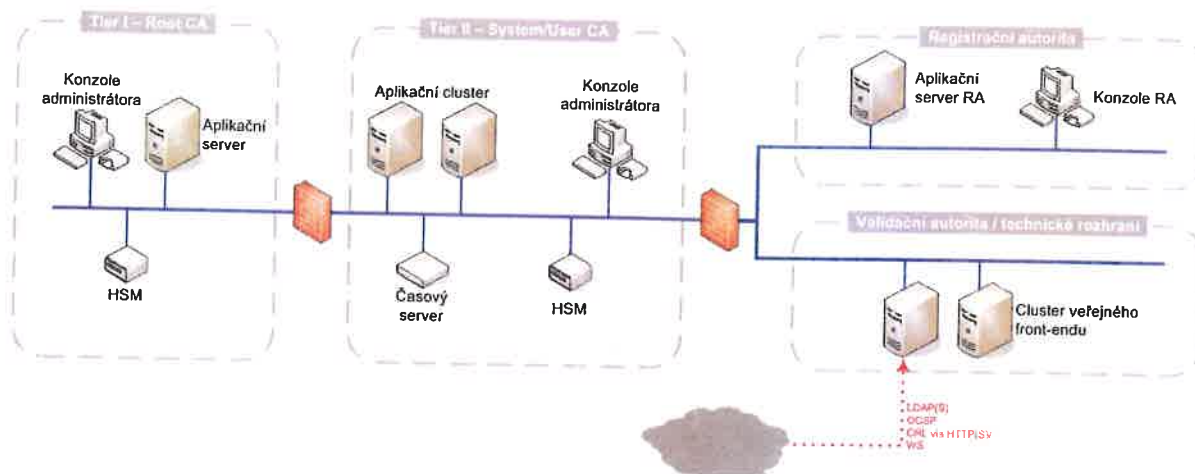


Požadavky na technologické řešení

Na obrázku níže je zobrazen minimální požadavek na síťovou konfiguraci. Tato konfigurace zohledňuje požadavky na bezpečnost (oddělení jednotlivých zón firewally) a dostupnost (clusterování klíčových komponent).



Obrázek 23: minimální požadavek na síťovou konfiguraci CA EET

Auditní záznamy

Systém musí zaznamenávat do auditního logu údaje, vážící se k bezpečnosti provozu.

V rámci provozu CA EET jsou zaznamenávány provozní události následujících typů:

- Události spojené s operacemi v rámci životního cyklu certifikátu
- Události spojené s řízením přístupu k systému CA EET
- Události spojené se změnami konfigurace systémů CA EE
- Události spojené s životním cyklem klienta
- Jiné významné události spojené s provozem systémů CA EET.

V rámci událostí, spojených s operacemi životního cyklu certifikátu, jsou zaznamenávány:

- Zavedení certifikátu
- Generování vlastní žádosti o certifikát
- Zpracování žádosti o certifikát klienta
- Vydání certifikátu
- Export certifikátů.

V rámci událostí, spojených s řízením přístupu k systému CA EET, jsou zaznamenávány:

- Zavedení uživatele
- Správa uživatele (zneplatnění, atd.)
- Úspěšné přihlášení uživatele
- Neúspěšný pokus o přihlášení
- Odhlášení uživatele.

V rámci jiných významných událostí, spojených s provozem systému CA EET, jsou zaznamenávány zejména:

- Spuštění systému CA EET
- Ukončení / přerušení provozu systému CA EET
- Provedení záloh
- Generování párových dat CA EET a certifikátů
- Provozní chyby.

Pro všechny události jsou zaznamenávány identifikace události, čas výskytu události a uživatele, závažnost události.

Události jsou zaznamenávány:

- Elektronicky, v databázi nebo logovacím souboru
- Případně současně v papírové formě (provozní deníky).

V rámci událostí, spojených se změnami konfigurace systému CA EET, jsou zaznamenávány zejména:

- Změny politiky CA EET (událost vedena v provozním deníku)
- Změny konfigurace systémů CA EET (událost vedena v provozním deníku).

Auditní záznamy jsou ukládány v textové podobě s následující strukturou:

- Závažnost události
- Datum a čas vzniku události
- Kategorie typu události (skupina a typ)
- Zdroj – komponenta generující auditní záznam
- Identifikace uživatele
- Identifikace role
- Unikátní číslo události
- Data – údaje blíže popisující zaznamenanou událost (vstupní údaje, výsledek operace apod.).

Integritu auditních záznamů garantuje jejich uložení se zabezpečením přístupových práv.

Po exportu auditních záznamů do archivu bude zachována struktura dat v textové podobě, data bude možno prohlížet standardními editory.

Zálohování, obnova, replikace dat

Dodavatel musí v rámci vývoje systému navrhnout procesy pro:

Replikace kryptografických klíčů

Při návrhu koncepce správy klíčů zvážit metody automatické replikace kryptografických klíčů, které by garantovaly sdílení stejných kryptografických klíčů ve všech HSM pracujících ve společném clusteru.

Replikace obsahu databáze

Za provozu musí být replikována databáze na oba uzly clusteru, případně bude cluster pracovat nad sdíleným diskovým polem.

Při ukončení činnosti na aktivním systému CA EET daného dne musí být provedena replikace (záloha) obsahu relevantních tabulek databáze pro přenos na Záložní systém.

Možnosti konfigurace

Z hlediska možností konfigurace musí CA EET:

- být konfigurovatelná pro použití všech přípustných kryptografických algoritmů
- mít konfigurovatelná uživatelská oprávnění
- být vybavena konfigurovatelným firewallem pro vytváření bezpečných komunikačních kanálů
- mít možnost ručně korigovat nastavení systémového času
- mít možnost konfigurovat profil vydávaného certifikátu
- musí mít možnost konfigurovat vytváření záznamů o provozu systému a činnostech uživatelů.

Požadavky na role a procesy

Dodavatel CA EET navrhne:

- strukturu důvěryhodných rolí pro obsluhu CA EET,
- jejich náplň činnosti,
- požadavky na slučitelnost a neslučitelnost rolí,
- procesy vyžadující součinnost více rolí

Dále dodá odhad pracovního vytížení pro jednotlivé role.

Požadavky na dokumentaci

Dodavatel CA EET zhotoví:

- Analytickou dokumentaci, tj:
 - Analýza technického řešení CA EET
 - Analýza rizik
 - Analýza bezpečnostních požadavků
 - Bezpečnostní projekt
 - Systémová bezpečnostní politika
 - Projekt technického řešení CA EET
- Provozní dokumentaci, tj.
 - Systémová příručka
 - Uživatelské příručky pro jednotlivé role
- Bezpečnostní dokumentaci, t.j.
 - Směrnice pro technickou bezpečnost
 - Směrnice pro netechnickou bezpečnost
 - Směrnice pro reakci na incidenty
 - Směrnice pro kontinuitu činností.

Bezpečnostní směrnice pro jednotlivé role.

Pro případ, že by byl považován CA EET za obecný informační systém veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, je pro splnění požadavků tohoto zákona požadováno:

- Systémová příručka popisuje způsob instalace, uvedení do provozu, pravidelné údržby a administrátorských úkonů na systému. Plní zároveň úlohu Systémové příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.

- Uživatelské příručky pro jednotlivé role popisují provádění jednotlivých úkonů v běžném provozu CA EET pracovníky v příslušných rolích. Pro každou roli je zpracována samostatná příručka. Plní zároveň úlohu Uživatelské příručky ve smyslu zákona č. 365/2000 Sb., a vyhlášky č. 529/2006 Sb.

Požadavky na školení

Součástí dodávaného systému bude příprava a provedení školení uživatelů a administrátorů jednotlivých částí dodávaného systému.

Součástí přípravy školení bude vytvoření dokumentace pro účastníky jednotlivých školení.

Veškerá školení budou provedena v dohodnutých termínech před zahájením ostrého provozu.

Součástí dodávaných školení nejsou konkrétní produktová školení dodávaná jednotlivými dodavateli hardware a software. Pokud objednatel uzná za nutné, aby obsluha a uživatelé byli vyškoleni v těchto produktech, doporučujeme přímo kontaktovat jednotlivé dodavatele, kteří nabízejí celou řadu školení a certifikačních programů.

Požadavky na hardwarové prvky prostředí

Aplikační server

Předpokládá se využití virtualizovaného řešení v rámci realizace samostatných serverů a jejich redundance. Umístění Certifikační autority bude logicky odděleno od ostatních systémů s využitím bezpečnostních aktivních prvků realizovaných v rámci komunikační infrastruktury EET.

Minimální konfigurace jednoho serveru:

Parametr	Doporučená hodnota
Virtualizace	Virtualizační prostředky schodné s celkovým pojetím virtualizace EET
Operační systém	systém unixového typu (RHEL, SUSE Linux ES, Debian Linux apod.)
CPU	architektura x86/x86-64, parametry dle doporučení pro operační systém
Paměť	Minimálně 8 GB na server
Disková kapacita	Vyhrazená disková kapacita , minimálně 1000 GB v RAID I konfiguraci
Síťové připojení	100/1000 MBit/s

HSM

Hardwarový bezpečnostní modul je základním kamenem návrhu certifikační autority. Zařízení musí být schopno generovat, ve spolupráci s hlavním HSM modulem, náhodné soukromé klíče a bezpečně je uchovávat. Veškeré operace vyžadující tyto klíče probíhají ve vnitřním výpočetním prostředí HSM, a tudíž klíče v čitelné podobě nikdy HSM neopouštějí.

Zálohování/obnova vnitřních dat HSM je citlivou operací a musí umožnit duplikaci dat na záložní zařízení pro potřeby zajištění vysoké dostupnosti anebo export obsahu zašifrovaného pomocí klíčů.

HSM zařízení musí mít odpovídající úroveň certifikace.

Požadovaná infrastruktura pro aplikační prostředí EET

Aplikační prostředí a potřebná infrastruktura bude dělena minimálně do následujících zón:

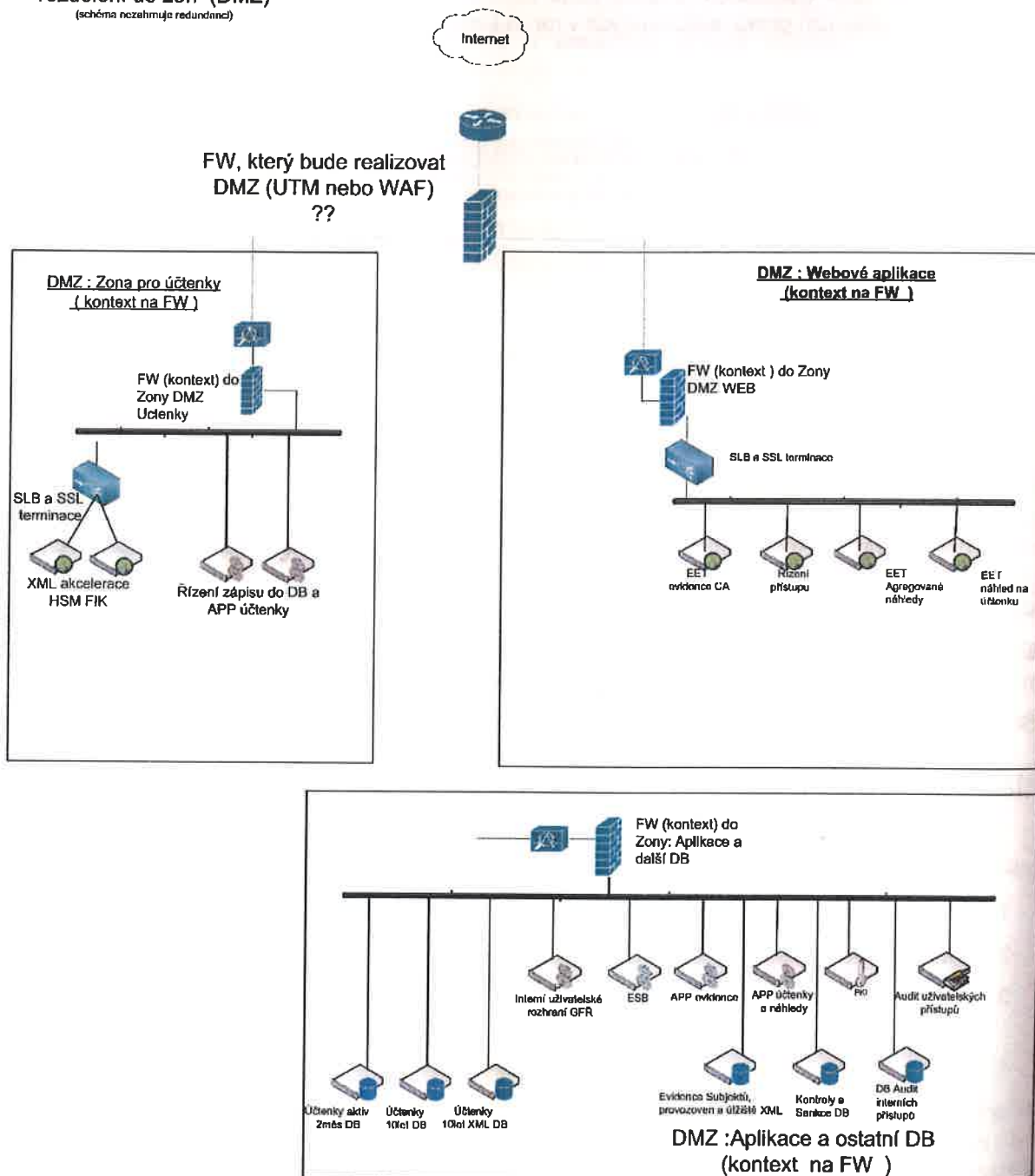
1. DMZ 1 – Zóna pro zpracování účtenek a vystavování evidenčního bezpečnostního kódu FIK
2. DMZ 2 – Webové aplikace. Webový uživatelský portál pro potřeby aplikačního rozhraní EET
3. APP a DB – realizace ESB sběrnice pro orchestraci služeb, aplikační servery pro jednotlivé požadované služby, interní uživatelské rozhraní, databázové prostředí
4. CA – certifikační autorita

Základní požadavkem na infrastrukturu EET je maximální virtualizace zdrojů, redundance jednotlivých částí infrastruktury v jednotlivých zónách. Pro virtualizované prostředí je předpokládáno možnost přesouvání jednotlivých virtualizovaných zdrojů mezi jednotlivými zónami.

Schéma základních zón

Základní schéma zón s rozdělením požadované funkcionality je patrné z následujícího obrázku:

Logické schéma
komunikační infrastruktury,
rozdělení do zón (DMZ)
(schéma nezahrnuje redundanci)



Obrázek 24: Základní schéma zón systému EET

Schéma logické komunikační infrastruktury

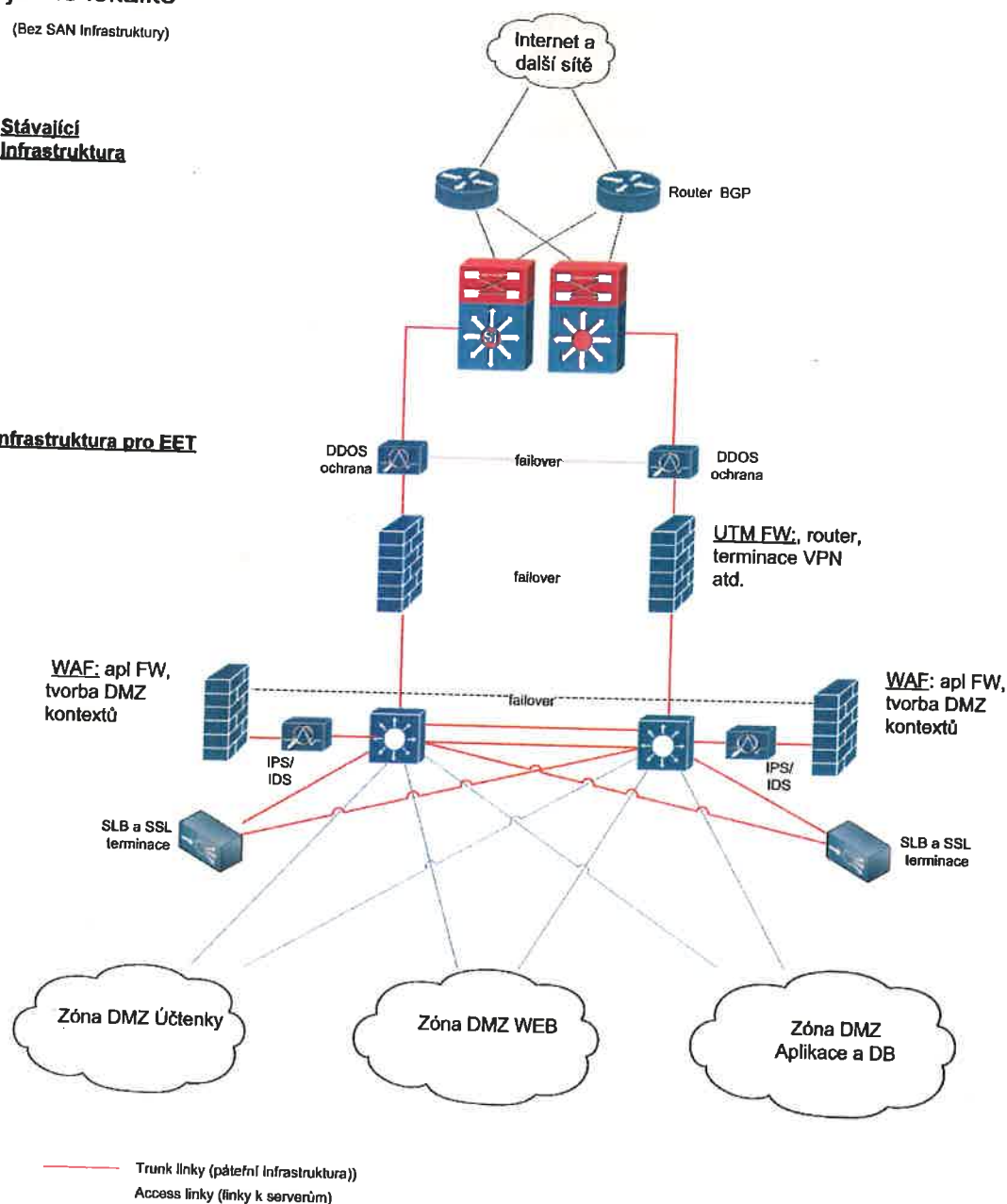
Základní schéma logické komunikační infrastruktury je uvedeno na následujícím obrázku:

