ČESKÁ REPUBLIKA MINISTERSTVO DOPRAVY	**Nařízení náměstka Sekce legislativní a právní č. SŘKB/2**	**Datum účinnosti: dnem schválení**

Architektonické principy Ministerstva dopravy

Vydáno náměstkem Sekce legislativní a právní

č. j. 1/2020-330-RDK/1

	ZPRACOVAL	OVĚŘIL
ÚTVAR	CENDIS, s.p.	O 330
FUNKCE	Senior konzultant	Ředitel odboru
JMÉNO	RNDr. Jiří Kopačka	Ing. František Štefela
DATUM	18. 12. 2020	18. 12. 2020
PODPIS	RNDr. Jiří Kopačka v. r.	Ing. František Štefela v. r.

OBSAH

HISTORIE DOKUMENTU

Upravený bod	Obsah úpravy
úpravy ve verzi 2	
čl. 1.1: Technické konvence	doplněn nový článek: technické konvence (namapování TCP/IP na OSI model)
čl. 3.4: Architektonické principy pro bezpečnost IS	doplněn bod f): pravidla pro šifrování komunikace
čl. 4.4 Architektonické principy pro bezpečnost infrastruktury	doplněn bod c): pravidla šifrování komunikace v rámci aplikační infrastruktury
příloha č. 1: Systémová dokumentace	upřesněn bod 2): popis komunikačních rozhraní
příloha č. 1: Systémová dokumentace	upřesněn bod 6): bezpečnost
příloha č. 1: Provozní dokumentace	upřesněn bod 10): řízení provozu a přečíslování (nově bod 9)

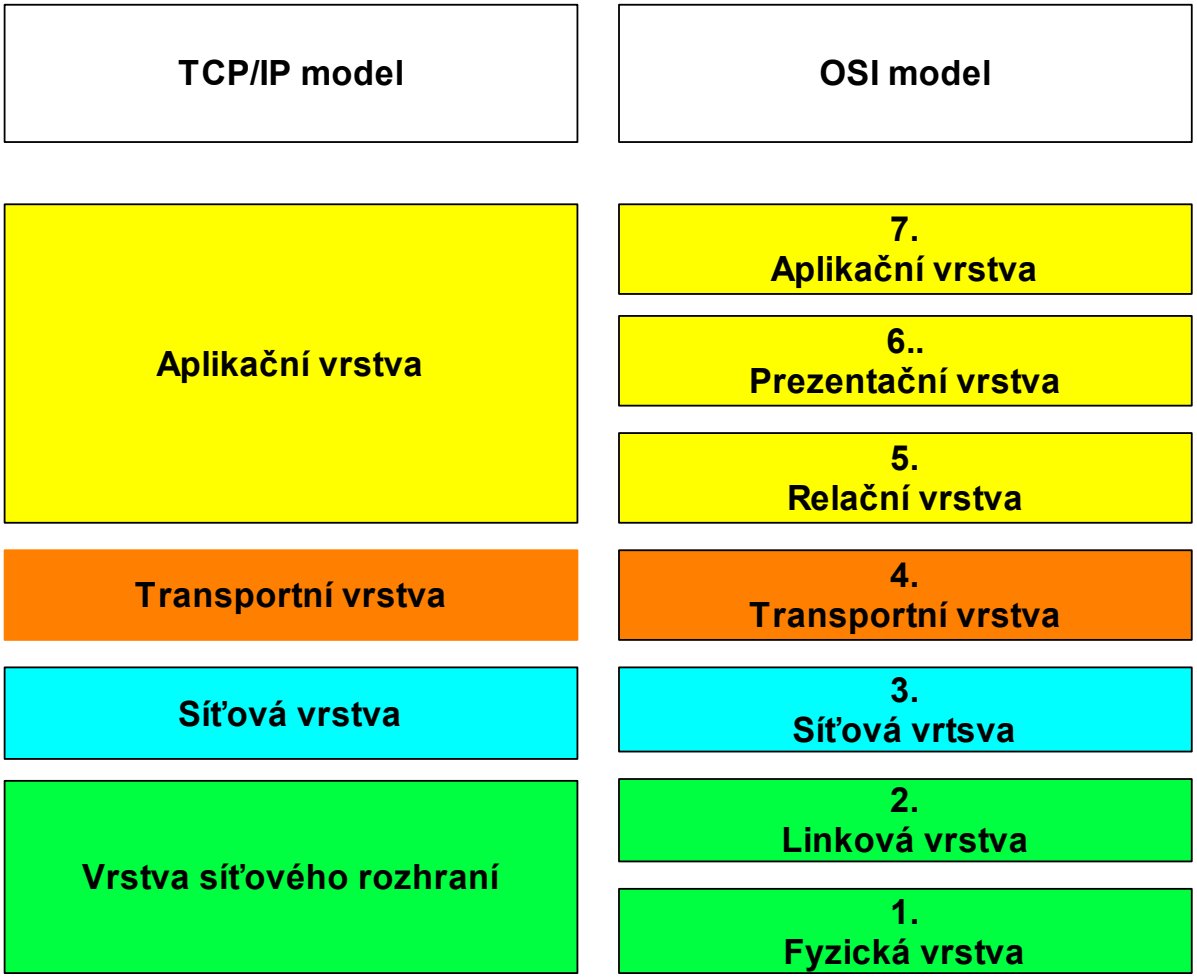
ČLÁNEK 1 POUŽITÉ ZKRATKY A SEZNAM PŘÍLOH

