DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Další pravidla a pomůcky tvorby architektury zdola

Referenční architektury úřadů a řešení

Koncepce referenčních modelů architektury úřadů VS

Jak je již uvedeno výše, bude OHA ve spolupráci a koordinaci s dalšími organizacemi vydávat příklady nejlepší architektonické praxe, klasifikační hierarchie a akcelerátory práce v architektonických angažmá v podobě tzv. referenčních modelů (dále i jenom RM).

Referenční modely představují buď povinnou, nebo fakultativní (podle doprovodné informace u každého z nich) referenci formy, tj. způsobu modelování a interpretace architektur úřadů.

Referenční modely budou vydávány převážně pro architektury celých úřadů nebo jejich podstatných částí, segmentů.

Pro vyšší využitelnost budou vedle generických, celostátně platných RM, vydávány i RM specifické pro určité odvětví (segment) veřejné správy, například zdravotnictví, infrastruktura apod., nebo pro úřady z jednotlivých vrstev hierarchie státní správy a samosprávy, se zahrnutím všech typů působnosti na dané úrovni (přímé, přenesené, samosprávné, soukromoprávní).

Lze očekávat vydání referenčních modelů na těchto úrovních:

- Referenční architektury ústředních správních úřadů - kromě ÚSÚ, se tím myslí i ostatní úřady s celostátní působností.
- Referenční architektury územních samospráv
- Zjednodušený příklad architektury kraje a krajské korporace, vytvořený ve spolupráci s Asociací krajů ČR
- Zjednodušený příklad architektury ORP a jeho korporace
- Zjednodušený příklad architektury malé obce - oba vytvořené ve spolupráci se SMO a KISMO
- Referenční architektury dalších typů orgánů veřejné moci - budou-li takové identifikovány.

Architektonické vzory klíčových oblastí úřadu

OHA bude postupně vydávat referenční typové schopnostní enterprise architektury těch oblastí architektury úřadů (zejména procesní a aplikační), které sice zůstávají většinou v lokální zodpovědnosti, ale jejichž **logická podoba** musí být pro splnění cílů koncepce centrálně předepsána a následně v řešeních dodržena.

IKČR uvažuje zejména o těchto kategoriích referenčních modelů typové procesní a aplikační architektury:

- Multikanálová uživatelská rozhraní
  - pro klienty VS
  - pro zaměstnance VS
- Klíčové části agendových IS
  - Sdílený agendový Front-office (CRM)
  - Specifický agendový Middle-Office (odborné části agendových IS), některé nadresortní (dotace, kontroly, údržba síťové infrastruktury státu, ...)
  - Sdílený agendový Back-Office (platební, znalostní a další systémy)
- Správa spisů, dokumentů a jejich toku (workflow)
- Provozní ERP systémy

- Rozšiřující systémy správy zdrojů úřadu
- Identity management
- Integrační platformy
- Správa kmenových dat a číselníků (s vazbou na ZR i bez)
- Business Intelligence (a její využití jak pro manažerské rozhodování, tak pro podporu transakčních agendových i provozních systémů)

Referenční model typové elektronické spisové služby úřadu

Bude doplněno.

Povinné vzory architektur typových řešení

OHA bude postupně vydávat vzorové referenční schopnostní enterprise architektury a architektury řešení těch oblastí architektury úřadů, jejichž podoba musí být pro splnění cílů koncepce centrálně předepsána a následně v řešeních dodržena. Proto se nazývají **povinnými architektonickými vzory**[1)].

Typicky se bude jednat o oblasti architektury využívající sdílené služby eGovernmentu nebo o další oblasti, v nichž bude pro naplnění zákonných povinností nebo dosažení efektivity žádoucí jednotné, standardizované řešení.