Logické schéma
komunikační infrastruktury,
Páteří infrastruktura v
jedné lokalitě

(Bez SAN infrastruktury)

**Stávající
Infrastruktura**

Infrastruktura pro EET



Obrázek 25: Schéma logické komunikační infrastruktury systému EET

Komunikační infrastruktura

- Propustnost prvků 4 Gbps
- Páteří switche s propustností 10 Gbps na portech s možností použití 1/10 Gbps rozhraní (optika, metalika)
- Zdvojená architektura
- Použití UTM - routovací funkce, Firewall, ukončení VPN – žádné další funkce nelze použít z důvodu garantování propustnosti zařízení
- Použití IPS/IDS – na základě požadavků zákona o kybernetické bezpečnosti a pro ochranu operačních systémů a middleware před sofistikovanými útoky.
- SSL terminace na Loadbalancerech (LB),
- Pro přístup na webové rozhraní použít WAF – ve spolupráci s LB
- SIEM – analýza nebezpečného chování/pokusů o průnik – viz zákon o kybernetické bezpečnosti
- Out of band management všech prvků z bezpečnostních důvodů (OOB).

Požadavek na použití **dedikovaných zařízení** pro následující funkce

- **DDOS ochrana** - je specifická, protože musí rozeznat SSL flood od regulérního SSL provozu aplikace. Toho lze dosáhnout jedině tak, že IPS nebo WAF dokáže pracovat jako sonda DDOS ochrany a indikovat včas pakety, které jsou vadné a svědčí o SSL útoku. DDOS podle indikace vytvoří pravidlo a škodlivé SSL pakety odfiltruje.
- **Firewall & routing** (ASIC na akceleraci) jsou to hlavní dvě funkce používané z UTM, UTM musí mít alespoň 100 virtuálních nezávislých firewallů s centrálním managementem a reportingem (vhodné realizovat separátními zařízeními)
- **Switching** (VLAN separace)
- **Switching pro OOB** (management prvků mimo provozní komunikační kanály – garantuje bezpečnost a navíc umožňuje spravovat jednotlivé prvky bez ohledu na jejich vytížení/zatížení/zahlcení v provozních kanálech, stačí porty 100/1000 Gbps)
- **IPS/IDS** (60000 connections /s) – chrání operační systémy a middleware před útoky/zneužitím jejich slabín
- **LoadBalancing** – Ukončení SSL (7000 connections a ASIC akcelerací pro ukončení SSL) – rozkládá zátěž
- **WAF** – chrání webové aplikační servery před zneužitím slabín v aplikacích (např. vytváření neregulérních komunikačních jader přes které lze vyčítat data), dataminingem, zneužitím SQL jazyka, může ukončovat SSL sizing odpovídá IPS/IDS, loadbalancerům a očekávané zátěži webových aplikačních serverech.
- **SIEM** – korelační analýza logů prováděná za účelem odhalení nebezpečných jevů vedoucích k odhalení útoků a zneužití.

XML appliance - B2B, webové a aplikační servery

Pro oblast řešení B2B komunikace s v rámci komunikace pokladních systémů s prostředím EET je požadována takové řešení, která bude sjednocovat potřebnou funkcionalitu spojenou s příjmem účtenky ve formátu XML certifikátem, kontrola certifikátu ve vztahu k účtence, kontrola správnosti XML, vystavení bezpečnostního kódu (FIK) a jeho odeslání v rámci kompaktního řešení a splňovat požadavky spojené se zabezpečením vystavování FIK odpovídající certifikacím pro HSM zařízení a uložení účtenky s FIK do databáze společně s podepsaným XML. Detailní popis procesu je součástí popisu požadovaných procesů.

Zařízení musí splňovat minimálně bezpečnostní certifikaci Common Criteria (EAL4) FIPS 140-2 level 3. Řešení musí splňovat požadavky vysoké dostupnosti a výkonnostní požadavky definované pro EET.

Pro **zabezpečenou oblast** zpracování XML dat v rámci evidence zaslaných účtenek je potřeba zpracovávat masivní datové toky generované vysokým počtem povinných subjektů a jejich pokladních systémů zasílajících XML soubory podepsané příslušným certifikátem. Pro náročnou úlohu ověřování XML a certifikátů je nutné zařízení, které maximálně akceleroje prováděné operace, které je schopno kumulovat několik funkčních požadavků oblasti propustnosti a bezpečnosti. Pro oblast bezpečnosti je nutné zajištění takových podmínek, aby byla zajištěna ochrana vložených **bezpečnostních kódů, nutných pro požadovanou funkcionalitu v rámci vystavování bezpečnostního kódu FIK**. Podmínkou oddělení zmíněných generických úkonů s aplikačními daty z aplikačního serveru na HW zařízení tzv. **SOA appliance, je vysoký výkon při zpracování XML dat a vysoká míra zabezpečení**. **DataPower SOA appliance** koncentruje požadovanou funkcionalitu tak, že zpracování XML je podpořeno HW akcelerátorem a integrovanými bezpečnostními vlastnostmi včetně integrovaného HSM modulu. Požadované užití v prostředí EET je typické případem, kdy zařízení DataPower zajišťuje zejména integraci systémů s externími entitami (B2B/B2G):

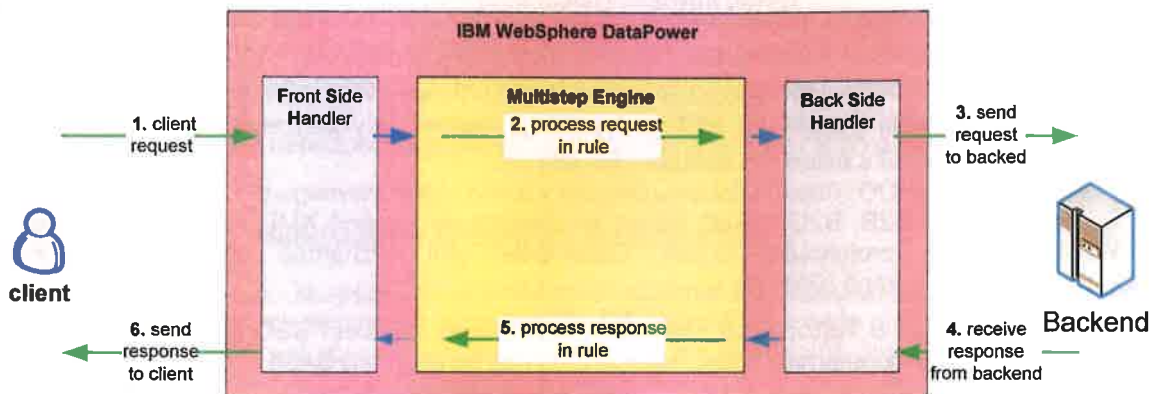
- Při implementaci B2B, B2G a B2C řešení založených na výměně XML zpráv např. s využitím WebServices a protokolem SOAP, DataPower plní významné bezpečnostní funkce v demilitarizované zóně (DMZ)
 - **Autentizace & Autorizace** požadavků a případné vytváření **SSO** tokenů pro propagaci identit od proprietárních řešení jako je LTPA až po standard SAML
 - **Validace zpráv** – např. zpráva musí být validní XML, následně validní SOAP, a také obsah (přenášená data) musí být validní podle XML schématu
 - **Digitální podpis a validace digitálního podpisu** pro zajištění **nepopiratelnosti zprávy**
 - **Šifrování a dešifrování** obsahu zprávy za pomoci integrovaného HSM modulu tak, aby byla uchráněna citlivá data před zneužitím
 - **Ochrana před XML útoky – při tvorbě B2B řešení a obecně je nutno uvažovat, že se často vystavují služby systémů, které nikdy nebyly k podobnému účelu určeny!**
 - Terminace **HTTPs** protokolu
 - Transformace formátu dat pro komunikaci s externí entitou na interní formát a opačně
 - Audit zpráv
- V rámci implementace portálového řešení EET, je žádoucí využít DataPower v demilitarizované zóně k řešení:
 - **Autentizace & Autorizace** požadavků a případné vytváření **SSO** tokenů pro propagaci identit od proprietárních řešení jako je LTPA až po standard SAML.
 - **Validace zpráv** – např. zpráva musí obsahovat data validní XML podle definovaného XML schématu.
 - Akcelerace **XSLT** transformací a snížení latencí spojených se zpracováním digitálního podpisu.
 - Ochrana před různými útoky (**XML threats**) – např. SQL injection.
 - **Loadbalancingu** požadavků na backend systémy.
- Implementace portálových a reportovacích řešení postavených na **XSLT**
 - Síla HW akcelerátoru pro XSLT v zařízení DataPower může pomoci ušetřit zdroje aplikačního serveru a snížit latence zpracování požadavků.

IBM WebSphere DataPower je SOA appliance, kterou je možno použít v závislosti na požadavcích zejména jako:

- Enterprise Service Bus (ESB) nebo jako jeho doplněk
- Bezpečnostní zařízení v demilitarizované zóně k ochraně interních systémů

Základní funkcionality DataPower

IBM WebSphere DataPower je možno si představit jako prostředníka (intermediary) ve zpracování požadavků. Klient (service requester) komunikuje na jedné straně se zařízením DataPower a na druhé straně zařízení DataPower komunikuje s poskytovatelem služby (service provider) na backend systému.



Princip práce zařízení DataPower

Na obrázku je vidět, že zařízení DataPower pracuje na principu Proxy.

Front Side Handler (FSH) zajišťuje komunikaci s klientem. DataPower se tak může přizpůsobit protokolu, který klient používá – např. http/https, ftp nebo MQ, WebSphere JMS, Tibco EMS. Komunikaci s backend systémem zajišťuje **Back Side Handler**. Vlastní logika zpracování zprávy je prováděna v tzv. **Multistep Engine**, který leží mezi **Front Side Handlerem** a **Back Side Handlerem**. **Multistep Engine** tak může zpracovat jak příchozí požadavek klienta před jeho propuštěním na backend system tak i odpověď vrácenou backend systémem před odesláním klientovi. Je například možno provést při zpracování požadavku autentizaci a autorizaci a rozhodnout, zda bude požadavek na backend system předán. Podobně při zpracování odpovědi je možno zprávu **digitálně podepsat**.

- 1) **DataPower: Multistep Engine** zpracuje zprávu požadavku nakonfigurovanou bezpečnostní a integrační logikou:
 - a) autentizace a autorizace
 - b) validace XML (metriky XML, validace schématu, externí reference...)
 - c) kryptografie (digitální podpis a šifrování na úrovni zprávy)
 - d) obohacení zprávy na základě volání jiné webové služby (enrichment)
 - e) Service Level Management (SLM)
 - f) content based routing
 - g) transformace obsahu zprávy
 - h) záznam požadavku pro účely auditu
- 2) **DataPower: Multistep Engine** předá výsledek zpracování na **Back Side Handler (BSH)**.
- 3) **DataPower: Back Side Handler (BSH)** přepošle zpracovanou zprávu na backend systém
 - a) Předávají se jen a pouze validní požadavky splňující nastavená pravidla – požadavky nesplňující nastavenou politiku služby se na backend nepropouštějí (firewalling).
- 4) **Backend:** Zpracování požadavku, vytvoření odpovědi a její zaslání zpět na **Back Side Handler**
- 5) **DataPower: Back Side Handler (BSH)** Akceptování odpovědi backend systému a přijetí dat/zprávy.
- 6) **DataPower: Back Side Handler (BSH)** Předání zprávy odpovědi na **Multistep Engine**.

- 7) **DataPower: Multistep Engine** zpracuje zprávu odpovědi nakonfigurovanou aplikační logikou (např. digitální podpis, šifrování nebo transformace obsahu). U synchronních operací má k dispozici Multistep Engine i data (zprávu) požadavku.
- a) validace XML (metriky XML, validace schématu, externí reference...)
 - i) validace odpovědi patří k důležité best practice v bezpečnosti webových služeb
 - b) obohacení zprávy na základě volání jiné webové služby (enrichment)
 - c) transformace obsahu
 - d) kryptografie (digitální podpis a šifrování na úrovni zprávy)
 - e) audit
 - i) Často se DataPower využívá k auditování vybraných dat ze zprávy požadavku a odpovědi (případně komunikačních metadat jako je identita klienta)
- 8) **DataPower: Multistep Engine** předá výsledek zpracování zprávy odpovědi na **Front Side Handler**.
- 9) **DataPower: Front Side Handler (FSH)** předá výslednou zprávu odpovědi pomocí komunikačního protokolu (např. SOAP message pomocí protokolu HTTP).
- 10) **Klient:** Zpracuje data odpovědi od zařízení **DataPower**

Variace vlastností DataPoweru je využita při návrhu B2B rozhraní systému EET pro sběr účtenek.

Podporované protokoly a standardy

1. Transport a konektivita
 - HTTP, HTTPS, WebSocket Proxy
 - FTP, FTPS
 - SFTP
 - WebSphere MQ and WebSphere MQ File Transfer Edition (MQFTE)
 - TIBCO EMS (Integration and B2B appliances)
 - WebSphere Java™ Message Service (JMS)
 - IBM IMS™ Connect, IMS Callout
 - NFS
 - DB2®, Microsoft SQL Server, Oracle, Sybase, and IMS database connectivity
 - IPv4, IPv6
 - Link Aggregation Control Protocol (LACP) IEEE 802.1ax, 802.3ad
 - Virtual LAN (VLAN) IEEE 802.1q
 - 10G Ethernet IEEE 802.3-2008
 - 1G Ethernet IEEE 802.3ab
 - Dynamic Host Configuration Protocol (DHCP)
 - SSH File Transfer Protocol (SFTP) Support

Podporované protokoly jsou následující:

- SSH-2 protocol definovaný IETF RFC 4251
- SFTP verze 3 definovaný podle draft-ietf-secsh-filexfer-02.txt Internet-Draft

2. Enforcement bezpečnostní politiky

- OAuth 2.0
- SAML 1.0, 1.1 and 2.0, SAML Token Profile, SAML queries
- XACML 2.0
- Kerberos, SPNEGO
- RADIUS
- LDAP versions 2 and 3
- Lightweight Third-Party Authentication (LTPA)
- Microsoft Active Directory
- Federal Information Processing Standard (FIPS) 140-2 Level 3 (with optional Hardware Security Module)
- FIPS 140-2 Level 1 (with built-in cryptographic software module)

- SAF and IBM RACF® integration with z/OS®
- Internet Content Adaptation Protocol (ICAP)
- W3C XML Encryption
- W3C XML Signature
- S/MIME encryption and digital signature
- WS-MediationPolicy, versions 1.6, 1.7, 1.8, and 1.9
- WS-Security 1.0, 1.1
- WS-I Basic Security Profile 1.0, 1.1
- WS-SecurityPolicy
- WS-SecureConversation 1.3

3. Webové služby

- WS-I Basic Profile 1.0, 1.1
- WS-I Simple SOAP Basic Profile
- WS-Policy Framework
- WS-Policy Attachments: Message Content Filters 1.3 (IBM standard)
- WS-Policy 1.2, 1.5
- WS-Trust 1.3
- WS-Addressing
- WS-Enumeration
- WS-Eventing
- WS-Notification
- Web Services Distributed Management (WSDM)
- WS-Management
- WS-I Attachments Profile
- SOAP Attachment Feature 1.2
- SOAP with Attachments (SwA)
- Direct Internet Message Encapsulation (DIME)
- Multipurpose Internet Mail Extensions (MIME)
- XML-binary Optimized Packaging (XOP)
- Message Transmission Optimization Mechanism (MTOM)
- Universal Description, Discovery, and Integration (UDDI versions 2 and 3), UDDI version 3 subscription
- WebSphere Service Registry and Repository (WSRR)

4. Transport Layer Security (SSL and TLS)

- SSL version 2 (deprecated)
- SSL version 3
- TLS versions 1.0, 1.1, and 1.2 (hardware accelerated on physical appliances)

5. Public key infrastructure (PKI)

- RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
- PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
- XKMS for integration with Tivoli® Security Policy Manager

6. Management

- Simple Network Management Protocol (SNMP)
- SYSLOG
- Secure Shell (SSH)
- Intelligent Platform Management Interface (IPMI)

Realizace webových a aplikačních serverů je doporučeno řešit na virtualizované platformě x86 se zajištěním požadavku vysoké dostupnosti. Žádný server nebude mít lokální diskový systém a musí být napojen do SAN/NAS via FC za pomoci běžně používaných protokolů.