1.1 Použité zkratky/pojmy

Zkratka	Význam
MD	Ministerstvo dopravy České republiky
BPI MD	Bezpečnostní politika informací Ministerstva dopravy
MV	Ministerstvo vnitra České republiky
KB	Kybernetická bezpečnost
OHA MV	Odbor hlavního architekta MV
IS	Informační systém
RFC	RequestForComments, tj. žádost o komentáře
VLAN	Virtuální lokální počítačová síť
HelpDesk	Kontaktní místo pro uživatele IS MD, určené pro předávání informací o incidentech, požadavcích na úpravy IS a podobně
NDA	Dohoda o mlčenlivosti
vendorlock	Situace, kdy je zákazník závislý na určitém dodavateli nebo dodavatelích a nemůže přejít k jiným dodavatelům nebo využívat jiný produkt bez značných nákladů na tuto změnu ať již z právních či technických důvodů
IPS	Systém pro detekci a prevenci průniku
SIEM	Řízení bezpečnostních informací a událostí
Právní předpisy	Jedná se zejména o zákon č. 365/2000 Sb. ve znění prováděcích předpisů, zákon č. 181/2014 Sb. ve znění prováděcích předpisů, zákon č. 250/2017 Sb. ve znění prováděcích předpisů, nařízení GDPR aj.
WSDL	Popis rozhraní webové služby
HTTP	Hypertextový přenosový protokol
trace	Metoda protokolu HTTP
TCP	Transportní vrstva internetového protokolu
UDP	Uživatelský datagramový protokol
firewall	Část počítačové sítě, která zvyšuje bezpečnost síťového provozu
IP	Internetový protokol
IPv4, IPv6	Vylepšené verze internetového protokolu IP
URL	Adresa určující umístění prostředku/dokumentu na internetu
proxy server	Počítačové zařízení, které slouží k propojení webového prohlížeče a internetu
Hyper-V	Označení pro jednu z technik virtualizace hardwaru počítače/serveru
VMware	Produkt, který zajišťuje virtualizaci jednoho nebo více počítačů na jednom hostitelském počítači
SLA	Dohoda o úrovni služeb
VLAN	Virtuální místní počítačová síť, slouží k logickému rozdělení počítačové sítě
CMDB	Konfigurační databáze, úložiště dat používané pro záznam atributů konfiguračních položek provozního prostředí a vztahů mezi konfiguračními položkami po celou dobu jejich životního cyklu

1.2 Technické konvence

Pro potřeby popisu síťových vrstev, služeb a požadavků používá tento dokument referenční model TCP/IP (nikoliv OSI); namapování jednotlivých vrstev obou modelů je na následujícím nákresu:



1.3 Seznam příloh

Číslo	Název
1	Dokumentace v jednotlivých fázích projektu
2	Architektonické principy MV k 19.11.2015(jedná se o odkaz, není fyzicky přílohou)
3	Bezpečnostní politika informací MD včetně příloh (jedná se o odkaz, není fyzicky přílohou)

ČLÁNEK 2 PŮSOBNOST

2.1. Toto nařízení je vydáváno v souladu s Článkem 10 Služebního předpisu č. 18 státního tajemníka Ministerstva dopravy ze dne 20. prosince 2018 Organizační řád.

2.2. Tyto architektonické principy navazují na požadavky vyplývající z právních předpisů a na architektonické principy stanovované MV. Jsou závazné pro zadavatele a dodavatele IS MD, a to jak IS tvořených pro MD zcela na klíč (např. Registr silničních vozidel, Centrální registr řidičů aj.), tak těch částí IS, které se specificky pro MD vytvářejí nad obecně vytvořenými a více uživateli sdílenými částmi IS (např. ekonomický systém,

personální systém aj.). Při výběru IS, které jsou upravovány pro potřeby MD doplňováním speciálně napsaných částí, by Architektonické principy MD měly být rovněž zohledňovány v míře ekonomicky odůvodnitelné; článek 6 se uplatní obdobně.

2.3. Tvorba a provoz IS MD musí vycházet z právních předpisů, přijaté informační koncepce MD a BPI MD (resp. jejich relevantních částí). Obecné principy IS MD jsou převzaty z požadavků MV, ato jsou:

- dostupnost,
- použitelnost,
- důvěryhodnost,
- transparentnost,
- bezpečnost,
- spolupráce a sdílení,
- udržitelnost,
- technologická neutralita,
- integrita (tzn. provoz systému garantuje integritu dat; není však uváděn ve výše citovaných požadavcích MV k datu vydání tohoto dokumentu).