Architektonický vzor typového agendového IS

Základní aplikační architektura ISVS v kontextu eGovernmentu

tady bude dovysvětleno

Detailní architektury specifických rozhraní agendového ISVS

tady bude další schéma a vysvětlení

Architektonické vzory využití sdílených služeb eGovernmentu

OHA bude vydávat také detailní architektonické vzory rozhraní pro využití sdílených služeb eGovernmentu, na úrovni jednotlivých weboch služeb a další prvků řešení a designu těchto rozhraní a způsobu jejich využití v lokálních architekturách úřadů.

IKČR zde ukládá povinnost respektovat v návrzích řešení tyto vzory tak, jak budou OHA publikovány, postupně a samostatně.

Architektonický vzor typové elektronické spisové služby úřadu

Bude doplněno.

Specifická pravidla pro architekturu úřadů

Pravidla pro architekturu dle velikosti a možností úřadů

Pro obce 1. a 2. typu má vize architektury veřejné správy následující podobu:

Architekturu IT úřadu obce 1. a 2. typu (do určité velikosti, viz níže) tvoří pouze koncová zařízení pro uživatele (dále jen zařízení), síťovou infrastrukturu jim jako sdílenou poskytuje kraj, aplikační služby pro státní správu v přenesené působnosti poskytnou ohlašovatelé agend a aplikační služby pro samosprávní působnost poskytne vyšší stupeň územní samosprávy (ORP, kraj) jako sdílenou službu.

Pro oblast samosprávy tak vychází koncepce z následujících principů:

1. Koncepce je závazná pro všechny subjekty samosprávy, které mají více než 10 zařízení.
1. Informační systémy pro činnosti a agendy v přenesené působnosti přebírají v plném rozsahu od centrálních úřadů. Samosprávné činnosti si každý územněsprávní celek zajišťuje sám.
1. Subjekty s méně než 10 zařízeními si pořizují pouze uživatelský HW a SW, tj. tato koncová zařízení, SW produkty pro výkon veřejné správy jim jako službu zajišťují subjekty, v jejichž správním obvodě leží.

Ad1) Územněsprávní celky, kraje, velká města a obce s rozšířenou působností, mají ve svých úřadech specializované útvary IT. Tyto útvary jsou schopné vlastními silami nebo za pomoci externích dodavatelů zajistit veškeré požadavky IKČR a metodicky řídit své zřizované organizace (technické služby, nemocnice, sociální ústavy, velké školy). Subjekty samosprávy, které mají do deseti zařízení, nedisponují žádným specialistou IT a jsou odkázány na pomoc větších subjektů.

Ad2) Státní správa, kterou samosprávní subjekty vykonávají v přenesené působnosti, je zpravidla podporována informačními systémy, které jsou centrální (živnostenský rejstřík, registr vozidel). Pořízení, vývoj a aktualizace těchto informačních systému je plně v gesci příslušného centrálního orgánu, který je za agendu odpovědný dle zákona. Naproti tomu pro každou samosprávnou činnost jsou informační systémy zajišťovány decentralizovaně (výběrem z nabídky IT firem, málokdy vlastním vývojem). Informační koncepce předpokládá, že také tyto informační systémy budou splňovat stanovené standardy a zásady informační koncepce.

Ad3) Velikost samosprávných subjektů je velmi rozdílná. Počínaje kraji, které disponují velkými úřady, přes obce s rozšířenou působností s úřady o desítkách zaměstnanců až po malé obce, kde je maximálně uvolněný starosta a jeden úředník. Stejná situaci je i u zřizovaných organizací (velké dopravní podniky, nemocnice, ústavy sociální péče) U těchto nejmenších obcí a zřizovaných organizací informační koncepce předpokládá, že budou pouze nakupovat hardware a jeho provozní SW s parametry, které požadují používané informační systémy. Informační systémy budou používat sdílené, jako službu. Informační systémy jim budou zajišťovat obce s rozšířenou působností, v jejichž správním obvodě malá obec nebo organizace leží. Obdobně síťovou infrastrukturu pro napojení na centrální prvky eGovernmentu a sdílené služby jim bude zajišťovat ORP nebo kraj, v jejichž správním obvodě malá obec nebo organizace leží.

