvatel při nabytí státního občanství určením otcovství
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny příjmení do agendového informačního systému evidence obyvatel
Zápis změny příjmení do agendového informačního systému evidence obyvatel
Využití údajů z agendového informačního systému evidence cestovních dokladů
Odstranění údajů o otci na základě popření otcovství v agendovém informačním systému evidence obyvatel
Přidělení rodného čísla
Vužití údajů z agendového informačního systému evidence občanských průkazu
Využití údajů z registru obyvatel
Využití údajů z agendového informačního systému evidence obyvatel a registru rodných čísel (§ 84 zákona č. 301/2000 Sb.)
Zápis rozhodnutí soudu o prohlášení za mrtvého do agendového informačního systému evidence obyvatel
Zápis jiného zákonného zástupce do agendového informačního systému evidence obyvatel
Zápis občana při narození do agendového informačního systému evidence obyvatel při narození
Zápis údaje o rozvodu manželství do agendového informačního systému evidence obyvatel
Zápis údaje o zdánlivém manželství do agendového informačního systému evidence obyvatel
Zápis údaje o neexistenci registrovaného partnerství do agendového informačního systému evidence
Zápis údajů o otci na základě určení otcovství do agendového informačního systému evidence obyvatel
Zápis údaje o neplatnosti manželství do agendového informačního systému evidence obyvatel
Zápis údajů o osvojení do agendového informačního systému evidence obyvatel
Zápis údajů o vzniku registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údajů o úmrtí do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny pohlaví do agendového informačního systému evidence obyvatel
Změna rodného čísla
Zápis údajů o uzavření manželství do agendového informačního systému evidence obyvatel
Zápis změny rodného čísla do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen a příjmení do agendového informačního systému evidence obyvatel
Zápis změny příjmení do agendového informačního systému evidence obyvatel
Zápis změny jména / jmen do informačního systému evidence obyvatel
Obecné služby RBOÚ
Formulář autorizovaná konverze z elektronické do listinné podoby dokumentu
Formulář katastru nemovitostí
Veřejný výpis údajů z registru osob
Výpis údajů z registru osob
Formulář autorizovaná konverze z listinné do elektronické podoby dokumentu
Žádost o vydání seznamů voličů
Konzulární ochrana občanů ČR v zahraničí
Formulář autorizovaná konverze z listinné do elektronické podoby dokumentu
Formulář autorizovaná konverze z elektronické do listinné podoby dokumentu
Výpis údajů z registru obyvatel
Formulář obchodního rejstříku
Formulář řízení o dědictví (pro notáře)
Ověření totožnosti a osobních údajů osoby (pro zastupitelské úřady)
Formulář Rejstříku trestů podle zákona č. 124/2008 Sb.
Žádost o poskytnutí údajů jiné osobě podle § 58a odst. 1 zákona č. 111/2009 Sb., o základních registrech,
Výpis Centrálního registru zbraní (pro exekutory)
Ověření provedení autorizované konverze
Žádost o změnu údajů při zjištění nesouladu v registru obyvatel
Žádost o změnu údajů v registru osob
Žádost o výpis z rejstříku trestů právnických osob
Agendy soudy
Hlášení o vykonatelném rozhodnutí, jímž se fyzická osoba omezuje na osobní svobodě dle zákona č. 300/2008 Sb.
Zápis údaje o neexistenci registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis rozhodnutí soudu o prohlášení za mrtvého do agendového informačního systému evidence obyvatel
Zápis údaje o omezení svéprávnosti k právním úkonům do agendového informačního systému evidence obyvatel
Zápis údaje o zbavení způsobilosti k právním úkonům do agendového informačního systému evidence obyvatel
Zápis údaje o zdánlivém manželství do agendového informačního systému evidence obyvatel