2.4. Podrobnosti/výklad lze nalézt na stránkách www.mvcr.cz[1]. Architektonické principy požadované MV k 19. 11. 2015 jsou pro uvedeny v příloze, vždy je však nutno pracovat s aktuální verzí publikovanou MV na webových stránkách.

ČLÁNEK 3 ARCHITEKTONICKÉ PRINCIPY PRO DODAVATELE/ PROVOZOVATELE INFORMAČNÍCH SYSTÉMŮ MD

3.1. Dodavatelé IS MD jsou povinni se řídit následujícími architektonickými principy.

3.2. Architektonické principy pro tvorbuIS

a) **Využívat výlučně architekturu „tenkého klienta“**, tj. navrhovat a realizovat IS výhradně tak, aby na straně pracovní stanice uživatele nebylo nutno instalovat žádný pro IS speciálně vytvořený software (preferovaným klientem je standardní webový prohlížeč).

b) **Využívat důsledně vrstvené architektury**, tzn. například při komunikaci s operačním systémem nebo databází lze využívat pouze standardizovaných rozhraní a standardní komunikační protokoly dle RFC.

c) Dokumentace IS musí být komplexní a úplná a musí umožnit instalaci a konfiguraci IS třetí stranou.

d) **IS nesmí vyžadovat pro svůj provoz administrátorská práva k produkčnímu prostředí** serverů a dalšího hardware, virtualizační platformy, operačních systémů a databází; datový model nesmí být dynamicky měněn**.**

e) **Plně oddělit kód IS a data IS**, tj. v kódu IS nesmí být žádné uživatelsky definované konstanty/parametry, odkazy na externí zdroje (např. důvěryhodné certifikační autority) atp. Veškeré možnosti změny nastavení musí být realizovatelné konfiguračně (s autentizací, autorizací i logováním) bez potřeby zásahu do kódu IS.

f) **Použití jen tzv. uzavřených číselníků/roletek** (položka "ostatní" jen v odůvodněných případech), tzn. koncový uživatel nesmí mít možnost „volně“ tvořit

[1]Konkrétní odkaz v době tvorby tohoto dokumentu: http://www.mvcr.cz/soubor/architektonicke-principy-vs-cr.aspx

obsah číselníků. Jedná se především o číselníky/roletky, které umožňují vkládat data, podle kterých se následně třídí, vybírají nebo párují informace. Změna (doplnění, odmazání apod.) číselníků musí být realizovatelná konfiguračně (s autentizací, autorizací i logováním) bez potřeby zásahu do kódu IS; ideálně jako samostatně přidělitelné oprávnění či role v IS (superuživatel).

g) **Zdrojový kód IS musí obsahovat komentáře v relaci s programátorskou dokumentací** minimálně ke každé použité funkci/proceduře/třídě/komponentě na takové úrovni, která umožní orientaci, porozumění kódu a jeho úpravy programátorům, kteří se na vývoji IS nepodíleli.

h) V průběhu přípravy tvorby resp. změny IS bude vytvořen a ze strany Objednatele (věcný odbor MD) schválen **procesní model** fungování zamýšleného IS resp. části IS po změně, který bude obsahovat minimálně popis případů použití, rámcový návrh obrazovek (wireframe) a logický datový model. Procesní model musí být schválen Objednatelem ještě před zahájením programování.

i) **Data musí být ukládána výhradně v databázích** (případně do filesystému) ve struktuře odpovídající datovému modelu a musí být možné jednotlivé datové položky vyhledat a přečíst prostředky databáze (resp. operačního systému), tj. bez nutnosti použít vlastní IS. Přímý přístup do databáze (resp. k filesystému s daty) smí být povolen administrátorovi pro každý jednotlivý případ na základě schválení Manažerem KB.

j) **Komunikace s jinými IS musí být realizována pomocí webových služeb** (web services) s popisem funkcí, vstupů a výstupů v jazyce WSDL.

k) Pro komunikaci přes HTTP smí být **povoleny pouze nezbytné HTTP metody**. Povolené nevyužité metody (např. zapnutí trace) představují zranitelnost a mohou způsobovat nežádoucí účinky (např. při útoku na server) a proto jejich použití musí být omezeno. IS musí splňovat RFC a další definované standardy (např. vyplnění hlaviček včetně flagů, nastavení cookies apod.)

l) IS smí k **síťové komunikaci využívat pouze statických portů** (na serverové straně) TCP nebo UDP portů (dynamické porty na straně serveru neumožňují nakonfigurovat firewall). K síťové komunikaci je možné použít IPv4 i IPv6 (obě alternativy bez nutnosti zásahu do IS).

m) IS musí umožňovat komunikaci s uživateli přes **proxy server**.

n) **Kryptografické prostředky používané IS musí být konfigurovatelné** bez zásahu do kódu IS. Změna kryptografických algoritmů, funkcí a délek klíčů musí být možná bez nutnosti programování v IS.