Navržené řešení musí umožňovat horizontální škálovatelnost.

Databázové servery a úložiště

Databázové servery musí splňovat požadavky vysoké dostupnosti včetně diskového úložiště umožňujícího „tierování“ jednotlivých diskových prostor v automatickém režimu. Databázové prostředí musí umožňovat ukládání velkého objemu dat jak co do počtu ukládaných záznamů tak co do velikosti uložených dat. Databázové nebo storage funkcionalita musí umožnit online replikaci dat do druhého úložiště.

Požadavky na minimální konfiguraci

		Platforma	Minimální počet jader fyzického serveru	Minimální paměť fyzického serveru	Minimální celkový počet jader virtuálního prostředí	Minimální velikost paměti virtuálního prostředí	
Webové a aplikační servery	Varianta 1	x86	16	64 GB	80	320 GB	
	Varianta 2	RISC	20	256GB	60	768 GB	
Databázové servery	Varianta 1	x86	72				Exadata
	Varianta 2	RISC	24	1TB	48	2TB	IBM
Virtualizovaná platforma (CPS)	Varianta 3	X86	-	-	270	552GB	MS

Minimální konfigurace aplikačních a databázových serverů je počítána bez výkonových nároků virtualizačních řešení.

Minimální kapacita Storage je požadována na 4-leté období provozu systému včetně diskových prostorů přiřazení pro jednotlivé virtuální stroje a virtualizační platformu s kapacitou 144 TB s možností rozšíření celkové kapacity na deseti násobek. Pro potřeby zajištění vysoké propustnosti je požadovaná minimální kapacita 2 TB na SSD. Požadované kapacity jsou netto kapacity dostupné pro systémy. Raw kapacita je závislá na konkrétním řešení diskových systémů.

SAN switching

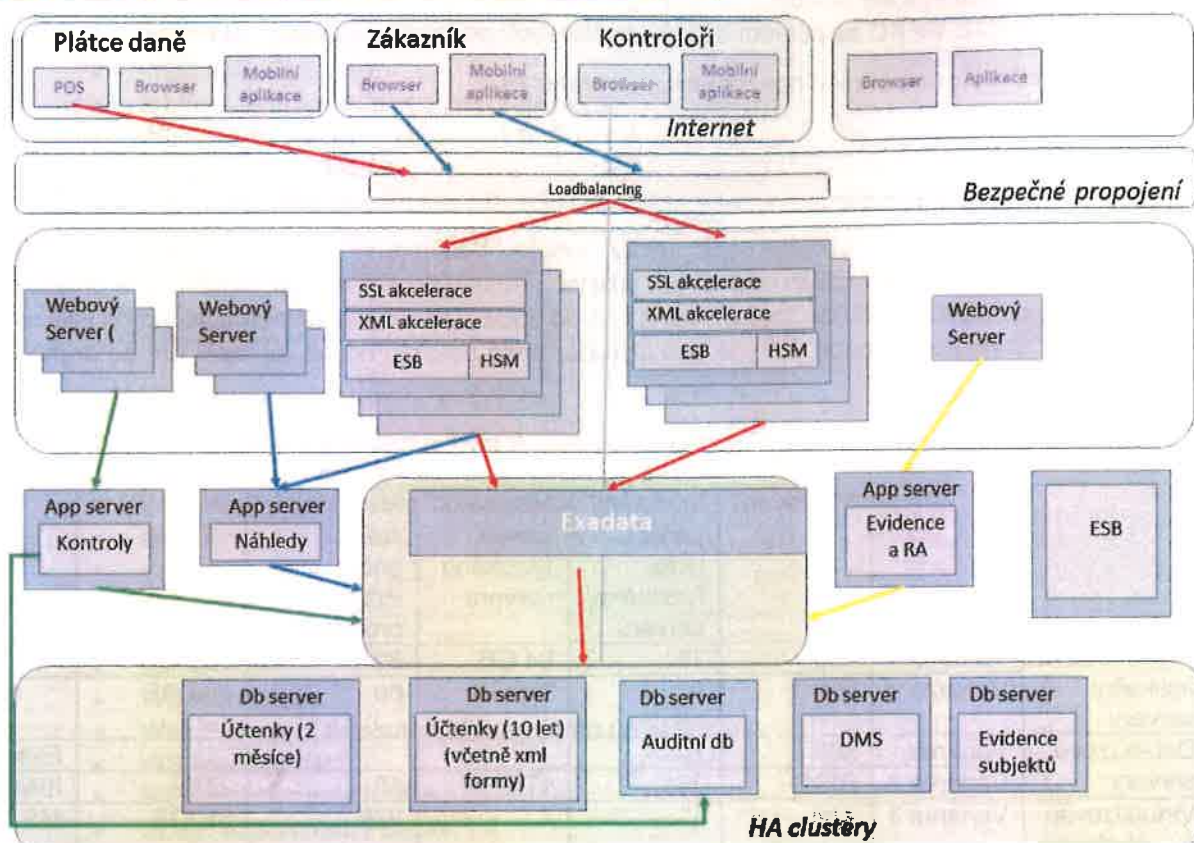
V rámci dodávky je požadováno dodání 4x SAN switch 48 port 8/16Gb.

Zapojení SAN switchů bude zajišťovat SAN FC redundantní infrastrukturu a to v každém ze dvou datových sálů datového centra SPCSS. To znamená, že každý sever bude mít vždy dvě FC spojení na datové úložiště.

Kabeláž

Požadavky na kabeláž musí být definovány v první fázi realizace projektu.

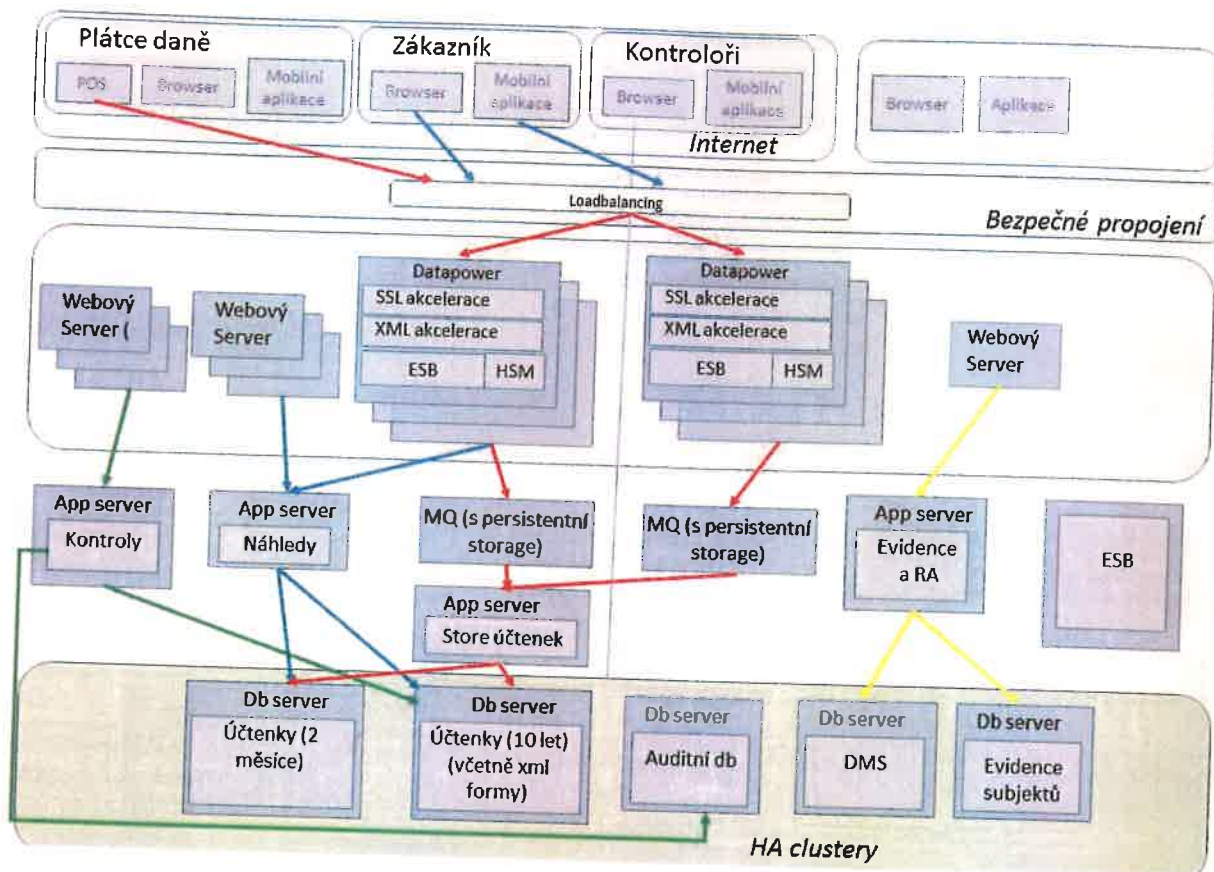
Varianta 1 aplikační vrstvy a Varianta 1 databázové vrstvy



Obrázek 26: Schéma aplikační a databázové vrstvy Varianty 1

Varianta 1 je postavena na platformě x86 a na konsolidovaném produktu ExaData, který realizuje kompaktní databázové prostředí. Aplikační a databázová oblast je řešena jako samostatné celky, kde aplikační oblast je plně virtualizována umožňuje dynamicky alokovat potřebný výkon určeným aplikačním virtuálním serverům. Databázové prostředí ExaData s databází Oracle umožňuje pracovat konfigurovat potřebná databázová prostředí dle aktuálních požadavků aplikace.

Vizualizace možného řešení pro Variantu 2 aplikační vrstvy a Varianty 2 databázové vrstvy kombinace



Obrázek 27: Schéma aplikační a databázové vrstvy Varianty 2

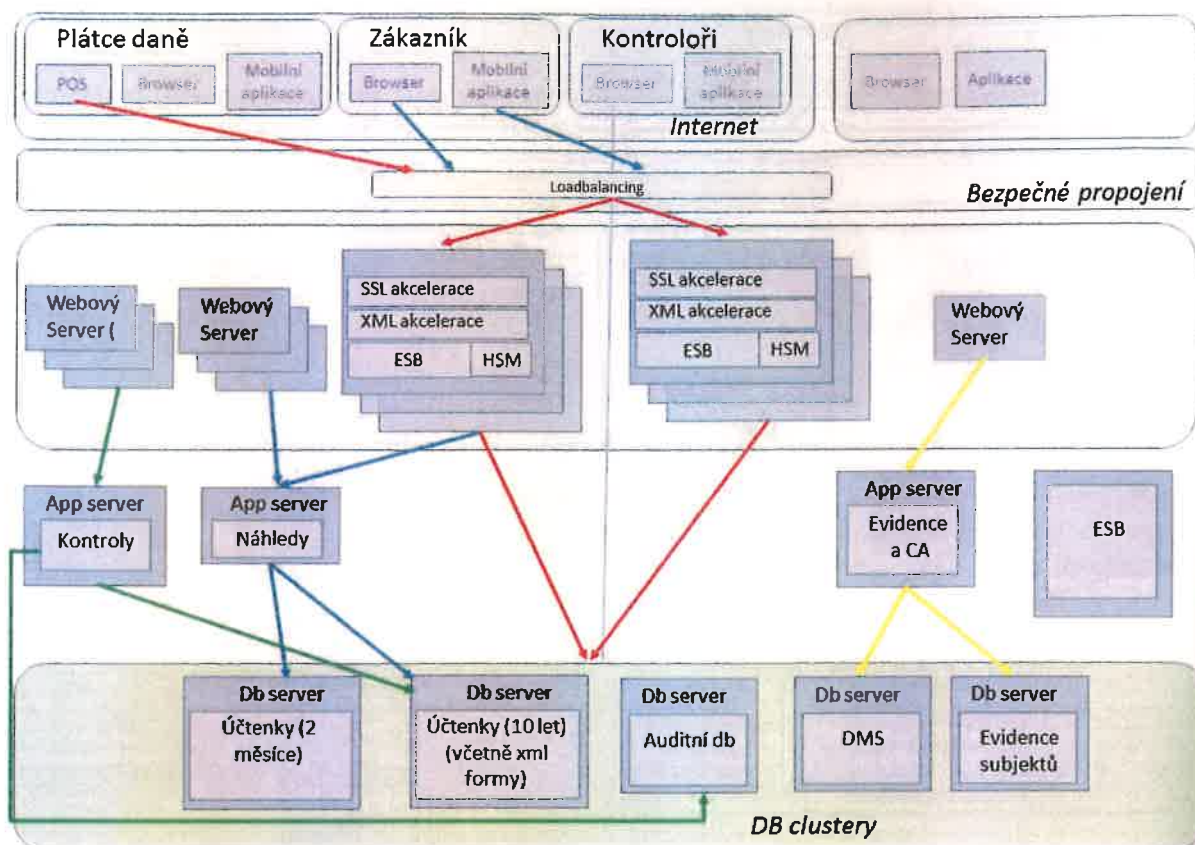
Variant 2 řeší realizaci na procesorové platformě RISC a produktech IBM. Varianta konsoliduje potřebný výpočetní výkon do jednotného virtualizačního prostředí a umožňuje dynamicky alokovaný výkon do příslušných částí systému dle aktuálních požadavků. Databázové prostředí je řešeno na platformě databázových serverů Informix nebo DB2.

Hlavní částí řešení pro B2B rozhraní jsou XML akcelerátory s integrovanými moduly HSM pro zajištění požadované propustnosti pro evidenci účtenek a vystavování bezpečnostního kódu FIK.

Variant 3 - Virtualizovaná Platforma (CPS)

1. **Konvergováný systém** – úplné HW&SW řešení dodávané na klíč, škálovatelné dle požadavků projektu EET
2. V současné době se jedná o řešení Microsoft a DELL, připravuje se v2: MS a HP
3. Řešení vychází ze zkušeností při návrhu, realizaci a provozu datových center
4. Podpora je zajištěna prostřednictvím služeb Premier Support, případné požadavky na integraci CPS do prostředí zákazníka zajišťují Microsoft Services
5. Řešení je postaveno na normalizovaném HW Dell s garantovanou kompatibilitou všech HW a SW komponent řešení
6. Řízené aktualizace: SW opravy a aktualizace všech komponent jsou nejprve testovány na totožné HW konfiguraci v laboratořích MS a následně jsou uvolněny pro nasazení na prostředky
7. Doporučený životní cyklus je v závislosti na způsobu nasazení odhadován na 3 - 5let
8. Řešení využívá technologii Microsoft.
9. CPS nabízí služby: IaaS, PaaS a DBaaS

CPS Stamp:



Škálovatelnost (stručně)

Řešení je flexibilní dle výkonových požadavků zákazníka. CPS je dodáváno v jednotkách, tzv. Stamp. Stamp znamená rovněž jednu management doménu provozované CPS instance.

Škálovatelnost Stamp:

- V rámci Stamp je možné zajistit efektivní škálování a rozšiřitelnost o sdílený výpočetní výkon, diskové úložiště.

Zálohování

Pro potřeby provozních záloh je požadováno zajištění zálohování na média s minimalizací dopadů na zdrojové systémy, které by mohli mít dopad na celkové zpomalení odezvy primárního systému. Systém a zvolený způsob zálohování musí splňovat požadavky na recovery time plynoucí z parametru RTO a RPO definovaným pro jednotlivé části informačního systému. Zařízení musí splňovat parametry pro možnost obnovitelnosti dat po celou dobu životního cyklu použitých zálohovacích médií.

Pro všechny HW a SW prostředky je požadována tříletá maintenance (HWMA 3y 24x7 Response time 4h).

Předběžný rozpočet systému EET a infrastruktury

V rámci **Varianty 1** jsou použity produkty Oracle a to jak HW tak SW. Prostředí je řešené na platformě x86 a řešení ExaData. Replika (online) dat je provedena na samostatný storage v druhém datovém sále.