Zápis údaje o zrušení registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis opatrovníka u osoby, u které došlo ke zbavení způsobilosti k právním úkonům do agendového informačního systému evidence obyvatel
Zápis údaje o neplatnosti registrovaného partnerství do agendového informačního systému evidence obyvatel
Zápis údaje o rozvodu manželství do agendového informačního systému evidence obyvatel
Zápis údaje o neplatnosti manželství do agendového informačního systému evidence obyvatel
Zápis údaje o opatrovníkovi u osoby, u níž došlo k omezení svéprávnosti do agendového informačního systému evidence obyvatel
OVM - ORP
OVM - ORP byznys
Samostatná působnost
Agenda ORP samostatná
Přenesená působnost
Agenda ORP přenesená
Služba ORP poskytovaná ostatním
Produkt ORP
portál ORP
Činnostní role agnedy ORP
Úředník ORP
Spis ORP
Elektronický dokument ORP
dokument ORP
Listinný dokument ORP
Přepážka ORP
Podatelna ORP
Příjem podání ORP
Zpracování podání ORP
OVM - ORP aplikace
Zpracování dokumentů a spisů ORP
Elektronický dokument ORP
Poskytování funkcionality ORP
Spisová služba ORP
Evidence dokumentů a spisů ORP
AIS ORP
Podpora výkonu agendy ORP
Provozní systémy ORP
Dohledové systémy ORP
OVM - ORP platformy
Poskytování datového úložiště ORP
Poskytování výkonu ORP
Dostupnost ORP
Přístupnost ORP
Platformy ORP
Funkcionality datového centra ORP
OVM - ORP sítě
Komunikační služby ORP
Vlastní komunikační síť ORP
Technologické centrum ORP
Lokalita TC ORP
OVM - Kraj
OVM - Kraj byznys
portál Kraje
Služba Kraje poskytovaná ostatním
Produkt Kraje
Agenda Kraje
Přepážka Kraje
Činnostní role agendy Kraje
Spis Kraje
Úředník Kraje
Elektronický dokument Kraje
dokument Kraje
Listinný dokument Kraje
Podatelna Kraje
Příjem podání Kraje
Zpracování podání Kraje
OVM Kraj - aplikace
Zpracování dokumentů a spisů Kraje
Elektronický dokument Kraje
Poskytování funkcionality Kraje
Spisová služba Kraje
Evidence dokumentů a spisů Kraje
AIS Kraje
Podpora výkonu agendy Kraje
Provozní systémy Kraje
Dohledové systémy Kraje
OVM Kraj - platformy
Poskytování datového úložiště Kraje
Poskytování výkonu Kraje
Dostupnost Kraje
Přístupnost Kraje
Platformy Kraje
Funkcionality datového centra Kraje
OVM Kraj - sítě
Komunikační služby Kraje
Vlastní komunikační síť Kraje
Technologické centrum Kraje
Lokalita TC Kraje
OVM - Ministerstvo
OVM - Ministerstvo byznys
portál Ministerstva
Služba poskytovaná ostatním
Produkt Ministerstva
Agenda Ministerstva
Přepážka Ministerstva
Činnostní role agendy Ministerstva
Spis Ministerstva
Úředník Ministerstva
Elektronický dokument Ministerstva
dokument Ministerstva
Listinný dokument Ministerstva
Podatelna Ministerstva
Příjem podání Ministerstva
Zpracování podání Ministerstva
OVM - Ministerstvo aplikace
Zpracování dokumentů a spisů Ministerstva
Elektronický dokument Ministerstva
Poskytování funkcionality Ministerstva
Spisová služba
Evidence dokumentů a spisů
AIS Ministerstva
Podpora výkonu agendy
Provozní systémy Ministerstva
Dohledové systémy Ministerstva
OVM - Ministerstvo platformy
Poskytování datového úložiště
Poskytování výkonu Ministerstva
Dostupnost Ministerstva
Přístupnost Ministerstva
Platformy Ministerstva
Funkcionality datového centra
OVM - Ministerstvo sítě
Komunikační služby Ministerstva
Vlastní komunikační síť
Technologické centrum Ministerstva
Lokalita TC Ministerstva
eGovernment backend
eGovernment aplikace
Dotazování do ZR
ZR
Ověření identity
Správa referenčních údajů
Dotazování skrze CzechPOINT
CzechPoint
Dotazy z moci úřední
Doručování datových zpráv
ISDS
Přenos datových zpráv
Identifikace/ autentizace
NIA
Identifikace/ autentizace
Centrální registr přestupků
Centrální registr poskytovatelů zdravotní péče
Centrální registr administrativních budov
Aministrativní registr ekonomických subjektů
Insolvenční rejstřík
CEDR
NDA/digitální archiv
eGovernment platformy
Státní datové centrum
Dohledové centrum eGov
eGovernment sítě
Služby CMS
CMS
Funkce CMS
Služby KIVS
KIVS
Funkce KIVS