3.3. Architektonické principy pro provoz IS

a) IS musí být možné variantně provozovat na fyzických serverech a na virtuálních serverech pod Hyper-V a VMware.

b) U použitých technologických komponent jsou v maximální možné míře odstraněny veškeré části, které nejsou nezbytné pro jejich fungování (nejsou instalovány nepotřebné komponenty, aplikační SW, v prostředí nejsou uloženy zdrojové kódy). Instalovány smí být pouze komponenty nezbytné pro provoz, správu a dohled IS.

c) Zajištění provozu a dostupnosti IS a řešení provozních incidentů je definováno v SLA (včetně vyhodnocovacích metrik), který je součástí smlouvy o provozu IS.

d) Musí být definovány postupy a časová okna pro údržbu IS a změnové řízení (Patch Management, Release Management).

3.4. Architektonické principy pro bezpečnost IS

a) IS musí dodržet/naplnit všechna (relevantní) ustanovení platné BPI MD.

b) IS musí zajistit veškeré logování své činnosti minimálně v rozsahu stanoveném zákonem č. 181/2014 Sb. ve znění prováděcích předpisů.

c) IS musí umožnit zasílání veškerých logů do systémů třetích stran (např. SIEM).

d) Umožnit monitoring chování IS včetně možnosti vyhodnocování systémy třetích stran (např. napojení na centrální dohledový systém).

e) Při navazování komunikace mezi jednotlivými moduly IS s různou úrovní ohrožení se vždy navazuje komunikace z modulu s vyšším stupněm ohrožení směrem k modulu s nižším stupněm ohrožení. Obrácená komunikace vyvolaná méně ohroženým modulem se provádí přes vyzvednutí požadavku na komunikaci více ohroženým modulem. Úroveň ohrožení modulu se posuzuje na základě analýzy bezpečnostních rizik.

f) Veškerá komunikace mezi klientem a aplikací a mezi komponentami aplikace musí být šifrována (pokud to není technicky možné, musí být uvedeno a zdůvodněno v dokumentaci včetně případných přijatých opatření proti narušení komunikace). Jsou-li v rámci řešení implementovány loadbalancery pro rozdělení zátěže klientů na aplikační servery, je šifrovaná komunikace klientů ukončena na loadbalanceru (kde musí být umístěn certifikát aplikace), na kterém je případně řešena i inspekce komunikace na aplikační vrstvě. Komunikace z loadbalanceru na jednotlivé aplikační servery musí být opět šifrována (pro ověření stran komunikace a šifrování je zde možné i použití self-signed certifikátů).

g) IS nezobrazuje uživatelům v chybových hlášeních žádné údaje, které by mohly být využity k narušení bezpečnosti (interní adresy, údaje o účtech, jiných uživatelích, ladicí informace a trasování, interní adresy atd.). Hláška chyby musí být taková, aby správce IS poznal jednoznačně specifické okolnosti chyby (potřebné detaily pak musí být dohledatelné v logu), nikoliv aby uživatel obdržel několik stran pro něj nesrozumitelných informací a musel je poskytovat k řízení incidentů.

h) IS kontroluje veškeré své vstupní údaje (včetně URL, cookies, HTTP hlaviček atd.). Ověřuje přípustný rozsah dat, kódování vstupních údajů, délku vstupních údajů a jiné relevantní charakteristiky, které by ho mohly dostat do nestandardního stavu. Zajistí v maximální možné míře, že se nedostanou nebezpečná nebo nekorektní data do zpracování. IS kontroluje veškerá výstupní data a nepovolí výstup dat, která by mohla ohrožovat jiné systémy.

i) IS nedovolí přístup bez autentizace k jakékoli funkci, která autentizaci má vyžadovat (např. přímý přístup při zadání celého URL není možný). Důležité IS (rozhodnutí Architekta KB) musí mít implementovánu dvoufaktorovou autentizaci.

j) U důležitých IS (rozhodnutí Architekta KB) se při přihlášení zobrazuje uživateli informace o čase předcházejícího úspěšného přihlášení a čase posledního neúspěšného pokusu o přihlášení. IS na vyžádání zobrazí uživateli historii úspěšných přihlášení a neúspěšných pokusů o přihlášení. IS musí mít možnost zakázat vícenásobné současné přihlášení téhož uživatele.

k) IS provádí reautentizaci uživatele po určité době nečinnosti. Tato doba je konfigurovatelná a pro důležité IS (rozhodnutí Architekta KB) může být odlišná pro různé kategorie (kombinace rolí) uživatelů (např. editor a čtenář). IS odhlásí uživatele po určité době nečinnosti. Tato doba je konfigurovatelná a pro důležité IS (rozhodnutí Architekta KB) může být odlišná pro různé kategorie (kombinace rolí) uživatelů.

l) Autorizace, povolující uživateli oprávnění k operacím, se provádí vůči jeho roli v IS. IS provádí autorizační omezení přístupu uživatele při každém provádění jakékoli operace či skupiny operací. Pravidlo se neaplikuje na veřejně přístupné operace, kde není potřeba oprávnění k přístupu na operace rozlišovat.

