

# 1. Aplikační architektura

Kapitola popisuje s použitím typové architektury požadavky na architekturu aplikace.

Cílem standardizace v této oblasti je optimalizace využití zdrojů, snížení nákladů na provoz a údržbu, dodržení požadavků vyplývajících z bezpečnostních standardů a urychlení nasazení nových funkcí a aplikací.

Dále uvedené požadavky je nutné chápat jako doporučený výchozí stav, který může být dále upřesněn při zadání, nebo v průběhu etap (například v rámci analýzy) projektu nasazení konkrétního systému.

## 1.1 Pravidla architektury

Požadavky na architekturu aplikace lze tak shrnout do následujících tezí:

- **centralizace** - aplikace jsou zásadně budované jako centralizované. Konkrétní geografické umístění aplikace je dáno zadáním a potřebami resortu. Rozdělení aplikace, nebo její jedné vrstvy do více geograficky oddělených lokalit se řídí zejména požadavky na dostupnost systému (viz níže uvedená kategorizace systémů)
- **vícevrstvá architektura** - aplikace jsou budovány ve vícevrstvé architektuře, která minimálně odděluje databázovou, aplikační a prezentační vrstvu. Je tak možno efektivněji zajistit rozšiřitelnost informačního systému a dosáhnout též vyššího stupně zabezpečení.
- **IaaS** - architektura aplikace musí být připravena na nasazení do prostředí IaaS. Zejména je nutné, aby bylo možné pro každou aplikační vrstvu přesně specifikovat požadavky na infrastrukturu (s respektováním technologických standardů ICT MPSV).
- **využití služeb** - prostředí ICT MPSV definuje sadu služeb, které je každá aplikace povinna využívat.

## 1.2 Dostupnost systémů

Systémy jsou rozděleny do čtyř tříd podle charakteru provozu. Třídy viz následující tabulka (údaje v rozdělení mají charakter maximálních hodnot):

Třídy dostupnosti		Doba uvedení do provozu (RTO)			
		< 4 hod	< 1 den	< 1 týden*)	> 1 týden*)
Ztráta dat (RPO)	< 4 hod	A	B		
	< 1 den			C	
	> 1 den				D

\*) skutečná doba závisí na smluvních podmínkách (např. na dodávce nového serveru)

Tabulka 1 Třídy dostupnosti

Vysvětlení pojmů:

- **RTO** - maximální doba uvedení systému do provozu po výpadku.
- **RPO** - maximální akceptovatelná ztráta dat. Při klasifikaci je nutno zvážit, zda aplikace obsahuje primární data, nebo zda jsou data součástí jiné aplikace.

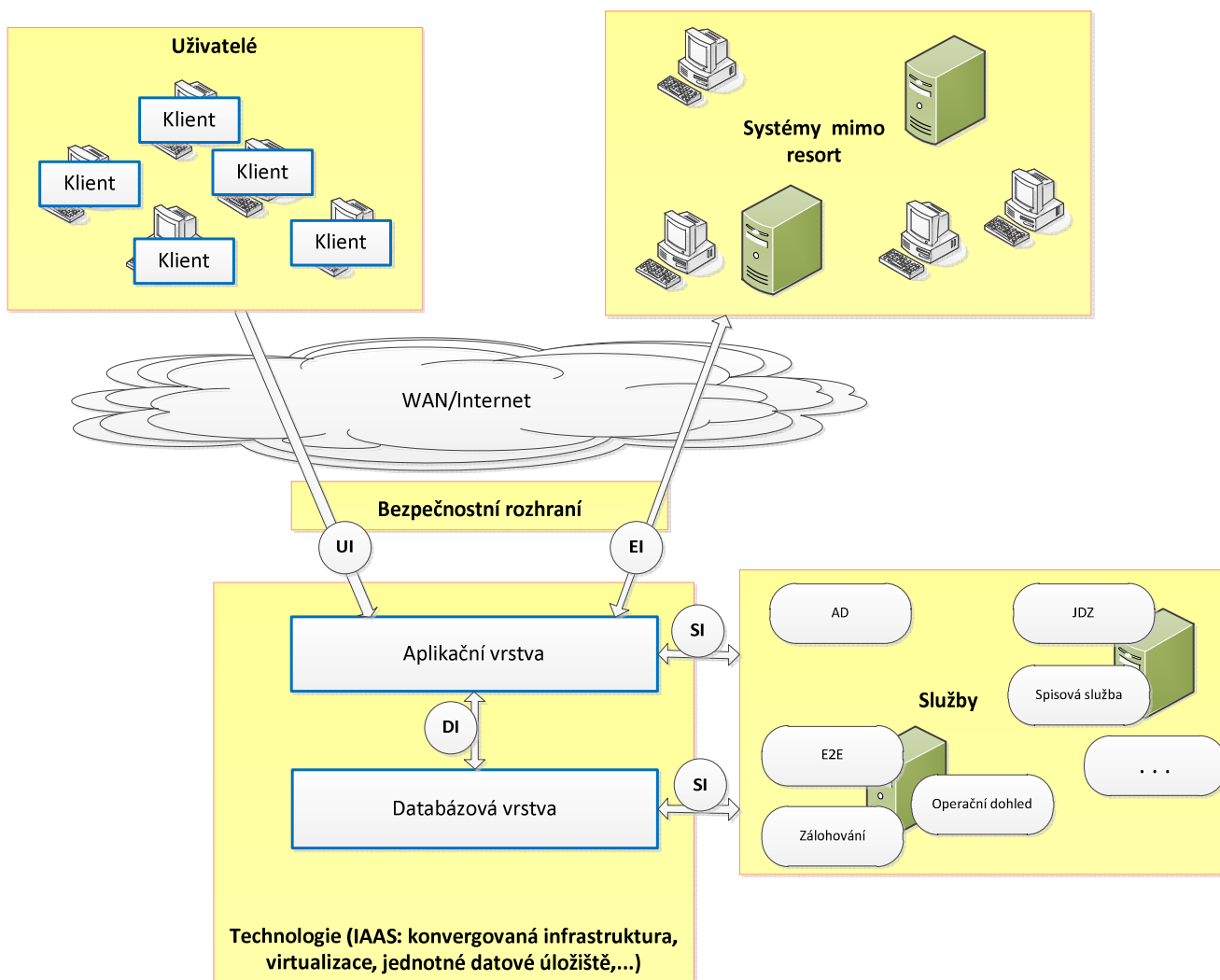
Popis tříd:

- **Třída A** – Hlavní systémy s nejvyšší požadovanou dostupností. Jedná se zejména o IS, pomocí kterých poskytuje MPSV služby klientům prostřednictvím elektronických kanálů (hlavní systémy, většina podpůrných systémů).
- **Třída B** - Hlavní systémy, pro které není nutná nepřetržitá dostupnost.
- **Třída C** - Ostatní systémy, zejména interní systémy, které nejsou bezprostředně třeba pro vykonávání zákonné činnosti MPSV.
- **Třída D** - Systémy, u kterých je akceptovatelný i delší výpadek, resp. MPSV je ochotno nést riziko delšího výpadku.

Každý nově realizovaný systém by měl mít definovanou třídu dostupnosti. Architektura systému je následně navržena tak, aby dané třídě odpovídala.

### 1.3 Zasazení aplikace do prostředí

Následující obrázek ukazuje typové zařazení aplikace do ICT prostředí resortu MPSV. Modře jsou orámovány komponenty aplikace.



Obrázek 1 Aplikace v prostředí ICT MPSV

**Klient** je primárně tenký klient komunikující zabezpečeným protokolem přes WAN síť nebo Internet. Klient musí splňovat:

- technologické standardy, zejména standard pro klienta a pro nasazení SW na koncové stanice,
- požadavky na propojení s aplikační vrstvou (definované rozhraním na obrázku označeným UI), požadavky jsou předmětem samostatného standardu,
- v případě, že je součástí zadání požadavek, aby aplikační vrstva nekomunikovala s klientem přímo, ale prostřednictvím již existující služby (například prostřednictvím Sharepoint, existující agendové aplikace a pod.) musí klient respektovat potřeby a možnosti tohoto koncového systému.

**Aplikační vrstva** je realizovaná jako centralizovaná. Aplikační vrstva musí splňovat:

- technologické standardy, zejména technologický standard pro nasazení aplikační vrstvy a pro instalaci serveru,
- z hlediska dostupnosti a škálovatelnosti se předpokládá možnost nasazení na větší počet fyzických, nebo virtuálních serverů, musí být známy možnosti škálování (nasazení aplikace na více serverů, rozdělení aplikace do více vrstev a pod.),
- aplikace musí respektovat možnost přepínání přístupu k jednotlivým instancím aplikace (tj. k jednotlivým fyzickým nebo virtuálním serverům) externím zařízením, které nebude integrální součástí aplikace (např. Content Switch implementovaný v rámci komunikační infrastruktury),
- nasazení odpovídající kategorii dostupnosti (například na více serverů, geograficky oddělené lokality a pod.),
- aplikační vrstva může být dále rozdělena na vlastní aplikační a na prezentační vrstvu implementovanou v datovém centru,
- v případě geograficky oddělených lokalit musí aplikace respektovat možnost rozdělení komunikačních sítí oddělených na úrovni L2.