Pravidla pro architekturu dle pozice úřadu ve struktuře VS ČR a vztahu ke sdíleným službám

Úřady, zodpovědné ze zákona jako věcní správci sdílených prvků služeb eGovernmentu, považují tyto jim svěřené prvky za nedílnou součást architektury svého úřadu. Vedle celkové architektury svých úřadů ještě samostatně modelují modely architektury těchto svěřených sdílených prvků, a to jak na úrovni EA (PSA), tak na úrovni podrobnosti tzv. architektury řešení, viz dále. Tyto úřady pro tyto prvky modelují také tzv. rozšířené modely, tj. modely zahrnující také prvky typové (logické) prvky architektury na straně typových (typických) odběratelů jejich sdílených služeb.

Úřady, užívající služeb sdílených prvků eGovernmentu, nemodelují tyto informační systémy v žádném případě jako aktivní prvky (aplikační a technologické komponenty a rozhraní) - nemají je v rozsahu své zodpovědnosti, nýbrž výhradně jako služby (byznys, aplikační nebo technologické a infrastrukturní - podle potřeby vyjádření) a

rozhraní vlastních komponent na tyto systémy.

Úřady zodpovědné, viz výše, za implementaci a provoz centrální registrů a AIS pro služby v přenesené působnosti, modelují architekturu svých úřadů přirozeně i včetně těchto systémů. Současně jsou povinny vytvářet a udržovat také tzv. rozšířené modely, tj. modely zahrnující také prvky typové (logické) prvky architektury na straně typových (typických) odběratelů jejich sdílených služeb, ukazující veškerý potřebný kontext (například integraci centrálního AIS na lokální eSSL a EkIS).

Úřady užívající tyto centrální AIS pro služby v přenesené působnosti, nemodelují ve svých architekturách úřadu tyto jako aktivní prvky (nemají je ve své zodpovědnosti), nýbrž jako služby těchto systémů a rozhraní vlastních komponent na tyto systémy.

Principy pseudonymizace osobních údajů v ISVS

Pseudonymizace znamená uložení dat technikou oddělení agendových a identifikačních údajů a jejich propojení pomocí AIFO. Pseudonymizace není anonymizací údajů, a i pseudonymizované údaje jsou nadále osobní údaje. Účelem pseudonymizace je tedy: • Snížení rizika neoprávněného nakládání s osobními údaji • Snížení rizika neoprávněného spojování osobních údajů (dále také „Profilování“) Oproti dnes běžně používanému postupu, kdy veškeré údaje o osobách jsou uloženy v jedné tabulce (tj. včetně údajů osobních), jde o systematické rozdělení uložených údajů tak, aby od sebe byly odděleny minimálně údaje: • Agendové – údaje vytvářené v rámci agendy, ve které se úřaduje • Referenční – údaje získané z registru obyvatel či jiných ZR • Agendové – údaje získané z jiných agend, relevantní k dané agendě Požadavky na pseudonymizaci osobních údajů jsou architektonické, implementační a procesní. Jejich zavedení musí být provedeno tak, aby v žádném případě neomezilo výkon veřejné správy. V ideálním případě by uživatelé ISVS neměli zaznamenat, že pro ukládání a práci s osobními údaji jsou použity procesy pseudonymizace. Konkrétní realizace tohoto požadavku závisí na komplexitě daného informačního systému a agend, které podporuje Doporučené architektonické postupy Pseudonymizace není výslovnou podmínkou zpracování osobních údajů, je však doporučeným postupem snižování rizika neoprávněného nakládání s osobními údaji, spolu s jinými technikami např. šifrováním. • Celostátní úroveň – důsledné využívání identifikátoru AIFO, prostřednictvím komunikace s Informačním systémem základních registrů (ISZR) a eGovernment online Service Bus (eGSB), při výměně údajů mezi jednotlivými ISVS, a současně zamezení/ukončení jakékoliv výměny agendových dat bez použití AIFO. • Lokální úroveň – oddělení primárních identifikačních údajů osoby (referenční údaje vedené v Registru obyvatel) od údajů vytvářených v rámci vlastní agendy, a také oddělení od údajů případně získaných z jiných agend na základě oprávnění při výkonu konkrétní agendy • Doprovodná opatření – šifrování uložených dat, které zvyšuje ochranu osobních údajů v případě odcizení datových souborů (i ve formě záloh) a důsledné logování přístupu k osobním údajům