3.5. Architektonické principy pro dokumentaci a eliminaci „vendorlock“

a) IS je/bude implementován do prostředí (operační systémy, databázové stroje, autentizační mechanismy apod.), které je již MD dominantně využíváno.

b) Dodavatel pro vývoj a provoz využije pouze prostředky, které mají zajištěnu dlouhodobou podporu výrobce spolu s perspektivou rozvoje produktu výrobcem.

c) Testovací a provozní prostředí IS (hardware, software) schvaluje (resp. definuje) Objednatel. Schválení Objednatele podléhá i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných).

d) Dokumentace musí být zpracována podle právních předpisů, pravidel OHA MV (viz webové stránky www.mvcr.cz) a interních požadavků MD na dokumentaci, které jsou uvedeny v Příloze č. 1 tohoto nařízení.

e) Dokumentace musí obsahovat minimálně:
- datový model,
- uživatelskou dokumentaci (včetně školicí),
- programátorskou dokumentaci,
- okomentovaný kompletní zdrojový kód IS,
- administrátorskou dokumentaci včetně instalačního manuálu,
- externí knihovny, resp. kódy třetích stran, nezbytné k funkčnímu sestavení IS,
- skripty pro sestavení IS (jsou-li použity),
- bezpečnostní dokumentaci včetně havarijních plánů a plánů obnovy,
- hesla a šifrovací klíče (jsou-li použity),
- Roll-aut plán/Exit strategii,
- provozní deník.

f) IS musí obsahovat uživatelskou dokumentaci on-line dostupnou na obrazovkách.

g) IS musí obsahovat tzv. „info-proužek“ umožňující z centrálního pracoviště provozovatele IS informovat uživatele stručným sdělením v průběhu užívání IS, aniž by činnost uživatelů tímto sdělením přerušovala.

h) Součástí dodávky a její ceny musí být komplexní licenční, resp. další práva k užívání a úpravám dodaných kódů a dokumentací k časově a teritoriálně neomezenému užití (včetně možnosti postoupit je pro účely úprav a rozvoje třetím stranám). Tato práva se musejí týkat i rozvoje dodaného IS.

ČLÁNEK 4 ARCHITEKTONICKÉ PRINCIPY PRO PROVOZOVATELE INFRASTRUKTURY

4.1. Architektonické principy pro vývojové, testovací a provozní prostředí

a) Využívat preferovaně dedikované (privátní) cloudy fyzicky umístěné v ČR.

b) Oddělené zdroje a monitoring jednotlivých provozovaných IS (alespoň virtuálně).

c) Oddělená správa/administrace zdrojů a monitoringu jednotlivých provozovaných IS.

d) Dodavatel/provozovatel využije pouze prostředky, které mají zajištěnu dlouhodobou podporu výrobce spolu s perspektivou rozvoje produktu výrobcem.

e) Dodavatel/provozovatel realizuje prostředí na škálovatelných produktech s možností flexibilní a bezpečné změny (tj. bez nutnosti reinstalace IS, realizovatelné v definovaných maintenance oknech apod.).

f) Testovací a provozní prostředí (hardware, software) schvaluje (resp. definuje) Objednatel. Schválení Objednatele podléhá i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných).

g) Testovací a produkční (a všechna další) prostředí musí být oddělena minimálně na úrovni (virtuálních) serverů i sítě (VLAN, IP).

4.2. Architektonické principy pro provoz infrastruktury

a) Dodavatel musí udržovat aktuální CMDB.

b) U použitých standardních technologických komponent jsou v maximální možné míře odstraněny veškeré části, které nejsou nezbytné pro jejich fungování (nejsou instalovány nepotřebné komponenty, aplikační SW, v prostředí nejsou uloženy zdrojové kódy). Smí být instalovány pouze komponenty nezbytné pro provoz, správu a dohledy IS/infrastruktury.

c) Zajištění provozu a dostupnosti infrastruktury a řešení provozních incidentů je definováno v SLA (včetně vyhodnocovacích metrik), který je součástí smlouvy o provozu prostředí.

d) Musí být definovány postupy a časová okna pro údržbu prostředí a změnové řízení (Patch Management, Release Management).

4.3. Architektonické principy pro dokumentaci infrastruktury

a) Dokumentace musí být zpracována podle právních předpisů, pravidel OHA MV (viz webové stránky www.mvcr.cz) a interních požadavků MD na dokumentaci, které jsou uvedeny v Příloze č. 1 tohoto nařízení.

b) Dokumentace musí obsahovat minimálně:
- datový model včetně popisu umístění dat,
- administrátorskou dokumentaci včetně instalačního manuálu,
- bezpečnostní dokumentaci včetně havarijních plánů a plánů obnovy,
- seznam a popis HW a SW prvků včetně popisu/schématu jejich propojení,
- konfiguraci a typ použitého HW a SW,
- hesla a šifrovací klíče (jsou-li použity),
- informace o licenčních pravidlech použitého SW,
- Roll-aut plán/Exit strategii,

- provozní deník.