**Databázová vrstva** je realizována jako centralizovaná. Databázová vrstva musí splňovat:

- technologické standardy, zejména technologický standard pro nasazení databázové vrstvy a pro instalaci serveru,
- z hlediska dostupnosti a škálovatelnosti musí být definovány možnosti posílení výkonu a realizace HA (více serverů, doplnění uzlů clusteru, pouze rozšířením kapacity serveru),
- nasazení odpovídající kategorii dostupnosti (například na více serverů, geograficky oddělené lokality a pod.)
- v případě geograficky oddělených lokalit musí aplikace respektovat možnost rozdělení komunikačních sítí oddělených na úrovni L2.

**Jako celek** musí dále aplikace splňovat požadavky:

- Požadavky na povinné využití služeb - viz rozhraní SI na obrázku výše, podrobnější informace je uvedena v kapitole 2 Služby prostředí.
- Pokud se jedná o systém přístupovaný uživateli (a to ať přímo, nebo zprostředkovaně např. přes portál) musí být v systému vytvořen uživatel pro testování běhu aplikace a monitorování odezvy pro účely E2E monitoringu.
- Mezi kterýmikoli vrstvami aplikace může být z bezpečnostních důvodů umístěn firewall (minimálně je tak mezi klientem a aplikační vrstvou). Aplikace musí toto respektovat. Pro nasazení aplikace do ICT prostředí definovány všechny datové toky pro rozhraní označená na obrázku UI, EI, SI a DI. V případě rozdělení aplikace mezi více lokalit musí být též definován datový tok probíhající mezi lokalitami v rámci aplikace.

- Aplikace musí poskytovat dokumentovaným způsobem informace o svém stavu, například počet současně přihlášených uživatelů, protokolování chyb, zasílání zpráv o stavu komponenty a pod. Přesná definice musí existovat a být součástí funkční specifikace.

## 2. Služby prostředí

Kapitola popisuje rozhraní SI viz *Obrázek 1*.

Následující tabulka shrnuje služby, které jsou aplikací (systémem) povinně využívány v případě, že tato oblast je implementována.

Služba	Charakteristika	Orientační popis
Identita	povinná pro autentizaci/autorizaci uživatelů	AD nebo LDAP pro zaměstnance resortu
CDES	povinná pro aplikace vyžadující specifický SW na koncových stanicích	systém pro evidenci koncových stanic a distribuci SW balíčků na koncové stanice
zálohování	systém centrálně řízeného zálohování	HP Open View Data Protector
DNS, NTP		

*Tabulka 2 Služby ICT MPSV*

Seznam služeb může být dále upřesňován.

### 3. Typy prostředí

Pro aplikaci, resp. informační systém může být konkrétním zadáním požadováno vytvoření jednoho, nebo více z následujících prostředí. Jejich konkrétní vlastnosti jsou předem definovány a dohodnuty v rámci nefunkčních parametrů systému.

- **Produkční prostředí** - slouží pro provoz aplikace, splňuje všechny funkční i nefunkční požadavky, tj. výkon, dostupnost, využití povinných služeb, bezpečnost atd. Na prostředí je nasazena poslední schválená otestovaná stabilní verze. Prostředí pracuje s platnými daty.
- **Předprodukční prostředí** - slouží pro ověření nových verzí aplikace, mělo by se jednat o prostředí identické s prostředím produkčním. Případné konkrétní odlišnosti od produkčního prostředí musí být definovány nejpozději před zahájením nasazení prostředí. Na prostředí je nasazena verze určená ke schválení a následnému nasazení na produkční prostředí. Rozsah a platnost dat je dána provozním řádem předprodukčního prostředí.
- **Školící prostředí** - slouží k proškolení nových uživatelů a pro školení nových verzí. Prostředí je dimenzováno na předpokládaný počet současně školených pracovníků s dostupností omezenou proti produkčnímu prostředí. Systém obsahuje aktuálně školenou verzi (obvykle stejnou, nebo novější než na produkčním systému). Použitá data jsou školící, tj. neodpovídají produkčním a to zejména v oblasti osobních a citlivých údajů.
- **Testovací prostředí** - testovací prostředí slouží k ověření nových verzí aplikace, k ověření integrace (s dalšími testovacími systémy) a pod. Podle provozního řádu testovacího prostředí mohou být prováděny testy funkční, výkonnostní, bezpečnostní a integrační.
- **Vývojové prostředí** - slouží pro vývoj aplikace.

Pokud aplikace poskytuje uživatelské rozhraní, musí být uživateli vždy zřejmé, s jakým prostředím pracuje.

Která prostředí budou pro konkrétní aplikaci či systém vybudována a s jakými SLA, je definováno v rámci projektu. Zároveň je určen a ze strany MPSV odsouhlasen *Provozní řád prostředí*.