Varianta 1	počet	SW/HW	cena	funkce	poznámka
Oracle Database Enterprise Edition	1	SW	218 850 615,96 Kč		
Partitioning	1	SW	23 573 523,85 Kč	DB	
Real Application Clusters	1	SW	5 707 274,19 Kč	DB	
Multitenant	1	SW	11 414 548,39 Kč	DB	
Tuning Pack	1	SW	8 684 982,47 Kč	DB	
Diagnostics Pack	1	SW	2 481 423,56 Kč	DB	
Exadata Storage Server Software	1	SW	3 722 135,34 Kč	DB	
WebLogic + service bus	1	SW	4 962 847,13 Kč	DB	
storage pro replikaci	1	SW	21 216 399,20 Kč	sběrnice služeb	
Exadata 5-2 Quarter rack	1	HW	2 000 000,00 Kč		
X5-2 server	1	HW	7 649 056,80 Kč	DB	
DataPower Gateway Appliance	4	HW	115 894,80 Kč	správa	
x3550 16 way 64 GB	4	HW	16 495 498,67 Kč	XML akcelerace, ESB, FIK,	
x3550 16 way 64 GB	4	HW	1 096 024,20 Kč	Aplikační servery	
CA s HSM	4	HW	1 096 024,20 Kč	Middleware servery	
Switch 48 port	3	HW	2 426 891,78 Kč	Certifikační autorita	
Diskove pole	2	HW	1 146 398,16 Kč	SAN infrastruktura	
TS3500	2	HW	2 312 177,42 Kč	Diskove pole	
TSM	1	HW	4 730 187,80 Kč	Pásková jednotka	
Implementace	1	SW	1 759 664,00 Kč	Zálohování	
DDOS	1		20 000 000,00 Kč	cena implementace	
UTM	2	Network	4 000 000,00 Kč	síťové prvky	
Switch	2	Network	6 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	2 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	3 000 000,00 Kč	síťové prvky	
WAF	2	Network	4 000 000,00 Kč	síťové prvky	
SIEM	4	Network	2 000 000,00 Kč	síťové prvky	
Implementace	1	Network	2 000 000,00 Kč	síťové prvky	
EET	200 MD		2 500 000,00 Kč	implementace síť prvků	
Tomcat			32 000 000,00 Kč	vývoj a implementace SW	
TSM		SW	- Kč	Aplikační servery	
bezpečnost		SW	1 759 664,00 Kč	Zálohování	
			15 000 000,00 Kč		

Varianta 2 vychází z předpokladu existence smlouvy ISLO s IBM..

Varianta 2	počet	SW/HW	cena	funkce	poznámka
			212 839 106,85 Kč		
S822 20c 256GB RAM	3	HW	3 277 085,36 Kč	Aplikační servery	
S824 24c 1TB RAM	2	HW	6 848 058,72 Kč	DB servery	
CA s HSM	2	HW	2 426 891,78 Kč	Certifikační autorita	
Storvize v7000	2	HW	9 248 709,68 Kč	Diskové pole	
TS3500	1	HW	4 730 187,80 Kč	Pásková knihovna	
Switch 48 port	2	HW	1 146 398,16 Kč	SAN infrastruktura	
DataPower Gateway Appliance	4	HW	22 828 832,00 Kč	XML akcelerace, ESB, FIK,	ISLO
TSM		SW	1 759 664,00 Kč	Zálohování	ISLO
Informix nebo DB2		SW	35 152 038,40 Kč	Databázový systém	ISLO
Tomcat		SW	- Kč	Aplikační servery	ISLO
WebSphere MQ		SW	6 321 120,00 Kč	Message Queue	ISLO
Integration Bus		SW	24 600 120,95 Kč	ESB	ISLO
Implementace	1		20 000 000,00 Kč	cena implementace	
DDOS	2	Network	4 000 000,00 Kč	síťové prvky	
UTM	2	Network	6 000 000,00 Kč	síťové prvky	
Switch	2	Network	2 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	3 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	4 000 000,00 Kč	síťové prvky	
WAF	4	Network	2 000 000,00 Kč	síťové prvky	
SIEM	1	Network	2 000 000,00 Kč	síťové prvky	
Implementace	200 MD		2 500 000,00 Kč	implementace sítí prvků	
Bezpečnostní projekt			15 000 000,00 Kč	Komplexní bezpečnostní dokumentace, bezpečnostní testy	
EET		SW	32 000 000,00 Kč	vývoj a implementace SW	

Varianta 3 je založena na virtualizované platformě CPS. Platforma je dodávána jako kompletní připravené řešení společností Microsoft včetně HW a SW prostředků. Virtualizované prostředí je schopné realizovat prostředí pro OS Microsoft a Linux.

Varianta 3	počet	SW/HW	cena	funkce	poznámka
			202 245 575,58 Kč		
CPS - APP,DB	2	HW	57 800 000,00 Kč	Aplikační a databázové servery	
TS3500	1	HW	4 730 187,80 Kč	Pásková knihovna - zálohování	
DataPower Gateway Appliance	4	HW	22 828 832,00 Kč	XML akcelerace, ESB, FIK,	
TSM		SW	1 759 664,00 Kč	Zálohování	
SQL server		SW	23 500 000,00 Kč	Databázový systém	
Integration Bus		SW	4 700 000,00 Kč	ESB	
CA s HSM	3	HW	2 426 891,78 Kč	Certifikační autorita	

Implementace	1		10 000 000,00 Kč	cena implementace	
DDOS	2	Network	4 000 000,00 Kč	síťové prvky	
UTM	2	Network	6 000 000,00 Kč	síťové prvky	
Switch	2	Network	2 000 000,00 Kč	síťové prvky	
Switch OOB	2	Network	2 000 000,00 Kč	síťové prvky	
IPS/IDS	2	Network	3 000 000,00 Kč	síťové prvky	
Loadbalancing	2	Network	4 000 000,00 Kč	síťové prvky	
WAF	4	Network	2 000 000,00 Kč	síťové prvky	
SIEM	1	Network	2 000 000,00 Kč	síťové prvky	
Implementace	200 MD		2 500 000,00 Kč	implementace síť prvků	
Bezpečnostní projekt			15 000 000,00 Kč	Komplexní bezpečnostní dokumentace, bezpečnostní testy	
EET		SW	32 000 000,00 Kč	vývoj a implementace SW	

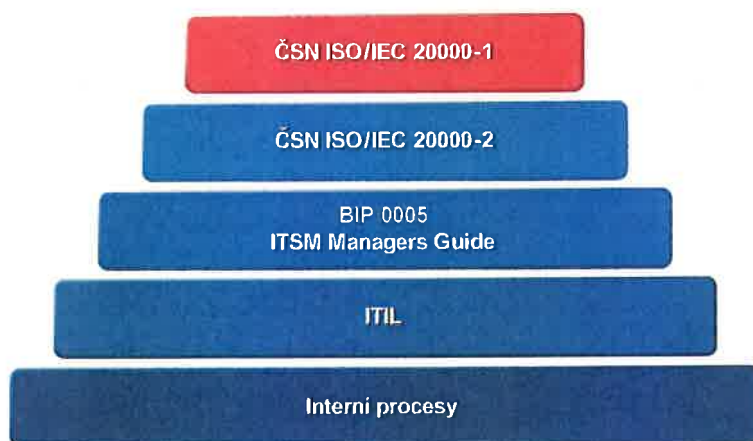
Řešení procesu správy a provozu služeb

Řešení procesů provozu a správy služeb systém EET bude řešeno v souladu s normou ISO/IEC 20000. Důraz bude kladen na procesy životního cyklu jednotlivých služeb poskytovaných koncovým uživatelům a na procesy dohledu, monitorování, podpory uživatelů a řešení incidentů.

Bude provedeno stanovení rozsahu a cílů řešení, provedena analýza rizik služeb (bude zajištěna úzká koordinace a propojení s analýzou rizik v rámci řešení bezpečnosti), příprava politiky IT služeb, katalogu služeb, plánu managementu služeb, provozních politik, návrhu SLA, provozních plánů, plánu a politiky zlepšování služeb a plánu školení a vzdělávání.

Procesy správy a provozu služeb

Zajištění shody s požadavky průmyslové normy ISO/IEC 2000 (respektive doporučení normy ISO/IEC 2000-2) je nezávislé na organizační struktuře. Poskytovatel služby musí použít strukturu, která je nejvhodnější pro efektivní službu. V návaznosti na to, nabízené řešení procesu správy a provozu služeb vhodně kombinuje ISO/IEC 20000 obsahujícím povinnosti a ITIL (aktuálně ve verzi 3), který zahrnuje nejlepší doporučení (best practices) správy služeb IT, která mohou být přizpůsobena potřebám organizací rozdílných velikostí a která jsou zaměřena na služby a na neustálé měření a zlepšování kvality dodávaných služeb IT a to jak z pohledu poskytovatele tak zákazníka.



Obrázek 28: Pojetí řešení procesu správy a provozu služeb

Řešení procesu správy a provozu služeb ve výše uvedeném pojetí bude tedy zaměřeno na následující (dále stručně vymezené) procesy:

Strategie služeb (Service Strategy)	<ul style="list-style-type: none"> • Správa financí (Financial Management) • Správa portfolia služeb (Service Portfolio Management) • Správa požadavků (Demand Management)
Návrh služeb (Service Design)	<ul style="list-style-type: none"> • Správa katalogu služeb (Service Catalogue Management) • Správa úrovně služeb (Service Level Management) • Správa kapacit (Capacity Management) • Správa dostupnosti (Availability Management) • Správa kontinuity služeb IT (IT Service Continuity Management) • Správa bezpečnosti informací (Information Security Management) • Správa dodavatelů (Supplier Management)

Přechod služeb (Service Transition)	<ul style="list-style-type: none"> • Správa změn (Change Management) • Správa aktiv a konfigurace (Service Asset and Configuration Management) • Správa znalostí (Knowledge Management) • Plánování a podpora přechodu (Transition Planning and Support) • Správa releasů a nasazení (Release and Deployment Management) • Ověření a testování služby (Service Validation and Testing) • Vyhodnocení (Evaluation)
Provoz služeb (Service Operation)	<ul style="list-style-type: none"> • Správa událostí (Event Management) • Správa incidentů (Incident Management) • Provádění požadavků (Request Fulfilment) • Správa přístupů (Access Management) • Správa problémů (Problem Management)
Neustálé zlepšování služby (Continual Service Improvement)	<ul style="list-style-type: none"> • Zlepšovací proces v 7 krocích • Měření služby (Service Measurement) • Vykazování služby (Service Reporting)

Řešení bezpečnosti systému EET

Řešení bezpečnosti Systému EET musí vycházet z předpokladu, že vzhledem k významu Systému EET bude tento zařazen mezi významné informační systémy dle písmena d) §2 dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále je předpoklad, že některá dokumentace Systému EET, obsahující popisy mechanismů zajišťujících bezpečnost celého systému může být klasifikovaná jako utajovaná informace až do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Pro Systém EET je tedy požadováno zavedení systému řízení bezpečnosti informací.

Řešení bezpečnosti Systému EET bude zahrnovat posouzení vstupních podmínek a bezpečnostních požadavků a řešení bezpečnostních požadavků v souladu s normou ISO/IEC 27001 a požadavky zákona. Při řešení bezpečnosti Systému EET musí Poskytovatel sledovat tři základní cíle:

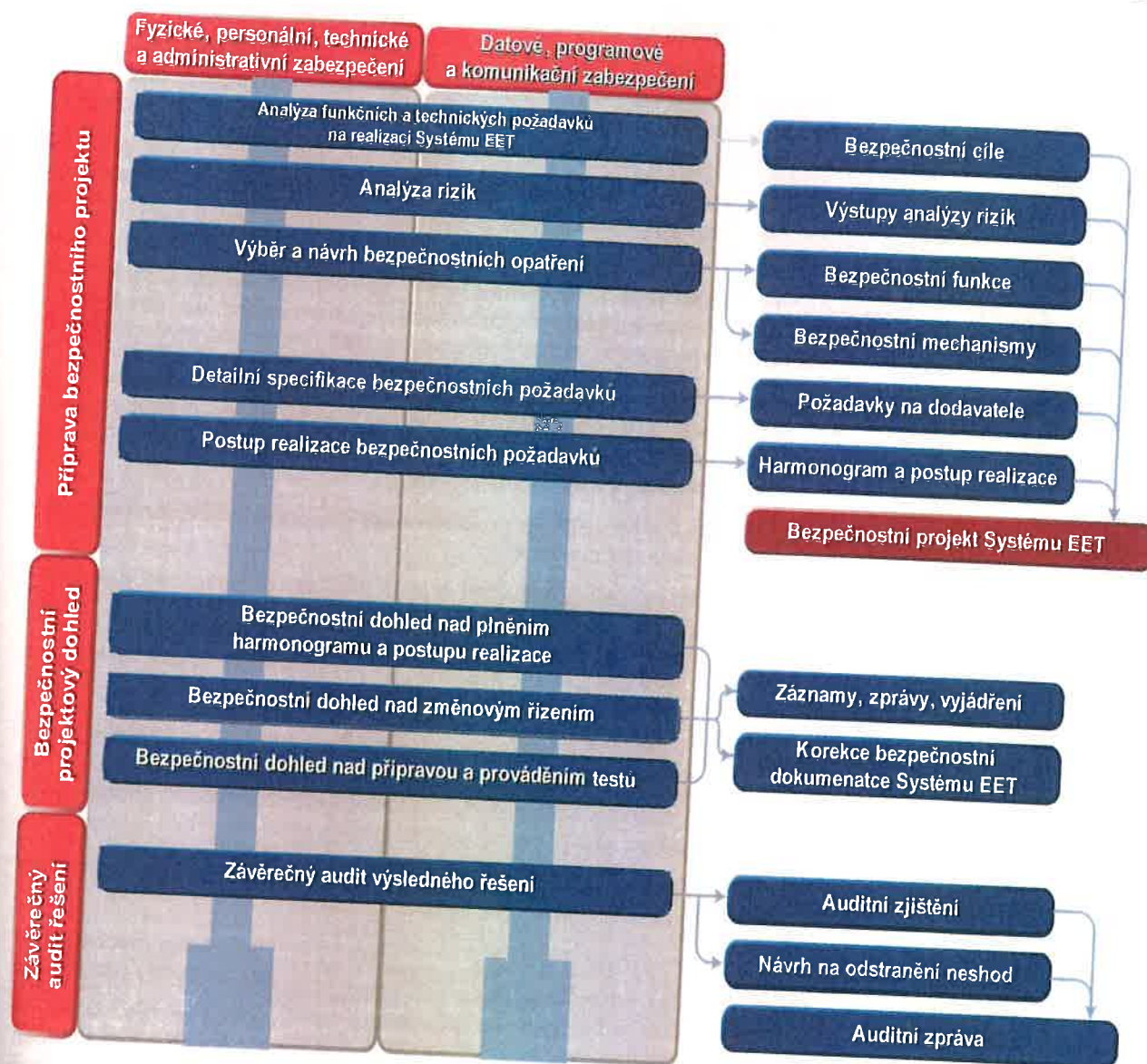
1. Zajistit zapracování bezpečnostních požadavků na Systém EET od návrhu až po implementaci celého systému bezpečnosti.
2. Vytvořit funkční systém řízení bezpečnosti informací Systému EET tak, aby bylo možné tento systém bezpečně provozovat.
3. Navrhnout a zavést systém řízení bezpečnosti a návrh bezpečnostních funkcí tak, aby byl v souladu s požadavky:
 - o normy ČSN ISO/IEC 27001:2014,
 - o zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a navazujících vyhlášek NBÚ (dále také „zákon č. 181/2014 Sb., a vyhlášky NBÚ“),
 - o zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (pro některé části dokumentace),
 - o požadavky kladenými na systémy veřejné správy a požadavky dalších relevantních právních norem.

Na základě výše uvedených cílů a požadavků zadávací dokumentace je požadováno, aby Poskytovatel řešení bezpečnosti Systému EET realizoval zavedení bezpečnosti Systému EET ve 3 po sobě jdoucích etapách následovně:

- **Etapa 1** – Analýza a návrh bezpečnosti Systému EET
- **Etapa 2** – Implementace bezpečnosti Systému EET
- **Etapa 3** – Monitorování a přezkoumání bezpečnosti Systému EET

Systém řízení bezpečnosti Systému EET musí být Poskytovatelem navržen a implementován tak, aby ho bylo možné, v případě potřeby, certifikovat podle normy ČSN ISO/IEC 27001:2014.

Bezpečnostní funkce budou navrženy ve formě Typizovaných bezpečnostních profilů s využitím ISO 15408.