4.4. Architektonické principy pro bezpečnost infrastruktury

a) Infrastruktura musí dodržet/naplnit všechna (relevantní) ustanovení platné BPI MD.

b) Infrastruktura musí zajistit veškeré logování své činnosti minimálně v rozsahu stanoveném zákonem č. 181/2014 Sb. ve znění prováděcích předpisů.

c) Komunikace mezi jednotlivými prvky aplikační infrastruktury (tím jsou myšleny servery, loadbalancery apod., nikoliv síťové prvky, firewaly apod.) musí být vždy šifrována (pro ověření stran komunikace a šifrování je zde možné i použití self-signed certifikátů).

d) Prvky infrastruktury musí umožnit zasílání logů do systémů třetích stran (např. SIEM).

e) Umožnit monitoring chování infrastruktury a provozovaných IS včetně možnosti vyhodnocování systémy třetích stran (např. napojení na centrální dohledový systém).

f) Zálohy dat jsou ukládány jinde než na produkčním serveru a pro důležité IS (rozhodnutí Architekta KB) i v jiné lokalitě. Funkčnost obnovy ze záloh musí být pravidelně kontrolována/ověřována.

g) Záznamy o provozu (logy) jsou ukládány pro důležité IS (rozhodnutí Architekta KB) na jiném serveru / zařízení s vlastním operačním systémem, než na kterém jsou záznamy vytvářeny.

h) Testovací, provozní i jakékoliv další prostředí (včetně vývojového), pokud se v něm vyskytují data MD (včetně dat anonymizovaných či pseudonymizovaných), musí být od veřejných i jiných (včetně prostředí pro provoz jiných IS) datových sítí odděleno minimálně jedním firewallem dozorováno IPS.

ČLÁNEK 5 ARCHITEKTONICKÉ PRINCIPY PRO DODAVATELE/ PROVOZOVATELE HELPDESKU

5.1. Architektonické principy pro integrace HelpDesku

a) Pro podporu uživatelů musí mít každý IS MD implementován HelpDesk, který zajistí podporu a evidenci průběhu řešení požadavků uživatelů a incidentů v rámci L1 (základní úroveň podpory), L2 (úroveň s hlubší technickou znalostí systému) a L3 (expertní znalost systému) podpory. V rámci implementace IS je nutné přesně stanovit, kdo bude zajišťovat jednotlivé úrovně podpory, jak budou tyto úrovně spolupracovat a jak bude měřena doba řešení.

b) HelpDesk musí podporovat měření kvality dodavatelem poskytovaných služeb (SLA), včetně reportovacích nástrojů.

c) Pokud se tak MD s dodavatelem dohodne, může dodavatel provozovat vlastní HelpDesk s tím, že do centrálního HelpDesku MD musejí být zasílány veškeré incidenty a informace, které mají vazbu na výše uvedené měření kvality služeb a reportování míry dodržování dohodnutých parametrů kvality služeb (SLA).

5.2. Architektonické principy pro dokumentaci HelpDesku

a) Dokumentace HelpDesku musí splňovat všechny požadavky na IS provozované na MD.

b) Dokumentace provozu/činnosti HelpDesku (může být realizováno např. funkčností aplikace HelpDesku) musí obsahovat úplný průběh řešení požadavku včetně časových záznamů.

ČLÁNEK 6 VÝJIMKY

6.1. Dodavatel může žádat o výjimky z těchto Architektonických principů MD. Výjimky musí dodavatel písemně zdůvodnit (včetně doby trvání výjimky), předložit a požádat o stanoviska Manažera a Architekta KB na odboru ICT (O330). O povolení výjimky, resp. o podmínkách, za kterých je výjimku možno akceptovat, rozhoduje ředitel Odboru ICT MD (O330) na základě výše uvedených stanovisek.

6.2. V případě žádosti o výjimku z ustanovení odkazovaných dokumentů je nutné žádat dle jimi definovaných procesů a o podání takové žádosti informovat ředitele Odboru ICT MD (O330).

ČLÁNEK 7 ZMĚNY INFORMAČNÍCH SYSTÉMŮ MD

7.1. Pokud Dodavatel předkládá MD návrh na změnu IS, která podléhá schválení OHA MV, musí si předem vyžádat stanovisko Manažera KB MD.

7.2. Manažer KB si může po realizaci vyžádat doložení splnění podmínek; nesplnění těchto podmínek může být překážkou v akceptaci, resp. důvodem k neakceptaci dodávky/řešení.

ČLÁNEK 8 PŘECHODNÁ USTANOVENÍ

8.1. Architektura je stanovována jako dlouhodobá, cílová. Pro stávající IS MD platí komplexně pouze v případě zásadní změny IS. Pokud budou prováděny úpravy, je nutné ji použít rovněž, avšak s promítnutím výjimek plynoucích z principu finanční a časové přiměřenosti. Prohlášení o stavu plnění architektonických principů však musí být součástí všech akceptačních protokolů.

ČLÁNEK 9 REVIZE NAŘÍZENÍ

9.1. Revize nařízení se provádí povinně v těchto případech:

a) V rámci aktualizace došlo ke změnám v BPI MD.

b) Byl zjištěn nesoulad s požadavky OHA MV.

c) V rámci řešení incidentu byl identifikován nedostatek v oblasti architektury IS MD.

9.2. V případě, že jsou činnosti uvedené v tomto nařízení upraveny zvláštním právním předpisem, postupuje se podle tohoto předpisu.