Celostátní úroveň

Na celostátní úrovni je zavedením Základních registrů založen bezpečný způsob výměny a správy osobních údajů. Každá agenda má přiděleno AIFO osoby a pouze převodník AIFO (ORG) je schopen převádět AIFO dané osoby mezi jednotlivými agendami. Každý takovýto převod je důsledně zalogován a výměna údajů je zaznamenána v logu Registru obyvatel. Při výměně údajů mezi agendami je vždy nutné zvážit rozsah údajů, které jsou přenášeny. Současný právní řád v mnoha případech zakládá oprávnění pro získání velkého rozsahu údajů mezi agendami z důvodu zajištění jednoznačné identifikace osoby, o které jsou údaje předávány. Zde je nutné si ale uvědomit, že ačkoli může existovat široké legislativní zmocnění k získávání údajů ze zdrojové agendy, s ohledem na ochranu osobních údajů je doporučeno využívat pouze údaje nezbytně nutné.

Pro identifikaci fyzické osoby při jejím kontaktu s veřejnou správou je ideální použití platného identifikačního dokladu, neboť každý orgán veřejné moci, který při své činnosti využívá některé referenční údaje vedené v registru obyvatel, je oprávněn využívat údaj o čísle a druhu elektronicky čitelných identifikačních dokladů . Pokud tedy fyzická osoba předloží nebo ve formuláři uvede druh a číslo svého elektronicky čitelného dokladu, pak může být jednoznačně ztotožněna v Registru obyvatel. V případě vzdálené identifikace a autentizace prostřednictvím Národního bodu je fyzická osoba jednoznačně identifikována bezvýznamovým směrovým identifikátorem (BSI), který je možné převést prostřednictvím informačního systému základních registrů na AIFO

(službou E226).

Lokální úroveň

V rámci informačních systémů jednotlivého orgánu veřejné moci je doporučeno využívání stejných principů, které jsou používány na celostátní úrovni s respektem k faktu, že jde o úřadování v konkrétní agendě, kde se velmi pravděpodobně vyskytují agendově specifické údaje, výjimečně i údaje z agend jiných.

Doprovodná opatření

• Logování – každý přístup k osobním údajům a jejich aktuální propojení musí být uložen do provozního logu po dobu minimálně dvou let v souladu s pravidly dle zákona 111/2009 Sb. Musí být tedy dohledatelné, kdo a v rámci jaké činnosti přistupoval k údajům a provedl jejich propojení. • Aktualizace údajů – referenční údaje o fyzické osobě musí být udržovány v aktuálním stavu prostřednictvím notifikačního systému základních registrů. Agendové údaje z jiných agend pak musí být udržovány aktuální podle pravidel platných v agendách, které údaje poskytují. Dle GDPR musí zpracovatel osobních údajů zajistit, že pracuje s aktuálními údaji tak, aby bylo minimalizováno nebezpečí chybného rozhodnutí na základě neaktuálních dat (např. zaslání rozhodnutí na neaktuální adresu osobu, či nevyužití datové schránky fyzické osoby, pokud ji má osoba zřízenu). Zde je nutné poznamenat, že každý orgán veřejné moci, který při své činnosti využívá některé referenční údaje vedené v registru obyvatel, je oprávněn rovněž využívat údaj o adrese, na kterou mají být doručovány písemnosti, o typu datové schránky a identifikátoru datové schránky, je-li tato datová schránka zpřístupněna .