Obrázek 29: Schéma bezpečnostních činností a související dokumentace

Při realizaci řešení bezpečnosti Systému EET bude se vycházet a řídit ustanoveními standardu ČSN ISO/IEC 27001:2014 s tím, že bude dále akcentovat další relevantní zákony, normy a standardy, zejména potom:

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 101/2000 Sb., o ochraně osobních údajů v platném znění
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- zákon č. 227/2000 Sb., o elektronickém podpisu v platném znění
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy v platném znění
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

Dále je požadováno realizovat řešení bezpečnosti EET v následujících krocích:

- **Příprava bezpečnostního projektu Systému EET** zahrnujícího analýzu bezpečnostních aspektů projektu včetně stanovení bezpečnostních cílů a analýzy rizik, návrh efektivních bezpečnostních opatření s následnou specifikací bezpečnostních funkcí a návrh jejich realizace ve formě bezpečnostních mechanismů na úrovni jednotlivých komponent Systému EET.
- **Bezpečnostní projektový dohled Systému EET** zahrnující dohled nad realizací a prosazováním bezpečnostních funkcí a bezpečnostních mechanismů v souladu s obsahem bezpečnostního projektu Systému EET.
- **Závěrečný bezpečnostní audit řešení Systému EET** za účelem ověření funkčnosti bezpečnostních funkcí a bezpečnostních mechanismů včetně jejich prosazení do relevantních interních procesů Systému EET.
- **Řízení a údržba bezpečnosti při provozu Systému EET**, která bude zahrnovat zejména udržení souladu stavu bezpečnost s bezpečnostními požadavky prostředí a udržení souladu stavu bezpečnosti s bezpečnostními potřebami Systému EET v souvislosti s jeho změnami prováděnými v rámci jeho implementace a provozu.

Jednotlivé složky, jejich návaznosti a postup realizace řešení bezpečnosti Systému EET jsou znázorněny na schématu uvedeném na následující straně.

Řešení bezpečnosti Systému EET musí být zajištěno v koordinaci s návrhem a implementací celého systému tak, aby bylo zajištěno okamžité zapracování bezpečnostních požadavků do implementovaného systému.

Vzhledem k tomu, že některá dokumentace systému EET, zejména část obsahující popisy mechanismů zajišťujících bezpečnost celého systému, může být klasifikována jako utajovaná informace až do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, jsou na Poskytovatele kladeny tyto požadavky:

- Poskytovatel musí být držitelem Osvědčení podnikatele pro přístup k utajované informaci, která u něho vzniká nebo je mu poskytnuta, nejméně pro stupeň „Důvěrné“.
- Zaměstnanci Poskytovatele, zpracovávající části dokumentace, obsahující popisy mechanismů zajišťujících bezpečnost celého systému, musí být držiteli Osvědčení fyzické osoby pro přístup k utajované informaci nejméně pro stupeň „Důvěrné“.
- Poskytovatel musí disponovat prostředky fyzické a administrativní bezpečnosti a bezpečnosti informačních systémů pro zpracování dokumentace v režimu utajované informace do stupně „Důvěrné“ dle zákona č. 412/2005 Sb., a prováděcích vyhlášek.

Dále následuje rozklad činností a obsah výstupů realizovaných v jednotlivých etapách řešení bezpečnosti.

Etapa 1 – Analýza a návrh bezpečnosti systému EET

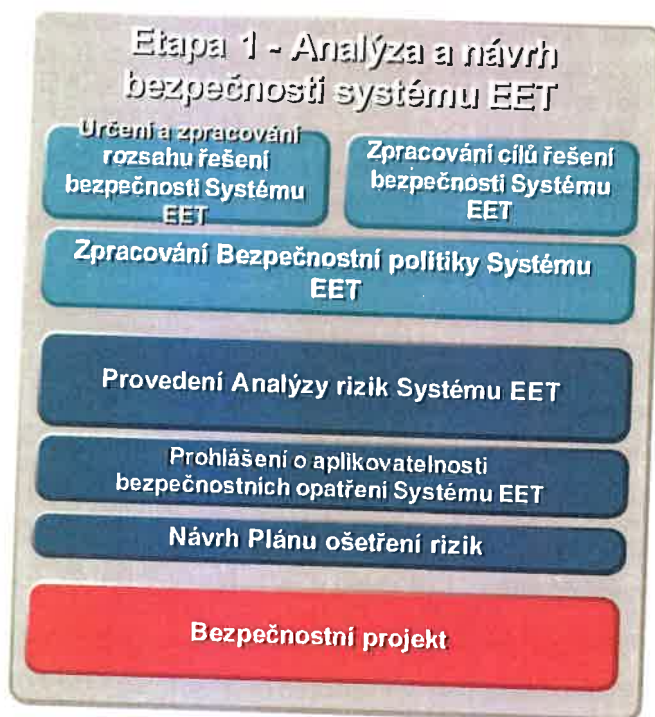
Analýza a návrh bezpečnosti systému EET bude mít za cíl identifikovat požadavky na bezpečnost systému EET a navrhnout bezpečnostní řešení Systému EET počínaje návrhem celého systému a konče jeho předáním do provozu.

V rámci této etapy bude provedeno stanovení rozsahu a cílů řešení bezpečnosti, analýza rizik, zpracování bezpečnostní politiky Systému EET včetně bezpečnostní strategie, připravení Prohlášení o aplikovatelnosti a Plánu ošetření rizik Systému EET. V závěru etapy bude zpracován bezpečnostní projekt Systému EET.

Etapa 1 musí obsahovat následující fáze:

1. Určení základních parametrů řešení bezpečnosti Systému EET
2. Hodnocení a řízení rizik Systému EET
3. Zpracování Bezpečnostního projektu Systému EET

Grafické znázornění činností požadovaných realizovat v této etapě je uveden na následujícím obrázku.



Obrázek 30: Schéma etapy 1 řešení bezpečnosti Systému EET

Fáze 1.1 – Určení základních parametrů řešení bezpečnosti systému EET

V první fázi řešení bezpečnosti Systému EET bude provedeno upřesnění rozsahu řešení bezpečnosti Systému EET, návrh cílů řešení bezpečnosti a následně zpracuje Bezpečnostní politiku informací systému EET.

V této fázi se provedou úkony důležité pro realizaci řešení bezpečnosti Systému EET:

- Analýzu funkčních a legislativních bezpečnostních požadavků na Systém EET a prostředí, v němž bude provozován.
- Definování rozsahu řešení bezpečnosti systému EET, který bude obsahovat interní a externí aspekt dle ČSN ISO/IEC 27001:2014.

Popis požadovaných základních výstupů:

1. **Rozsah řešení bezpečnosti Systému EET – upřesní** rozsah řešení bezpečnosti Systému EET z hlediska zapojených organizačních složek, vybraných prostor, definovaných aktiv a technologií. Rozsah bude mít následující strukturu:
 - a. organizační struktura ve vztahu k řešení bezpečnosti Systému EET
 - b. umístění organizačních útvarů a zařízení pokrývaných v rámci k řešení bezpečnosti Systému EET
 - c. základní aktiva a technologie pokrývaní v rámci k řešení bezpečnosti Systému EET
 - d. rozhraní řešení bezpečnosti Systému EET
 - e. závislosti k řešení bezpečnosti Systému EET.
2. **Cíle řešení bezpečnosti Systému EET** – budou obsahovat stručný výčet cílů, kterých má být dosaženo řešením bezpečnosti v určeném rozsahu řešení bezpečnosti Systému EET. Cíle budou konkrétně stanoveny na období implementace s výhledem na zajištění provozu systému EET.
3. **Bezpečnostní politiku informací systému EET** je požadováno zpracovat ve formě koncepčního dokumentu shrnujícího strategii a zásady bezpečnosti systému EET ve všech oblastech bezpečnosti informací s důrazem na uvedení odpovědností za oblast bezpečnosti a popis zaváděných bezpečnostních zásad v rámci jednotlivých oblastí bezpečnosti. Pro Bezpečnostní politiku systému EET je požadována následující struktura:
 - a. Strategie bezpečnosti Systému EET
 - b. popis systému EET
 - c. funkční bloky systému EET
 - d. bezpečnost prostředí systému EET
 - e. regulatorní, právní a smluvní požadavky na řešení bezpečnosti Systému EET
 - f. kritéria hodnocení rizik
 - g. zásady bezpečnosti informací v Systému EET:
 - organizace bezpečnosti informací
 - bezpečnost lidských zdrojů
 - řízení aktiv
 - řízení přístupu
 - kryptografie
 - fyzická bezpečnost a bezpečnost prostředí
 - bezpečnost provozu
 - bezpečnost komunikací
 - dodavatelské vztahy
 - řízení incidentů bezpečnosti informací
 - kontinuita bezpečnosti informací
 - soulad s požadavky
 - h. způsob řízení bezpečnostní dokumentace Systému EET
 - i. způsob vyčleňování a řízení zdrojů pro zajištění bezpečnosti Systému EET
 - j. způsob monitorování a měření efektivity řešení bezpečnosti Systému EET.

Fáze 1.2 – Hodnocení a řízení rizik systému EET

Cílem hodnocení a řízení rizik bude identifikovat aktiva Systému EET, a zjistit úroveň rizik možného uplatnění hrozeb, které na aktiva mohou působit.

V počátku fáze bude navržena metodika hodnocení a řízení rizik Systému EET. V návaznosti na vybranou metodiku identifikuje aktiva, která budou zahrnuta do rozsahu řešení bezpečnosti Systému EET, spolu s určením jejich bezpečnostních parametrů (důvěrnost, integrita, dostupnost). Dále budou identifikovány a hodnoceny hrozby a zranitelnosti působící na aktiva Systému EET a následně navržena opatření k pokrytí rizik. Zdůvodnění výběru opatření bude provedeno v dokumentu Prohlášení o aplikovatelnosti bezpečnostních opatření Systému EET. Způsob řízení rizik bude následně popsán v Plánu ošetření rizik Systému EET.

V závěru analýzy rizik bude zajištěno provedení zvládání a řízení rizik prostřednictvím návrhu přiměřených bezpečnostních protipatření pokrývajících zjištěná rizika. Pro naplnění bezpečnostních cílů a snížení bezpečnostních rizik bude vybrána vyvážená kombinace technických a netechnických bezpečnostních opatření pro Systému EET.

V této fázi budou provedeny úkony, vyžadované normou ČSN ISO/IEC 27001:2014:

- stanovení kritérií rizik bezpečnosti informací, která zahrnují:
 - kritéria akceptace rizik
 - kritéria pro provádění posouzení rizik bezpečnosti informací
- identifikace rizika bezpečnosti informací:
 - používá proces posuzování rizik bezpečnosti informací k identifikaci rizik spojených se ztrátou důvěrnosti, integrity a dostupnosti informací v rozsahu systému řízení bezpečnosti informací
 - identifikuje vlastníky rizik
- analýza rizika bezpečnosti informací:
 - posuzuje potenciální následky, které by nastaly, pokud by se realizovala identifikovaná rizika
 - posuzuje reálnou pravděpodobnost výskytu rizik
 - určuje úroveň rizik
- hodnocení rizika bezpečnosti informací:
 - porovnává výsledky analýzy rizik s kritérii rizik
 - stanovuje priority analyzovaných rizik pro ošetření rizika
- Definování procesu ošetření rizik bezpečnosti informací pro:
 - výběr vhodných variant pro ošetření rizika bezpečnosti informací s ohledem na výsledky posuzování rizik
 - určení všech opatření nezbytných k implementaci vybrané varianty (variant) pro ošetření rizika bezpečnosti informací
 - verifikace opatření určených výše s cílem ověřit, že žádné nezbytné opatření nabylo vynecháno
 - vytvoření Prohlášení o aplikovatelnosti, které obsahuje nezbytná opatření a zdůvodnění pro jejich zahrnutí, ať už jsou nebo nejsou implementována
 - formulace Plánu ošetření rizik bezpečnosti informací
 - získání souhlasu vlastníků rizik ohledně plánu ošetření rizik bezpečnosti informací a přijetí zbytkových rizik bezpečnosti informací.

Metodika analýzy rizik musí zároveň odpovídat zákonu č. 181/2014 Sb., a jeho prováděcím vyhláškám.

Popis požadovaných základních výstupů

1. **Zpráva o hodnocení rizik Systému EET** – souhrnný dokument, který musí obsahovat:
 - a. základní pravidla a postupy analýzy rizik a příslušná hodnotící kritéria včetně metodologie
 - b. přehled aktiv včetně určení bezpečnostních parametrů a vlastníků
 - c. výčet hrozeb a zranitelností, která na aktiva (skupiny aktiv) působí
 - d. výsledky analýzy pro jednotlivá aktiva
 - e. stanovení variant pro ošetření rizika
 - f. stanovení priorit pro ošetření rizik
 - g. přehled vlastníků rizik
 - h. detailní výsledky analýzy rizik.
2. **Prohlášení o aplikovatelnosti bezpečnostních opatření Systému EET** – uvede **souhrnný** přehled opatření dle přílohy A normy ČSN ISO/IEC 27001:2014, která jsou aplikována při řešení bezpečnosti Systému EET a případné důvody, pro které nebyla nevhodná opatření aplikována. Součástí prohlášení o aplikovatelnosti bude specifikace a rozhodnutí o výši zbytkových rizik.
3. **Návrh Plánu ošetření rizik Systému EET** – bude obsahovat **stanovení** cílů bezpečnosti Systému EET, relevantních jednotlivým funkcím a úrovním řízení. Při plánování jak dosáhnout cílů bezpečnosti informací musí Poskytovatel určit:
 - a. co bude vykonáno
 - b. jaké zdroje budou vyžadovány
 - c. kdo bude odpovědný
 - d. kdy to bude dokončeno
 - e. jak budou výsledky vyhodnoceny.

Fáze 1.3 – Zpracování Bezpečnostního projektu Systému EET

Cílem přípravy bezpečnostního projektu Systému EET bude zpracovat souhrnný podkladový dokument **Bezpečnostní projekt systému EET** přehled posuzovaných bezpečnostních funkcí, přehled a odůvodnění bezpečnostních funkcí vybraných k realizaci a postup a způsob jejich realizace.

Úkolem bezpečnostního projektu Systému EET bude **navrhnout bezpečnostní profily** (sady bezpečnostních funkcí), které budou snadno a jednoznačně implementovatelné.

Bezpečnostní profil systému je specifikací konkrétních bezpečnostních funkcí, které jsou definovány na základě určení systému, analýzy prostředí, v kterém bude provozován, a požadovaných bezpečnostních cílů. Bezpečnostní funkce jsou směřovány do všech oblastí bezpečnosti, včetně bezpečnosti provozního prostředí. Hlavním cílem bezpečnostních profilů tedy je výběr bezpečnostních funkcí pro funkční celky systému EET a jejich komponenty podle normy ČSN ISO/IEC 15408 a určení navazujících profilů ochrany.

Norma ČSN ISO/IEC 15408 stanovuje následující strukturu bezpečnostního profilu, jeho obsahu a významu jednotlivých dílčích částí:

- **úvod** – vymezuje základní charakteristiky bezpečnostního profilu,
- **charakteristika systému** – obecný popis systému, pro který je bezpečnostní profil určen,

- **bezpečnost prostředí** – rozbor bezpečnosti prostředí, ve kterém je systém provozován, zde jsou upřesněny základní aktiva, předpoklady pro bezpečné fungování systému, bezpečnostní zásady a hrozby, kterým systém musí čelit,
- **bezpečnostní cíle** – upřesnění bezpečnostních cílů, které musí být při řešení bezpečnosti dosaženy, ty jsou rozděleny na bezpečnostní cíle pro informační technologie a na bezpečnostní cíle pro prostředí, ve kterém jsou systémy provozovány,
- **požadavky na bezpečnost** – naplnění cílů návrhem bezpečnostních požadavků, tyto požadavky jsou rozděleny na požadavky na bezpečnostní funkce, které jsou prosazovány informačními technologiemi, na požadavky na záruky, kde je upřesněna míra záruk za správnost, a na požadavky na bezpečnost prostředí, které upřesňuje opatření v přímém okolí informačních technologií.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

- výběr relevantních bezpečnostních profilů pro funkční celky systému EET a jejich komponenty;
- konkretizace bezpečnostních funkcí;
- návrh realizace bezpečnostních funkcí v rámci systému EET.

Popis požadovaných základních výstupů

1. **Bezpečnostní projekt** – bude **zpracován** dle formální struktury profilu ochrany dle normy ČSN ISO/IEC 15408. Budou rozpracovány výchozí bezpečnostní cíle stanovené v souladu s Bezpečnostní politikou informací systému EET do bezpečnostních funkcí. Bezpečnostní projekt bude zahrnovat:
 - a. Popis systému EET na úrovni vymezení účelu, hranic a struktury;
 - b. Specifikaci bezpečnostního prostředí Systému EET na úrovni základních aktiv, služeb, bezpečnostních předpoklad, hrozeb a zásad bezpečnostní politiky;
 - c. Vymezení bezpečnostních cílů Systému EET na úrovni cílů bezpečnosti pro informační technologie a cílů bezpečnosti pro prostředí;
 - d. Stanovení požadavků na bezpečnost Systému EET na úrovni požadavků na bezpečnost jednotlivých klíčových komponent, požadavků na bezpečnost prostředí, interpretace bezpečnostních požadavků a záruk;
 - e. Mapování vzájemných vztahů mezi cíli, předpoklady a hrozbami.