ČLÁNEK 10 ZRUŠOVACÍ USTANOVENÍ

10.1. Zrušuje se Nařízení náměstka Sekce legislativně právní č. SŘKB/1, č.j. 1/2019-330-RDK/1, ze dne 22. ledna 2019 „Architektonické principy Ministerstva dopravy“.

ČLÁNEK 11 ÚČINNOST

11.1. Toto nařízení bylo schváleno dne 21. prosince 2020

Mgr. Jakub Kopřiva v. r.
náměstek ministra
Sekce legislativní a právní

Dokumentace v jednotlivých fázích projektů

Tento dokument je součástí metodiky řízení projektů, protože tvorba dokumentace probíhá postupně v rámci životního cyklu projektu. Níže je pak popsáno, který dokument by měl v jaké etapě projektu vzniknout a co by mělo být jeho obsahem.

I. etapa (návrh):

Projektové dokumenty podle rozhodnutí vedoucího projektu nebo zvoleného standardu (např. Základní dokument projektu, Plán projektu, Metodika vedení projektu, zápisy, Katalog rizik, Změnové požadavky)

II. etapa (vývoj):

Školicí příručka, Uživatelská příručka, Instalační příručka, Administrátorská příručka, Systémová dokumentace a Vývojová dokumentace.

III. etapa (Pilotní provoz):

Provozní dokumentace (katalogové listy, způsob zajištění provozní podpory, způsob zajištění podpory uživatelů, způsob měření SLA, provozní deník), projektové dokumenty (především pak zápisy a změnové požadavky, které vzniknou v rámci Pilotního provozu), Závěrečná zpráva/Vyhodnocení Pilotního provozu.

IV. etapa (příprava produkčního provozu):

Aktualizace provozní dokumentace a veškerých dokumentů v návaznosti na změny, provedené v průběhu Pilotního provozu.

V. etapa (podpora nebo zajištění produkčního provozu):

Aktualizace veškerých dokumentů v návaznosti na změny, provedené v průběhu ladění/optimalizace systému).

Poznámky:

1. Projektové dokumenty (Základní dokument projektu, Prováděcí projekt, Závěrečná zpráva/Vyhodnocení Pilotního provozu) se řídí pravidly projektového řízení. Veškeré požadované dokumenty musejí být smluvně zajištěny buď odkazem na příslušný standard, nebo explicitně ve smlouvě.

2. Všechny požadované dokumenty je nutné zahrnout explicitně do smlouvy (stačí odkaz na standard, pokud existuje) a případně v ní ještě detailněji upřesnit obsahovou stránku.

3. Bezpečnostní dokumentace vychází z BPI MD a může být součástí (jednou z kapitol) Administrátorské příručky – viz výše. Schvaluje ji Manažer KB.

4. Upřesnění k obsahu jednotlivých dokumentů (musí být též součástí Release Managementu):

Školící příručka (odpovídá dodavatel)

Slouží pro provádění školení „běžných“ uživatelů, klíčových uživatelů a administrátorů.

Uživatelská příručka (odpovídá dodavatel)

Obsahuje návod práce se systémem, včetně popisu scénářů použití (jak co udělám), menu, obrazovek, chybových stavů.

Instalační příručka (odpovídá dodavatel)

Je rozdělena do několika oblastí, přičemž odkazy mezi jednotlivými dokumenty jsou případně prováděny v části prerekvizity instalace:

1) databáze
   a. popis instalačního balíku, jednoznačná identifikace, obsah
   b. prerekvizity instalace
   c. instalace
      - postup instalace
      - kontrola logů
      - chybové stavy
      - adresářová/DB struktura instalace (kde se co po instalaci nachází)
2) aplikační vrstva (může být rozdělena do částí: webové služby, tenký klient, workflow, plánované úlohy, každá pak obsahuje níže uvedené části)
   a. popis instalačního balíku, jednoznačná identifikace, obsah, popis adresářů pro instalaci
   b. prerekvizity instalace:
      - konfigurace bezpečnostních mechanismů (včetně hesel a šifrovacích klíčů)
      - konfigurace sítě
      - další…
   c. instalace:
      - postup instalace, kontrola logů, chybové stavy, adresářová struktura instalace (kde se co po instalaci nachází)
   d. konfigurace:
      - popis konfiguračních souborů a významu parametrů včetně požadovaného nastavení
   e. konfigurace dohledu a monitoringu
3) klient
   a. popis instalačního balíku, jednoznačná identifikace, co klient obsahuje, popis adresářů pro instalaci
   b. prerekvizity instalace
   c. instalace:

- postup instalace
- kontrola logů
- chybové stavy
- adresářová struktura instalace (kde se co po instalaci nachází)

d. konfigurace:
   - popis konfiguračních souborů
   - význam parametrů včetně požadovaného nastavení.