Uvedené architektonické požadavky musí být provedeny na databázové a aplikační úrovni tak, aby uživatelé informačního systému nebyli omezováni ve výkonu podporovaných agend. Současně při nutné datové analýze musí být stanoveno, jaké údaje je nezbytně nutné vést v rámci informačního systému. Opět je nutné vzít do úvahy, že ačkoli zákonné ustanovení umožňuje vedení údaje, nemusí být tento údaj veden ve své hodnotě, ale může být veden formou referenční či jiné vazby. Konkrétní rozhodnutí věcného správce agendy musí vycházet s procesních požadavků agendy a není zde možné stanovit paušální jednoznačné pravidlo. Příkladem může být vedení adres v rámci České republiky, kdy je doporučeným postupem vedení tohoto údaje formou referenční vazby do Registru územní identifikace (RUIAN) či lokální kopie adresních míst, která je udržována aktuální v souladu s RUIAN. Tím je následně vyloučen chybný správní postup, kdy je použita neplatná adresa. Dalším příkladem je situace, kdy v agendě není využíváno například datum narození osoby pro vyhledávání či třídění, pak toto datum narození je možné vést ve formě referenční vazby do registru obyvatel a konkrétní údaj získávat pouze v potřebných případech.

Právní aspekty

Zákonem 111/2009 Sb. o základních registrech byl zaveden základní princip pseudonymizace ve veřejné správě formou Agendového identifikátoru fyzické osoby (AIFO) , který zajišťuje pseudonymizaci v rámci výkonu veřejné správy. Důsledné využívání AIFO v rámci ISVS zajišťuje snížení rizika Profilování ve smyslu neoprávněného spojování údajů o konkrétní osobě z různých agend. Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen GDPR) ve článku 4. definuje pseudonymizaci následovně: „pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě S odkazem na výše uvedené je nutné poznamenat, že v současnosti stále ještě využívané rodné číslo je v přímém konfliktu s požadavkem na pseudonymizaci, protože RČ, kromě toho že jde o významový identifikátor (obsahuje údaj o datu narození a pohlaví osoby), zejména umožňuje spojování jakýchkoli údajů, které jsou ve spojení s ním vedeny.

Architektonické a IT standardy

Standardy návrhu a vývoje elektronických služeb veřejné správy

Standard elektronických služeb veřejné správy definuje kritéria, jejichž naplnění je předpokladem pro tvorbu a provoz kvalitních a úspěšných služeb veřejné správy[2]). Naplnění standardu je vyžadováno od všech transakčních elektronických služeb poskytovaných veřejnou správou pro externí klienty.

Soulad nových a upravovaných služeb se standardem je předmětem posuzování záměrů OHA (§4 odst. 1 písm. e) zák. 365/2000 Sb. a usnesení vlády č. 998 ze dne 2. listopadu 2015).

OHA bude standardy nárvhu a vývoje elektronických služeb VS vydávat průběžně a publikovat je na portálu a v dalších komunikačních kanálech OHA.

Výchozí sada standardů je uvedena v Dodatku G této IKČR.

Technické standardy informačních systémů

V návaznosti na referenční modely, povinné vzory, standardy návrhu služeb a další součásti NAP může MV ČR vydávat a publikovat tzv. IT standardy součástí IT řešení, tj. formátů, jazyků, protokolů, platforem, zabezpečení, atp., v návaznosti na mezinárodní normy a standardy a domáci zkušenosti.

1)
Angl. Mandatory solution architecture patterns
2)
Zdroj: odvozeno a převzato z Digital Service Standard Velké Británie (https://www.gov.uk/service-manual/service-standard

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

Permanent link:
https://archi.gov.cz/nap:dalsi_pravidla_a_pomucky_tvorby_architektury_zdola?rev=1566126944

Last update: **2019/08/18 13:15**