Etapa 2 – Implementace bezpečnosti Systému EET

Cílem této fáze bude rozpracovat vybraná bezpečnostní opatření a bezpečnostní funkce do bezpečnostních pravidel a postupů Systému EET.

V návaznosti na výsledky analýz a bezpečnostního projektu musí poskytovatel zpracovat bezpečnostní směrnice Systému EET, bezpečnostní příručky a navazující postupy (případně návazností na jiné existující či zpracované postupy) včetně příručky/bezpečnostní směrnice pro činnost bezpečnostního správce.

Etapa 2 obsahuje následující fáze:

- 2.1 Implementace bezpečnostních opatření Systému EET
- 2.2 Bezpečnostní školení a vzdělávání v Systému EET.
- 2.3 Zpracování bezpečnostních příruček a zajištění kontinuity Systému EET

Grafické znázornění činností požadovaných realizovat Poskytovatelem v této etapě je uveden na následujícím obrázku.



Obrázek 31: Schéma etapy 2 řešení bezpečnosti Systému EET

Fáze 2.1 – Implementace bezpečnostních opatření Systému EET

V této fázi budou rozpracovány cíle a opatření bezpečnosti informací do postupů ve formě směrnic (dle ČSN ISO/IEC 27001:2014 – Příloha A - bezpečnostních profilů dle ISO/IEC 15408).

Nedílnou součástí bezpečnostních činností bude návrh a popis nástrojů relevantních pro Systém EET dle odst. 3) § 5 zákona č. 181/2014 Sb.

Ve směrnicích Poskytovatel stanoví ve spolupráci se Zadavatelem Systému EET role, navrhne úpravu pracovních náplní a odpovědnosti v procesu řízení bezpečnosti Systému EET. Bezpečnostní směrnice Systému EET budou zařazeny do systému řízení dokumentace provozovatele.

Způsob, formální uspořádání směrnic a jejich počet navrhne Poskytovatel na základě zpracovaného bezpečnostního projektu Systému EET. Směrnice však vždy budou obsahovat zapracování všech oblastí a náležitosti normy ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

- zavedení a zdokumentování vybraných bezpečnostních opatření (ČSN ISO/IEC 27001: 2014;)
- určení a zdokumentování způsobu měření účinnosti vybraných bezpečnostních opatření.

Popis požadovaných základních výstupů

1. **Směrnice řízení bezpečnosti Systému EET** bude zpracována v rozsahu:
 - a. Management bezpečnosti informací definující pravidla a postupy pro management bezpečnosti informací a bezpečnosti informací v projektovém řízení včetně určení odpovědností za průběh celého cyklu ISMS a uvedení způsobu měření účinnosti ISMS.
 - b. Bezpečnost lidských zdrojů definující bezpečnostní pravidla a postupy pro oblast personální bezpečnosti.
 - c. Klasifikace informací určující způsob klasifikace informací včetně klasifikačního schématu a způsob manipulace s citlivými informacemi.
 - d. Fyzická bezpečnost a bezpečnost prostředí definující bezpečnostní pravidla a postupy, jejichž cílem je předcházet neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do informací a do prostor, ve kterých se nacházejí zařízení pro zpracování informací.
 - e. Shoda s bezpečnostními požadavky rozpracovávající konkrétní postupy v oblasti zajištění souladu přijímaných opatření s legislativou a bezpečnostními či technologickými postupy dle přijatých norem a standardů.
2. **Směrnice bezpečnosti informačních a komunikačních technologií Systému EET** bude zpracována v rozsahu:
 - a. Bezpečnost provozu a bezpečnost komunikací stanovující opatření zaměřená na řádný a bezpečný provoz prostředků pro zpracování informací a služeb a procesů s tím souvisejících.
 - b. Řízení přístupu stanovující opatření zaměřená na ochranu a kontrolu přístupu k informacím, službám a procesům.
 - c. Akvizice, vývoj a údržba informačních systémů definující pravidla a postupy pořizování, vývoje a údržby Systému EET k prosazení bezpečnosti informací do celého životního cyklu Systému EET od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
3. **Směrnice řízení incidentů bezpečnosti informací a zajištění kontinuity činností Systému EET** bude zpracována v rozsahu:
 - a. Řízení incidentů bezpečnosti informací stanovující postupy hlášení bezpečnostních incidentů, reakce na ně a jejich vyhodnocování.
 - b. Řízení kontinuity činností a základní rámec řízení kontinuity podnikatelských činností, zahrnující stanovení rolí, procesů, struktury dokumentace a odpovědností.

Fáze 2.2 – Bezpečnostní školení a vzdělávání v Systému EET

V této fázi bude provedeno seznámení pracovníků provozovatele Systému EET se zaváděnými bezpečnostními opatřeními. Bude vytvořen program budování bezpečnostního povědomí, jehož úkolem bude zabezpečit znalost a pochopení postupů a činností v oblasti bezpečnosti Systému EET zaměstnanci provozovatele.

Dále budou vyškoleni pracovníci provozovatele Systému EET, kteří jsou zahrnuti do rozsahu řešení bezpečnosti Systému EET. Tito zaměstnanci budou seznámeni s pravidly a úkoly, které jim ze zajištění bezpečnosti Systému EET vyplývají. Zvláštní pozornost musí být věnována přípravě zaměstnanců, kteří budou provádět interní audity bezpečnosti Systému EET. Pro školení pracovníků bude vytvořen e-learningový portál.

V této fázi budou provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti informací Systému EET:

- zpracování programu školení a zvyšování bezpečnostního povědomí (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ)
- zpracování podkladů pro školení zainteresovaných zaměstnanců provozovatele Systému EET – upřesnění kategorií, pro které bude školení provedeno, příprava prezentace a Desatera bezpečnosti informací (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ)

- proškolení zaměstnanců provozovatele Systému EET, po určených kategoriích (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBÚ).

Popis základních požadovaných výstupů

1. **Program školení a zvyšování bezpečnostního povědomí** – obsahuje koncepci tvorby a budování bezpečnostního povědomí subjektů účastnících se správy, provozu a užívání Systému EET. Rozsah programu bude následující:
 - a. Způsob budování bezpečnostního povědomí:
 - základní cíl budování bezpečnostního povědomí,
 - strategie budování bezpečnostního povědomí,
 - kategorie zaměstnanců,
 - plánování budování bezpečnostního povědomí,
 - odpovědnost za budování bezpečnostního povědomí,
 - odpovědnost zaměstnanců,
 - odpovědnost za organizaci a provedení školení zaměstnanců provozovatele Systému EET,
 - odpovědnost za seznámení zaměstnanců třetích stran s bezpečnostními postupy Systému EET
 - b. Obsahová náplň budování bezpečnostního povědomí
 - školení k systému řízení bezpečnosti Systému EET,
 - Vstupní školení bezpečnosti Systému EET,
 - Periodické školení bezpečnosti Systému EET,
 - Mimořádné proškolení bezpečnosti Systému EET,
 - vzdělávání v oblasti bezpečnosti Systému EET.
2. **Materiály školení bezpečnosti Systému EET** – tvoří ppt prezentace a podkladové materiály pro provedení školení k zajištění bezpečnosti Systému EET pro jednotlivé kategorie zaměstnanců provozovatele Systému EET.
3. **E-learningový portál** – Vlastní školení bude pro vhodné kategorie zaměstnanců provedeno formou e-learningu. Poskytovatel zajistí vytvoření standardního e-learningového portálu včetně vhodného obsahu.

Fáze 2.3 – Zpracování bezpečnostních příruček a zajištění kontinuity Systému EET

V této fázi budou rozpracovány bezpečnostní postupy a pravidla Systému EET do nejnižší provozní úrovně.

Rozsah činností a konkretizace výstupů bude upřesněna na počátku fáze a musí vycházet z implementovaných bezpečnostních opatření vybraných na základě provedené analýzy rizik, bezpečnostního projektu Systému EET.

V rámci fáze musí být vytvořena bezpečnostní provozní dokumentace zejména v oblastech:

- Informační bezpečnosti Systému EET;
- zajištění kontinuity činností Systému EET

Důraz musí být položen na zpracování **bezpečnostních příruček pro jednotlivé role**. Tvorba příruček pro oblast bezpečnosti se bude opírat o informace ve směrnících a o informace ze schůzek s pracovníky, kteří budou zastávat jednotlivé role. Struktura příruček musí vycházet ze struktury existujících směrnic.

V rámci této fáze musí být zapracována problematika bezpečnosti do uživatelské dokumentace Systému EET.

V této fázi musí být provedeny následující úkony, které jsou důležité pro realizaci řešení bezpečnosti Systému EET:

zavedení a zdokumentování vybraných bezpečnostních opatření (ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., včetně vyhlášek NBU).

Popis požadovaných základních výstupů

1. **Bezpečnostní příručky a navazující postupy** definující konkrétní činnosti a pravidla chování pro jednotlivé role a účastníky správy a provozu Systému EET. Základní rozsah jedné příručky (zde pro příklad bezpečnostního manažera systému EET) je následující:

- a. Bezpečnostní příručka bezpečnostního manažera Systému EET:
 - řízení bezpečnosti s důrazem na roli bezpečnostního manažera,
 - řízení a klasifikace aktiv Systému EET s důrazem na evidenci aktiv a zacházení s aktivy v závislosti na jejich klasifikaci,
 - zajištění bezpečnosti lidských zdrojů s důrazem na: povinnosti bezpečnostního manažera při přijímání, školení a bezpečném odchodu pracovníků provozu Systému EET,
 - řízení bezpečnosti komunikací a provozu Systému EET s důrazem na provozní postupy, řízení změn, zálohování a monitorování,
 - řízení přístupu k systémům Systému EET s důrazem na roli bezpečnostního manažera a dohled a kontrolu přístupových práv,
 - akvizice, vývoj a údržba informačních systémů v rámci Systému EET s důrazem na stanovení bezpečnostních požadavků a dokumentace,
 - fyzická bezpečnost a bezpečnost prostředí s důrazem na pravidla práce v zabezpečených oblastech,
 - správa incidentů a řízení kontinuity s důrazem na povinnosti bezpečnostního manažera,
 - Bezpečnostní příručka bezpečnostního správce Systému EET bude zpracována v obdobném rozsahu jako příručka bezpečnostního manažera Systému EET.

Etapu 3 – Monitorování a přezkoumání bezpečnosti Systému EET

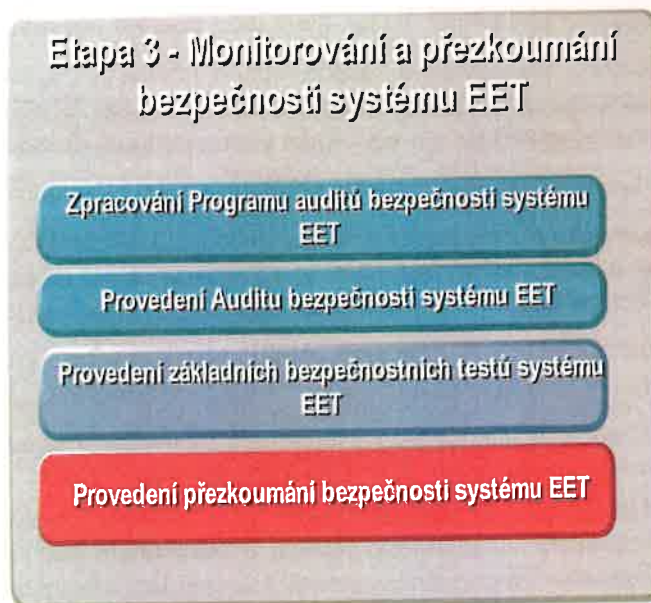
Cílem etapy bude zavést postupy pro zajištění efektivního řízení bezpečnosti Systému EET a jeho zlepšování. V rámci etapy musí Poskytovatel navrhnout a zavést metriky pro měření účinnosti bezpečnosti Systému EET, postupy interního auditu bezpečnosti a postupy pro pravidelná přezkoumání bezpečnosti Systému EET.

V rámci této etapy budou provedeny základní bezpečnostní testy Systému EET v rozsahu konfiguračních a penetračních testů k ověření výsledné implementace řešení před spuštěním Systému EET do produkčního provozu.

Etapu 3 musí obsahovat následující fáze:

- 3.1 Příprava a provedení auditu bezpečnosti Systému EET
- 3.2. Povedení přezkoumání bezpečnosti Systému EET

Grafické znázornění činností požadovaných realizovat v této etapě je uveden na následujícím obrázku.



Obrázek 32: Schéma etapy 3 řešení bezpečnosti Systému EET

Fáze 3.1 – Příprava a provedení auditu bezpečnosti Systému EET

Cílem této fáze bude zajistit provádění kontrolní a auditní činnosti k posouzení efektivního provozu bezpečnosti Systému EET. Fáze bude zahrnovat přípravu a provedení interního auditu bezpečnosti Systému EET.

V rámci fáze bude zpracován plán interních auditů bezpečnosti Systému EET, včetně popisu způsobu provádění interních auditů bezpečnosti Systému EET a metrik měření účinnosti přijatých opatření. V tomto dokument Poskytovatel uvede:

- vstupy pro zhodnocení, které budou mimo jiné zahrnovat výsledky auditů a analýz bezpečnosti Systému EET, zajištění zpětné vazby od zainteresovaných stran, stavu preventivně nápravných činností a doporučení pro zlepšení bezpečnosti Systému EET (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., a vyhlášky NBÚ);
- výstupy zhodnocení, které budou zahrnovat jakákoliv rozhodnutí a činnosti vztahující se k zlepšování efektivnosti, změny postupů a potřeby zdrojů na zajištění bezpečnosti Systému EET (dle ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., a vyhlášky NBÚ);
- interní audity bezpečnosti Systému EET, které zajistí, že cíle a opatření bezpečnosti Systému EET vyhovují požadavkům na systém, normě ČSN ISO/IEC 27001, legislativě a požadavkům na bezpečnost informací a jsou funkční a jsou zavedeny a udržovány efektivně (dle ČSN ISO/IEC 27001:2014 a zákon č. 181/2014 Sb., a vyhlášky NBÚ).

V rámci této fáze bude zpracován program pro první audit, provede vzorový interní audit s vyčleněnými pracovníky Zadavatele bezpečnosti Systému EET dle normy ČSN ISO/IEC 27001:2014 a zpracuje zprávu z tohoto auditu. Dále budou připraveni a vyškoleni interní auditoři pro oblast bezpečnosti Systému EET Strukturu auditu je požadována v následující:

- zpracování programu auditu,
- zahájení a příprava auditu – ustavení jeho základního rámce,
- příprava auditu – příprava auditních podkladů, upřesnění rámce a průběhu auditu a příprava jeho účastníků na straně provozovatele Systému EET,

- provedení auditu – shromáždění relevantních informací z auditovaných oblastí, jejich posouzení, zpracování a schválení ve formě auditních záznamů a příprava závěrů auditu z auditovaných oblastí.
- vyhodnocení auditu – bude zjištěna úroveň shody aktuálního stavu auditovaných oblastí se zvolenými kritérii auditu – požadavky na bezpečnost Systému EET a normou ČSN ISO/IEC 27001:2014. Výsledky budou uvedeny ve Zprávě z interního auditu bezpečnosti Systému EET.

Popis požadovaných základních výstupů

1. **Plán auditů bezpečnosti Systému EET** – stanoví způsob provádění pravidelných přezkoumávání a ověřování bezpečnosti Systému EET k zajištění účelnosti, dostatečnosti a efektivnosti celého řešení bezpečnosti.
2. **Materiály školení interních auditorů** – budou tvořit ppt prezentace a podkladové materiály pro provedení interního auditu bezpečnosti Systému EET spolu s přípravou modulu do e-learningového školení.
3. **Program interního auditu bezpečnosti Systému EET** – bude tvořit dokument propisující způsob provedení, kritéria a organizační zajištění konkrétního (prvního) auditu stavu bezpečnosti Systému EET.
4. **Zpráva z interního auditu bezpečnosti Systému EET** – bude tvořit dokument, jehož cílem bude poskytnout komplexní zprávu o stavu bezpečnosti Systému EET.

Fáze 3.2 – Provedení přezkoumání bezpečnosti Systému EET

Cílem fáze bude zpracovat Přezkoumání bezpečnosti Systému EET, které bude tvořit základní hodnotící dokument pro další provoz a zlepšování bezpečnosti Systému EET.

Návrh Přezkoumání bezpečnosti Systému EET bude zpracován ve spolupráci s bezpečnostním managementem resortu MFČR v následující struktuře:

- návrh na zlepšení bezpečnosti Systému EET do dalšího přezkoumání bezpečnosti Systému EET
- doporučení ke zlepšení efektivity bezpečnosti Systému EET a k aktualizaci hodnocení rizik
- návrh změny postupů zajištění bezpečnosti Systému EET
- zdroje potřebné pro zlepšování bezpečnosti Systému EET
- doporučení ke zlepšení účinnosti opatření bezpečnosti Systému EET
- návrh cílů ISMS pro další cyklus provozu bezpečnosti Systému EET.