Administrátorská příručka (odpovídá dodavatel)

Na jejím základě musí být administrátor schopen provádět veškeré činnosti, které jsou nutné pro řádný chod IS včetně zálohování. Zároveň musí obsahovat metodiku pro zjištění, že je IS nefunkční. Akceptuje ji oddělení projektového řízení. Obsahuje:

1) obecné informace o fungování IS
2) databáze
   a. seznam a popis pravidelně prováděných činností
   b. popis využití volání funkcí DB stroje
   c. popis bezpečnostních funkcí a způsobu jejich aplikace
   d. popis log souborů a způsob jejich vyhodnocování
   e. popis chybových stavů a jejich náprava
3) aplikační vrstva
   a. seznam a popis pravidelně prováděných činností
   b. popis využití a volání systémových zdrojů
   c. popis bezpečnostních funkcí a způsobu jejich aplikace
   d. popis log souborů a způsob jejich vyhodnocování
   e. popis chybových stavů a jejich náprava
   f. popis číselníků a jejich význam
4) klient
   a. seznam a popis pravidelně prováděných činností
   b. popis bezpečnostních funkcí a způsobu jejich aplikace
   c. popis log souborů a způsob jejich vyhodnocování
   d. popis chybových stavů a jejich náprava.

Systémová dokumentace (odpovídá dodavatel)

Obsahuje popis fungování systému (resp. jeho jednotlivých modulů) včetně vazeb a způsobu jeho zasazení do IS MD. Je vytvořena zejména pro potřeby integrace s jinými IS. Proto musí obsahovat nejen popis „logiky fungování“ IS, ale i popis rozhraní, chybových kódů s opravnými postupy, metody a postupy škálovatelnosti výkonu a popis log souborů včetně metodiky jejich vyhodnocení. Zároveň musí splňovat požadavky, dané architekturou/architektonickými principy. Je určena zejména pro oddělení provozu, jehož vedoucí ji také akceptuje. Obsahuje:

1) popis funkce a logiky IS včetně návrhu začlenění do stávajícího systému,
2) seznam a popis komunikačních rozhraní, obsahující přinejmenším tyto informace:
   a. komu a k čemu slouží
   b. právní základ (např. ustanovení zákona, nebo ustanovení smlouvy)
   c. datové toky

d. použitá technologie (např. WS SOAP, REST)
e. síťové řešení (např. přímý přístup, loadbalancer)
f. bezpečnost:
    - procesní řízení přístupu (kdo schvaluje, kdo nastavuje)
    - technické řízení přístupu (např. login+heslo, certifikát)
    - způsob a forma komunikace (klient, server)
    - šifrování komunikace (zejména hranice šifrované komunikace, konkrétně použité algoritmy, klíče, Key Management)
    - další ochrana komunikace (např. filtrování provozu na FW)

3) seznam využívaných rozhraní jiných IS
4) popis toku a objemů dat
5) požadavky na změny a nastavení spolupracujících IS
6) bezpečnost, resp. bezpečnostní model:
    a. popis autentizačních a autorizačních mechanismů
    b. definice rolí
    c. popis bezpečnostní architektury (např. oddělení jednotlivých modulů, předávání dat mezi moduly)
    d. pravidla ochrany komunikace (zejména hranice šifrované komunikace, síla šifrovacích algoritmů),
    e. popis logování (co se loguje z infrastruktury, co z aplikace a co z rozhraní, případné napojení na SIEM, kdo a jak logy vyhodnocuje)
7) licenční podmínky.

Vývojová dokumentace (odpovídá dodavatel)

Poskytuje veškeré potřebné podklady pro další rozvoj a údržbu systému. Musí proto obsahovat popis architektury (v souladu s požadavky OHA MV) a veškeré analytické dokumenty, zejména pak:

1) popis stavových diagramů s datovými toky (event- flow diagram)
1) namapování aplikačních objektů na logický datový model
2) namapování logického datového modelu na fyzický datový model
3) podrobná programátorská dokumentace (jednotnou formou komentovaného kódu podle požadavků architektury)

Konkrétní rozsah Vývojové dokumentace může pro daný projekt upřesnit oddělení projektového řízení, které ji také akceptuje.

Provozní dokumentace (odpovídají administrátoři IS)

Dokumentuje průběh produkčního provozu, specifická nastavení konkrétní implementace a veškeré provozní zásahy. Obsahuje:

1) seznam a popis HW prvků včetně popisu/schématu jejich propojení
2) seznam a popis SW prvků včetně popisu/schématu jejich propojení
3) konfigurace a typ použitého HW

4) konfigurace a verze použitého SW (včetně informace o licenčních pravidlech)
5) popis rozmístění dat
6) dokumentace specifických nastavení (např. zálohování, politik pro řízení přístupu apod.)
7) provozní deník - dokumentace veškerých provozních zásahů a úprav (např. změny nastavení, instalace bezpečnostních i jiných oprav operačního systému, databáze či aplikační vrstvy)
8) dokumentace průběžně prováděných testů (např. test funkčnosti záloh)
9) sledování provozu (Log Management), řízení incidentů (Incident Management), řízení změn (Change Management) a řízení konfigurace (Release a Configuration Management)
10) dokumentace změn v prostředí IS a podpůrných systémů (např. změny v antiviru, dohledový systém apod.)
11) havarijní plány a plány obnovy.