Client view - legal entities



Client view - natural persons


Klienti VS
Fyzická osoba
Činění úkonu. Podání se vyznačuje svým obsahem bez ohledu na název
Příjemce / Žadatel informací
Fyzický úkon
Podání
Elektronický úkon
Autentizační modul
eMail
Webový prohlížeč
eOP
Počítač
Internet
eGovernment frontend
eGovernment byznys
Asistovaná přepážka
Pošta
CzechPOINT klasik
CzechPOINT @home
CzechPOINT @office
Aplikace webového portálu
ISDS
Portál občana
Poskytování dat PPDF
Podepsaný dokument Listinný
CzechPOINT
Základní registry
Datové schránky
Výpis z veřejných rejstříků
Úplný výpis
Výpis platných
Spolkový rejstřík
Nadační rejstřík
Rejstřík ústavů
Rejstřík společenství vlastníků jednotek
Obchodní rejstřík
Rejstřík obecně prospěšných společností
Výpis z rejstříku trestů právnické osoby
Výpis z katastru nemovitostí
Přijetí žádosti podání podle živnostenského zákona
Vidimace
Výpis z živnostenského rejstříku
Výpis z obchodního rejstříku
Podání do registru účastníků provozu modulu autovraků ISOH
Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů
Výpis z insolvenčního rejstříku
Autorizovaná konverze dokumentů
Výpis z bodového hodnocení řidiče
Výpis z rejstříku trestů
Úschovna systému CzechPOINT
OVM - ORP
OVM - ORP byznys
Samostatná působnost
Agenda ORP samostatná
Přenesená působnost
Agenda ORP přenesená
Služba ORP poskytovaná ostatním
Produkt ORP
portál ORP
Činnostní role agendy ORP
Úředník ORP
Spis ORP
Elektronický dokument ORP
Listinný dokument ORP
dokument ORP
Přepážka ORP
Podatelna ORP
Příjem podání ORP
Zpracování podání ORP
OVM - ORP aplikace
Zpracování dokumentů a spisů ORP
Elektronický dokument ORP
Poskytování funkcionality ORP
Spisová služba ORP
Evidence dokumentů a spisů ORP
AIS ORP
Podpora výkonu agendy ORP
Provozní systémy ORP
Dohledové systémy ORP
OVM - ORP platformy
Poskytování datového úložiště ORP
Poskytování výkonu ORP
Dostupnost ORP
Přístupnost ORP
Platformy ORP
Funkcionality datového centra ORP
OVM - ORP sítě
Komunikační služby ORP
Vlastní komunikační síť ORP
Technologické centrum ORP
Lokalita TC ORP
OVM - Kraj
OVM - Kraj byznys
portál Kraje
Služba Kraje poskytovaná ostatním
Produkt Kraje
Agenda Kraje
Přepážka Kraje
Činnostní role agendy Kraje
Spis Kraje
Úředník Kraje
Elektronický dokument Kraje
Listinný dokument Kraje
dokument Kraje
Podatelna Kraje
Příjem podání Kraje
Zpracování podání Kraje
OVM Kraj - aplikace
Zpracování dokumentů a spisů Kraje
Elektronický dokument Kraje
Poskytování funkcionality Kraje
Spisová služba Kraje
Evidence dokumentů a spisů Kraje
AIS Kraje
Podpora výkonu agendy Kraje
Provozní systémy Kraje
Dohledové systémy Kraje
OVM Kraj - platformy
Poskytování datového úložiště Kraje
Poskytování výkonu Kraje
Dostupnost Kraje
Přístupnost Kraje
Platformy Kraje
Funkcionality datového centra Kraje
OVM Kraj - sítě
Komunikační služby Kraje
Vlastní komunikační síť Kraje
Technologické centrum Kraje
Lokalita TC Kraje
OVM - Ministerstvo
OVM - Ministerstvo byznys
portál Ministerstva
Služba Ministerstva poskytovaná ostatním
Produkt Ministerstva
Agenda Ministerstva
Přepážka Ministerstva
Činnostní role agendy Ministerstva
Spis Ministerstva
Úředník Ministerstva
Elektronický dokument Ministerstva
Listinný dokument Ministerstva
dokument Ministerstva
Podatelna Ministerstva
Příjem podání Ministerstva
Zpracování podání Ministerstva
OVM - Ministerstvo aplikace
Zpracování dokumentů a spisů Ministerstva
Elektronický dokument Ministerstva
Poskytování funkcionality Ministerstva
Spisová služba Ministerstva
Evidence dokumentů a spisů
AIS Ministerstva
Podpora výkonu agendy
Provozní systémy Ministerstva
Dohledové systémy Ministerstva
OVM - Ministerstvo platformy
Poskytování datového úložiště
Poskytování výkonu Ministerstva
Dostupnost Ministerstva
Přístupnost Ministerstva
Platformy Ministerstva
Funkcionality datového centra
OVM - Ministerstvo sítě
Komunikační služby Ministerstva
Vlastní komunikační síť
Technologické centrum Ministerstva
Lokalita TC Ministerstva
eGovernment backend
eGovernment aplikace
Dotazování do ZR
ZR
Ověření identity
Správa referenčních údajů
Dotazování skrze CzechPOINT
CzechPoint
Dotazy z moci úřední
Doručování datových zpráv
ISDS
Přenos datových zpráv
Identifikace/ autentizace
NIA
Identifikace/ autentizace
Centrální registr přestupků
Centrální registr poskytovatelů zdravotní péče
Centrální registr administrativních budov
Administrativní registr ekonomických subjektů
Insolvenční rejstřík
CEDR
NDA/digitální archiv
eGovernment platformy
Státní datové centrum
Dohledové centrum eGov
eGovernment sítě
Služby CMS
Služby KIVS
CMS
Funkce CMS
KIVS
Funkce KIVS

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

Permanent link:
https://archi.gov.cz/en:nap_dokument:pravidla_tvorby_a_udrzby_vlastni_ctyrvrstve_architektury_jednotlivych_uradu

Last update: **2021/08/17 15:04**