Přezkoumání bezpečnosti Systému EET – bude tvořit dokument, jehož cílem bude zhodnotit úroveň zavedení bezpečnosti Systému EET a navrhnout další postup při provozování a zlepšování bezpečnosti Systému EET.

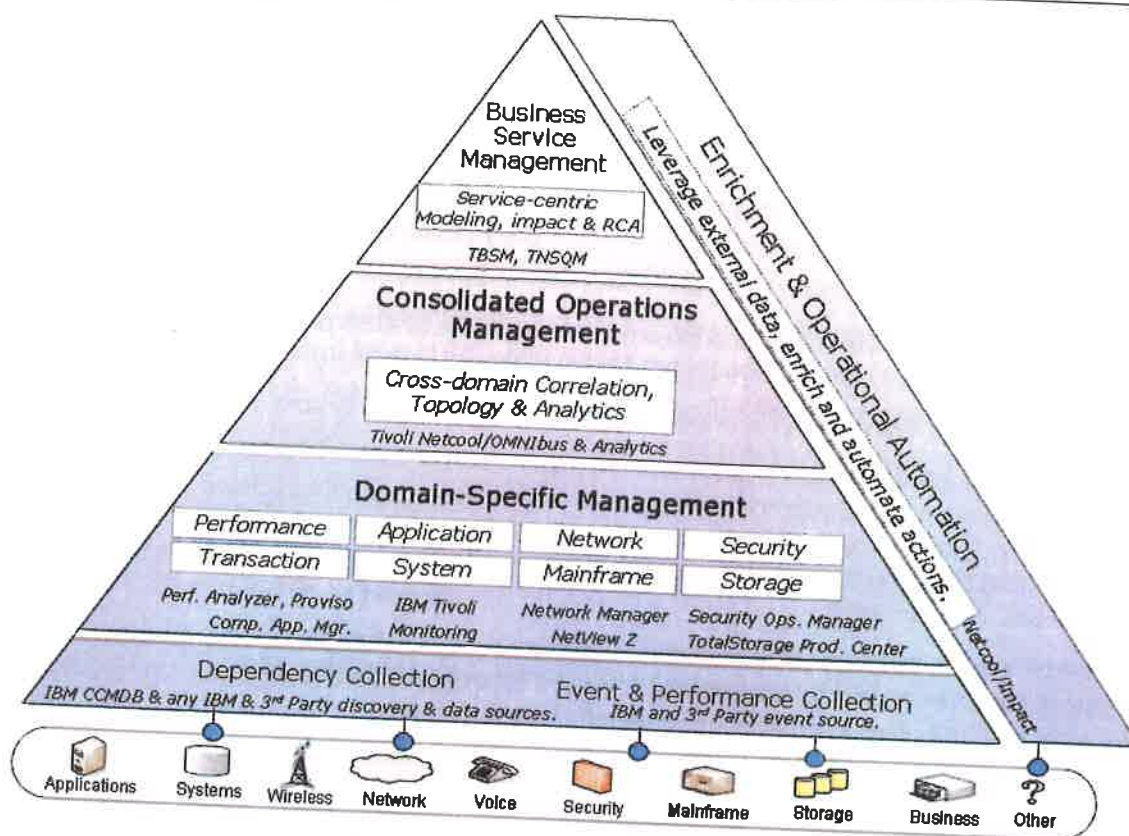
Požadavky na monitoring a prostředí datových sálů pro systém EET

Monitoring systému EET

- provádí nepřetržitý dohled provozního stavu a datové průchodnosti aktivních prvků
- průběžně monitoruje zejména kvalitu a dostupnost služeb EET, odchylky parametrů od normálního stavu, sleduje trendy a reportuje dosažení prahových hodnot
- provádí primární vyhodnocení alarmů a nestandardních provozních stavů a jejich eskalace
- pořizuje záznamy provozních událostí do Trouble Ticket System (TTS)
- zpracovává a distribuuje periodická hlášení a reporting o dostupnosti služeb a datovém zatížení infrastruktury
- provádí zálohování dat podle schválené dokumentace
- dohlíží na dodržování postupů Řízení změn (Change management), Řízení konfiguračních položek (Configuration management) HW a SW a jejich dokumentace
- plánuje a provádí ověřovací a profylaktické činnosti
- provádí správu a uchovávání logů
- klasifikuje poruchy a odchylky od provozního stavu, spoluvytváří postupy pro jejich odstraňování a provádí jejich dokumentaci prostřednictvím TTS (trouble ticket systém)
- spolupracuje s administrátory při řešení incidentů

Všeobecné vlastnosti monitoringu:

- Konsolidace a korelace systémových událostí v reálném čase a "root-cause"
- Kompletní viditelnost všech KPI a SLA napříč aplikacemi, síťovými segmenty nebo provozními jednotkami.
- Jednotné grafické prezentační prostředí a single-sign on
- Integrace s externími systémy a tzv. business context - tedy jak jsou technologie napojeny na podnikové/obchodní funkce
- Drill-down – vizualizace od přehledových pohledů až po detailní pohledy pro konkrétní technologie
- Nativní provázanost s ostatními moduly – síťový a aplikační performance management, Service Desk, Storage, atd.



Obrázek 33: Monitoring systému EET

Koncepčně existují tyto funkční bloky:

- **Business Service Management:** Nejvyšší vrstva, která poskytuje celkový přehled o službách, aplikacích, transakcích a procesech. Tato vrstva sleduje agregované KPI a vyhodnocuje SLA a celkovou výkonnost IT organizace
- **Consolidated Operations Management:** Konsolidace fault a performance dat a tzv. umbrella management, tedy jednotná správa nad celou heterogenní technologickou a aplikační infrastrukturou
- **Domain Management:** Správa jednotlivých technologických domén jako jsou sítě, aplikace, security, storage, VoIP atd.

Metriky:

- Objem transakcí
- Transakční chyby
- Výkonnost procesů a jejich degradace
- Celkový zisk služby, dostupnost, SLA a případná penalizace
- Záznamy o incidentech a problémech
- Žádosti o změnu ('change request')

SLA Monitoring

- Aktuální stav SLA
- Procentuální poměr, kdy je služba dostupná

- Celkový down-time služby pro dané SLA
- Zbývající čas do překročení SLA
- Celková cena (penalizace) za nedostupnost služby
- Systémová architektura

Monitoring infrastruktury

Prostředky pro správu a dohled EET budou připojeny k infrastruktuře SPCSS prostřednictvím nezávislé administrativní sítě.

Do jednotlivých VLAN logických sítí jsou připojovány jednotlivé komponenty admin (Out-Of-Band) sítě.

Pro vzdálené připojení administrátorů z prostředí Internetu nebo Intranetu slouží tentýž hardware ve funkci VPN koncentrátoru. Autentizace administrátorů je možná prostřednictvím AAA serveru umístěným v jednom z bezpečných segmentů admin sítě nebo prostřednictvím „master“ AAA serveru SPCSS. Vlastní autentizace je realizována prostřednictvím hesla a certifikátu pro identifikaci uživatele resp. klíč pro IPSEC komunikaci.

Pro větší bezpečnostní oddělení administrátorů bude mezi administrátora a vlastní spravované prostředky vložen server s terminálovými službami. Vlastní nástroje pro administraci pak mají jednotliví uživatelé umístěny na těchto aplikačních terminálových serverech. Přenášena data mezi administrátorem a terminálovým serverem jsou data „o obrazovce a klávesnici“.

Síťové prvky v admin síti musí podporovat technologii PVLAN (Private VLAN).

Každý dohlížený prvek je do OOB sítě zapojen samostatným Ethernet portem s možností nastavení protokolových pravidel na tomto portu (síťové prostředky Access-list, servery lokální firewally jako je např. iptables v linuxu apod.)

Každý síťový prvek je navíc připojen do OOB sítě ještě jedním nezávislým kanálem a to je konzolový port. Konzolové porty z admin sítě jsou dostupné přes síťový terminálový server.

Požadavky na fyzické a technologické zabezpečení datový sálů EET

Prostory, kde bude datový sál EET umístěn, musí odpovídat následujícím požadavkům:

- a) teplota prostředí se pohybuje v rozmezí od 19°C do 25°C, relativní vlhkost v rozmezí 35% - 65%,
- b) v místnostech, kde je datový sál EET umístěn, jsou instalována požární čidla na kouř a teplotu,
- c) tyto prostory jsou napojeny na systém elektronické protipožární signalizace a elektronické zabezpečovací signalizace, a jsou vybaveny kamerovým systémem hlídající vstup do prostor a jednotlivé uličky mezi stojany s možností přisvětlení ve tmě
- d) prostory jsou vybaveny stabilním hasicím zařízením s hasicím médiem FM 200, Novec 1230 či obdobným
- e) technologické prostory datového sálu EET musí mít instalovaný dveřní systém v bezpečnostní třídě WK 2 podle EN 1627 s mechanickým zavíračem dveří, včetně přidržovacího elektromagnetického zařízení a elektronického zámku s napojením na stávající systém EKV
- f) požadavky zajištění silnoproudých rozvodů:
 - i. všechny technologické prostory jsou vybaveny mezilehlým rozvaděčem se dvěma samostatnými okruhy:
 - i. nezálohovaná AC síť 230V,
 - ii. AC síť 230V zálohovaná generátorem,

- b. technologické prostory jsou vybaveny distribučním stojanem se dvěma samostatnými okruhy určeným pro napájení zařízení ve stojanových řadách, jeden okruh bude napájen ze zálohované sítě generátorem a druhý bude napájen ze záložního generátoru přes centrální UPS jako zdroj nepřerušitelného napájení.,
- g) požadavky zajištění zálohování silnoproudého napájení:
 - a. technologické prostory jsou vybaveny nepřerušitelným zdrojem v kapacitě min. 50 kVA v modulární výstavbě s možností výkonového rozšíření na 80 kVA, s umístěním co nejbližší distribučního stojanu, na překlenutí náběhu generátoru max. 5 min.,
 - b. modulární řešení UPS předpokládá redundanci N+1, jak řídících, tak výkonových modulů, včetně řešení redundance baterií (2 okruhy). Požadujeme možnost výměny výkonových modulů i baterií bez přerušení provozu. UPS vybavit modulem pro vzdálený dohled (SNMP a WWW přístup) ,
- h) požadavky zajištění klimatizace
 - a. všechny technologické prostory požadujeme vybavit klimatizačním systémem na plánovanou kapacitu.
 - b. návrh řešení komplexního chladicího systému musí obsahovat flexibilní a modulární systém klimatizačních prvků, modulů s možností reakce na změny zátěže v jednotlivých místnostech i stojanových řadách v průběhu doby dle požadavků provozovatele.
 - c. řešení klimatizace musí umožňovat redundanci N+1 a střídání základních modulů, jak chladicího systému, tak ventilačního systému, včetně možnosti výměny vadného modulu bez přerušení provozu. Systém vybavit modulem pro vzdálený dohled (SNMP a WWW přístup)
 - d. řešení chladicího systému musí zohledňovat uzavřenou stojanovou řadu se stojany 800 x 1000 mm s chladicím výkonem 8 kW na každý stojan, určené pro technologická zařízení s příkonem přesahujícím 2,5 kW.
- i) v datovém sálu EET musí být instalované stojany modelově „řady DK-TS8“, určené pro zařízení s montáží do 19" lišt o hloubce 1 m a montážní výškou 42U s následujícími vlastnostmi: robustní svařovaný rám, statická zatížitelnost 1000 kg, čtyřbodové zamykání, včetně bezpečnostního zámku vpředu i vzadu, 19" montážní rám vpředu i vzadu, zemnění všech částí stojanu,
- j) v datovém sálu EET je instalován systém zvýšené podlahy pro aplikaci komunikační kabeláže a silnoproudých rozvodů s zátěží dimenzovanou minimálně na 850 kg/m², při požadavku na vyšší nosnost - možnost instalace roznášecích roštů
- k) je zajištěna vnější ochrana budovy bezpečnostní službou nepřetržitě 24 hodin denně a 7 dní v týdnu, přičemž jsou prokazatelně evidovány osoby vstupující do objektu, v němž se prostory s datovým sálem EET nacházejí,
- l) datový sál EET splňuje podmínky Vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. pro **stupeň utajení Důvěrné**,
- m) prostory, v nichž se datový sál EET nachází, leží mimo zátopovou oblast tzv. stoleté vody,
- n) datové sály EET jsou z hlediska geografické lokalizace umístěny ve dvou různých lokalitách, které splňují podmínku, že jsou od sebe vzdáleny více než 6000 metrů a méně jak 30000 metrů a jsou napájeny z různých rozvodů elektrické energie,
- o) možnost instalace systému datových komor s možností rozšíření nebo demontáže a následné montáže, splňující fyzickou bezpečnost dle *Certifikátu technického prostředku NBÚ, třída 2, požadované krytí IP56*),
- p) datové sály EET jsou redundantně připojeny na páteřní infrastrukturu MFČR a Internet

Kapacita datových sálů

V datovém sále EET je požadováno umístění minimálně 5 stojanů modelově „řady DK-TS8“, určené pro zařízení s montáží do 19" lišt o hloubce 1 m a montážní výškou 42U.

Specifikace požadavků na testování systému

Testování je nedílnou součástí životního cyklu vývoje webových služeb a výstavby prostředí pro provoz systému EET. Zabezpečuje udržování kvality celého řešení. Testování se řídí podobnými pravidly jako tvorba aplikace. Z pohledu RUP jako obecné metodiky pro tvorbu aplikací je na začátku testování nutné vytvořit testovací případy (testcase). Je to obdoba tvorby případů užití (usecase) v rámci návrhu aplikace.

Test Case je obvykle tvořen jedním nebo vícero kroky. Test case obsahuje následující údaje:

- test case ID,
- test case popis,
- testovací kroky nebo pořadí testování,
- nutné požadavky k výkonu testu,
- síla testu,
- test kategorie,
- autor,
- označení, jestli test je automatizován, nebo ne (jestli je možno jej pravidelně spouštět),
- výsledek testu (úspěšný/neúspěšný),
- poznámky.

V případě testování celého řešení EET budou jednotlivé testy rozděleny do několika oblastí:

- Testování infrastruktury (non-functional test)
- Testování webových služeb (functional test)

Testování infrastruktury v sobě zahrnuje:

- Výkonnostní testování
- Integrovaní testování
- Bezpečnostní testování
- Disaster-Recovery testy
- Load test

Cílem testování samotné infrastruktury je:

- ladění systémových parametrů,
- odstranění potencionálních problémů z pohledu bezpečnosti, výkonnosti,
- nastavení spodních prahových hodnot pro další testování, při postupné instalaci jednotlivých aplikačních komponent,
- otestování obnovy systému při jeho pádu (single-point-of-failure)
- testování rozkládání zátěže mezi jednotlivé komponenty v rámci clusteru
- otestování přepnutí do záložní lokality a obnova primární lokality
- otestování monitorování prostředí
- otestování zálohování prostředí a obnova jednotlivých komponent

Test Disaster Recovery

Speciálním typem funkčního testu z pohledu funkcionality EET je test disaster-recovery. Tento test bude proveden k otestování:

1. fyzické kapacity infrastruktury,
2. validaci postupů navržených pro účely disaster-recovery,
3. validaci týmu pro provedení jednotlivých procesů,
4. validaci časového plánu,
5. zjištění možných ztrát dat při ztrátě jedné lokality,
6. validaci postupů návratu zpět do primární lokality,
7. validaci času potřebného pro návrat do primární lokality.

Tyto testy budou prováděny pravidelně podle stanoveného plánu těchto testů.

K tomu, abychom mohli dostatečně kvalitně otestovat infrastrukturu, bude zapotřebí vytvořit vlastní testovací služby, které běží na jednotlivých komponentách a zároveň vytvoření vlastních "pokladen" simulujících reálný provoz.

Zátěžový test (load test)

Zátěžový test patří mezi nefunkční testy, slouží pro validaci výkonnosti:

- samotných služeb,
- provozního prostředí.

Pro správné otestování zátěže bude nutné vytvořit sadu klientů (pokladen), kteří budou simulovat reálný provoz. To znamená vytvořit zhruba až 4000 transakcí za sekundu simulujících pokladniční systémy povinných subjektů, které nám vytvoří zátěž s následujícími parametry:

- 4000 dotazů za 1s na fiskalizační rozhraní
- 100 editačních dotazů za 1s na portále.

Výsledky této zátěže budou zpracovány do formy výstupního reportu. Zátěžové testy budou prováděny za přítomnosti monitorovacích nástrojů. Důvodem je zjištění jednotlivých časových zpoždění, která vznikají na komponentách infrastruktury nebo konkrétních služeb.

Nutnou podmínkou zátěžového testu je monitorování jednotlivých komponent na úrovni:

- hardware (využití CPU, paměť),
- propustnost sítě,
- výkonnosti samotné služby,
- výkonnosti aplikačních platforem.

Na základě výsledku zátěžového testování, bude identifikováno, kde jsou slabá místa v rámci infrastruktury EET a jednotlivých služeb implementovaných v rámci EET.

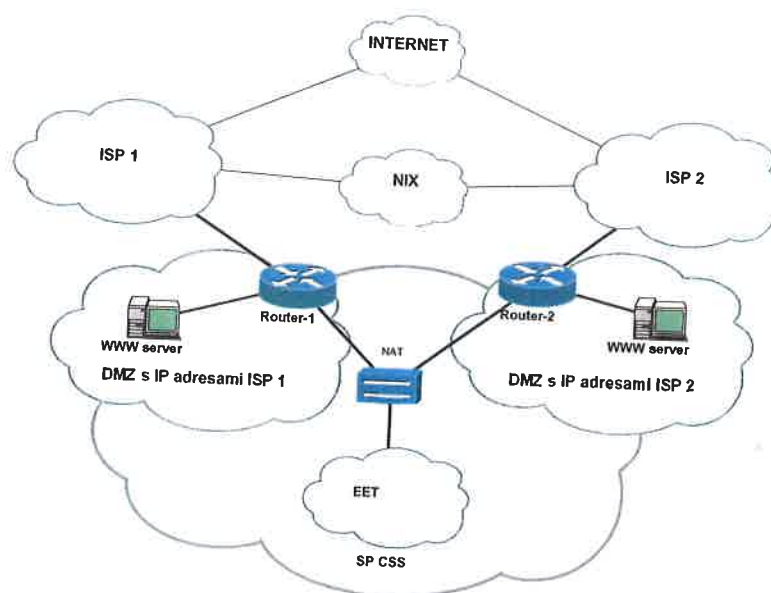
Požadovaná architektura připojení do Internetu pro systém EET

K poskytování služby EET, u které je zapotřebí udržet vysokou dostupnost fiskalizačních serverů, je nutné mít zálohované připojení. Vícenásobné připojení k jednomu poskytovateli (ISP - Internet Service Provider) je nejjednodušší variantou. Připojení SPCSS k síti Internet je v současné době realizováno prostřednictvím poskytovatele T-Mobile, dvěma nezávislými optickými spoji o rychlosti 100 Mbit/s.

Takovéto připojení však neřeší zajištění dostupnosti služby v případě problému na hraničních zařízeních ISP. Zajištění velmi vysokých nároků na dostupnost je možné dosáhnout pouze při připojení na více poskytovatelů. Pro realizaci projektu EET bude zapotřebí navýšit kapacity a způsob připojení SPCSS k síti Internet. Kapacitu připojení bude zapotřebí navýšit na 2 x 1Gb/s (1Gb/s dvěma optickými spoji). Architektura a možné způsoby realizace připojení SPCSS k síti Internetu pro potřeby projektu EET jsou rozebrány níže. Jedná se o připojení SPCSS do dvou nezávislých přístupových bodů internetu a 3 možné varianty připojení na vícero poskytovatelů připojení k síti Internet. Jako nejvhodnější se jeví poslední varianta připojení prostřednictvím vlastního autonomního směrovacího systému.

Připojení s použitím adres od více ISP

Tato možnost je často používána. Organizace obdrží od každého poskytovatele blok adres, který použije při adresaci svých serverů.



Obrázek 34 : Schéma zapojení s použitím adres více ISP

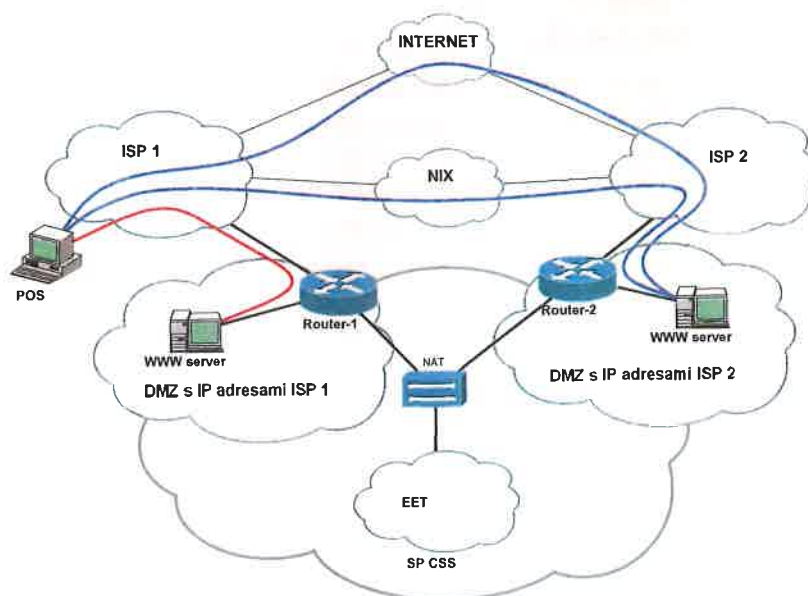
Pojmenování serverů je možné v DNS provést dvěma způsoby:

- každé IP adrese je přiřazeno jméno
- všem IP adresám je přiřazeno pouze jediné jméno

Pokud je každé IP adrese přiřazeno jiné jméno je pokladní systém povinného subjektu (dále jen POS) nucen si vybrat z různých připojení to, u kterého má nejlepší odezvu. Sám POS si vybírá nejlepší cestu (Obrázek 35). V případě nedostupnosti sám musí zkusit připojení na další server.

Pokud je adresám přiřazeno pouze jediné jméno nemusí sice POS vyhledávat nejlépe dostupný server, ale jmenné servery mu vrací IP adresy serverů v cyklu (tzv. round robin). Stává se tedy, že přestože stále vstupuje na tentýž odkaz, mívá různou odezvu podle toho, kterou IP adresu dostane od jmenného serveru. Nejlepší připojení je přímo u ISP (Obrázek 35 - červená cesta). U ostatních cest (Obrázek 35

- modré cesty) již dochází ke zpoždění. Při připojení přes NIX nemusí být zpoždění nijak dramatické, ale zpoždění na vytižených zahraničních linkách již může být pro POS obtěžující.

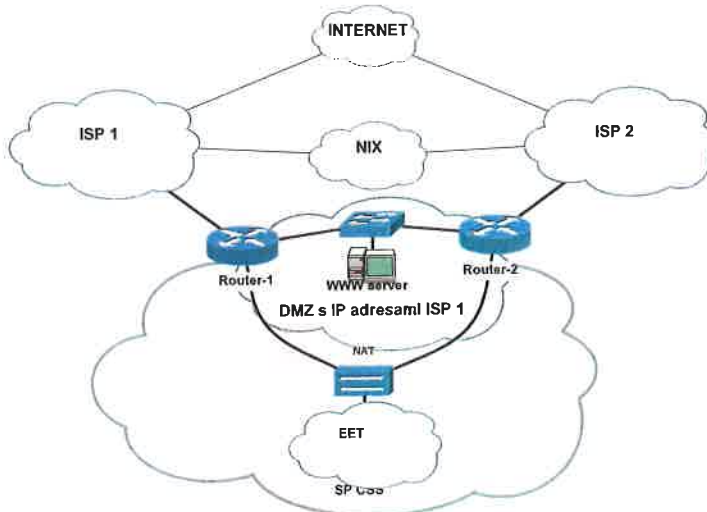


Obrázek 35 : Schéma přístupu POSu k serverům

Tato varianta tudíž není příliš vhodná pro poskytování služeb EET. Její výhodou je však jednoduchost a možnost provozování bez nutnosti nadstandardní spolupráce s ISP.

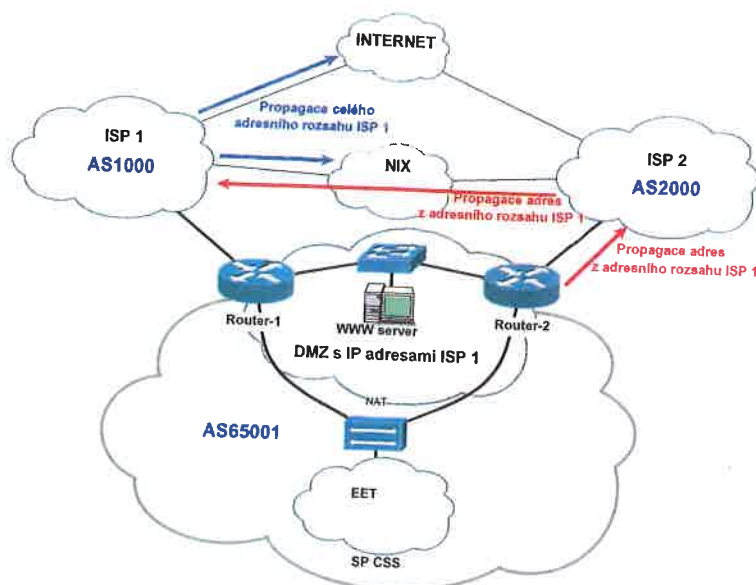
Připojení s použitím adres jednoho z ISP

Mnohem efektivnější než předchozí varianta je využít připojení s adresním prostorem pouze jediného poskytovatele připojení (Obrázek 36). Díky jedinému adresnímu prostoru je zajištěno, že POS vždy k serverům přistupuje pouze jedinou cestou, která se za normálního stavu nemění.



Obrázek 36 : Schéma zapojení pouze s IP adresami jednoho z ISP

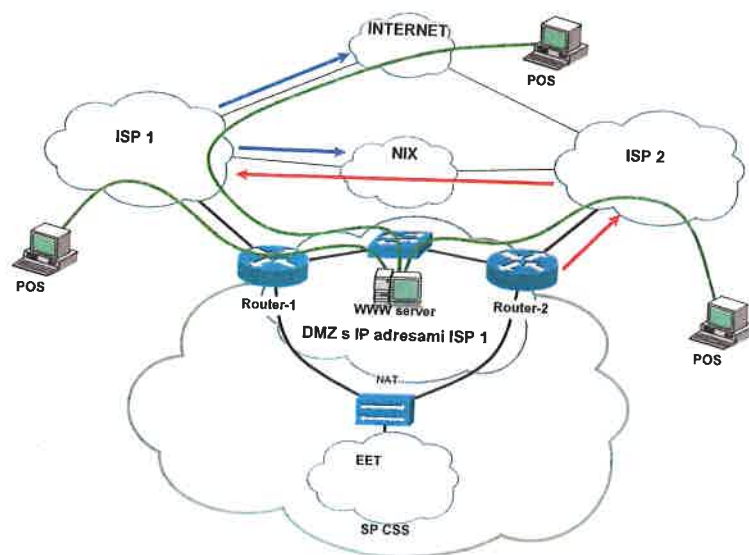
Tato varianta je mnohem vhodnější pro komunikaci mezi systémem EET a POsem, ale vyžaduje nadstandardní spolupráci s poskytovateli připojení. Také již vyžaduje použití vnějšího směrovacího protokolu. Z důvodu zamezení nežádoucího propojení mezi sítěmi ISP je téměř nezbytné použití BGP (Border Gateway Protocol).



Obrázek 37 : Schéma zapojení s použitím směrovacího protokolu BGP

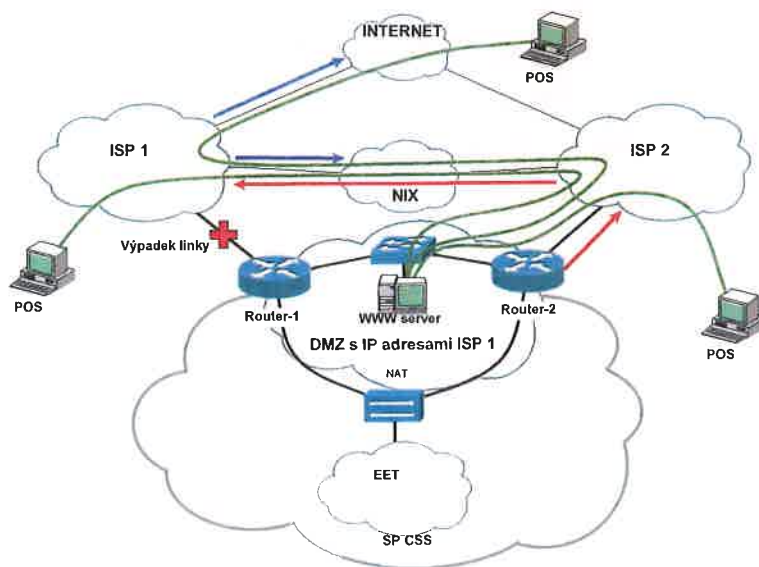
Je nutné zajistit domluvu a souhlas ISP k šíření bloku adres, který je přidělen jednomu z poskytovatelů i v ostatních sítích (Obrázek 37). ISP 1 jehož adresy jsou použity šíří směrovací informace do internetu standardním způsobem (modré šipky). Do sítě dalších poskytovatelů se po dohodě šíří směrovací informace o bloku adres z privátního autonomního systému AS65001, v němž jsou použity adresy přidělené poskytovatelem ISP1. Tito ostatní poskytovatelé mohou tyto směrovací informace předávat hraničním směrovačům ISP1 (červené šipky).

Poskytování směrovacích informací z privátního AS dalším poskytovatelům umožní přímý přístup k serverům i POSům připojeným prostřednictvím těchto ISP (Obrázek 38).



Obrázek 38 : Schéma toku dat za normálního stavu sítě

Předávání směrovacích informací o bloku adres použitým v privátním AS na hraniční směrovače poskytovatele ISP1 vytváří záložní spojení pro případný výpadek linky mezi organizací a ISP (Obrázek 39).



Obrázek 39 : Schéma toku dat při výpadku linky k ISP

Poskytování směrovacích informací jiným poskytovatelům nebo do obecně internetu je sice možné, ale nemusí vždy fungovat. Většina ISP totiž kontroluje a filtruje směrovací informace, které neodpovídají doporučení a informacím uvedených v databázích organizace RIPE (Réseaux IP Européens).

Mimo jiné akceptují směrovací informace s minimálním prefixem /19 případně /20 (Tabulka 2) a menší bloky ignorují. Dále mohou akceptovat směrovací informace o síti pokud přichází z AS uvedeného v databázích organizace RIPE.

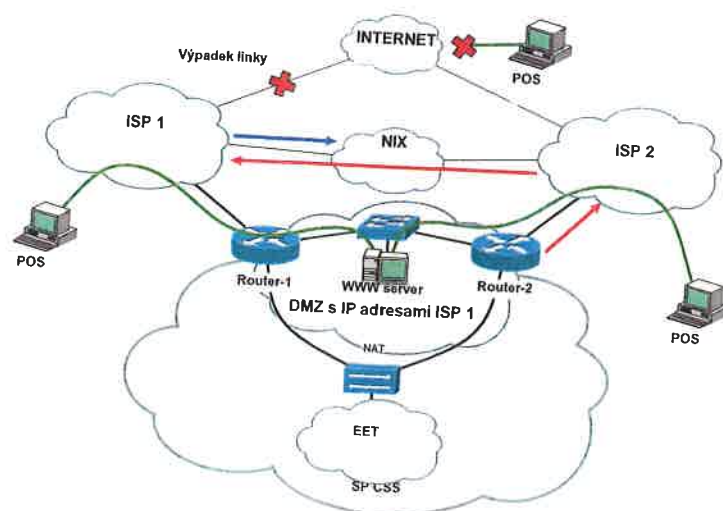
Počet adres	Počet bitů	Prefix	Maska
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1K	10	/22	255.255.252.0
2K	11	/21	255.255.248.0
4K	12	/20	255.255.240.0
8K	13	/19	255.255.224.0
16K	14	/18	255.255.192.0
32K	15	/17	255.255.128.0
64K	16	/16	255.255.0.0

Počet adres	Počet bitů	Prefix	Maska
128K	17	/15	255.254.0.0
256K	18	/14	255.252.0.0
512K	19	/13	255.248.0.0
1M	20	/12	255.240.0.0
2M	21	/11	255.224.0.0
4M	22	/10	255.192.0.0
8M	23	/9	255.128.0.0
16M	24	/8	255.0.0.0
32M	25	/7	254.0.0.0
64M	26	/6	252.0.0.0
128M	27	/5	248.0.0.0
256M	28	/4	240.0.0.0
512M	29	/3	224.0.0.0
1024M	30	/2	192.0.0.0

Tabulka 2 : Označování velikosti adresního prostoru a směrovacího předčísli (routing prefix)

počet bitů	Velikost přiřazeného adresního prostoru v bitech
počet adres	Množství dostupných adres při použité masce. Je však nutné mít na paměti, že normálně je počet stanic o 2 nižší, protože nejnižší a nejvyšší adresy (samé nuly, samé jedničky v části označující stanici) jsou rezervovány.
prefix	Délka směrovacího předčísli (routing prefix) adresního prostoru.
maska	Síťová maska definující směrovací předčísli (routing prefix) ve formě čtyř čísel oddělených tečkou.

Při dodržování pravidel a doporučení je tedy možné, v případě ztráty konektivity ISP1 do internetu, že se zákazníci nebudou moci připojit (Obrázek 40). Obdobné problémy by mohly nastat i v případě ztráty konektivity do NIXu.



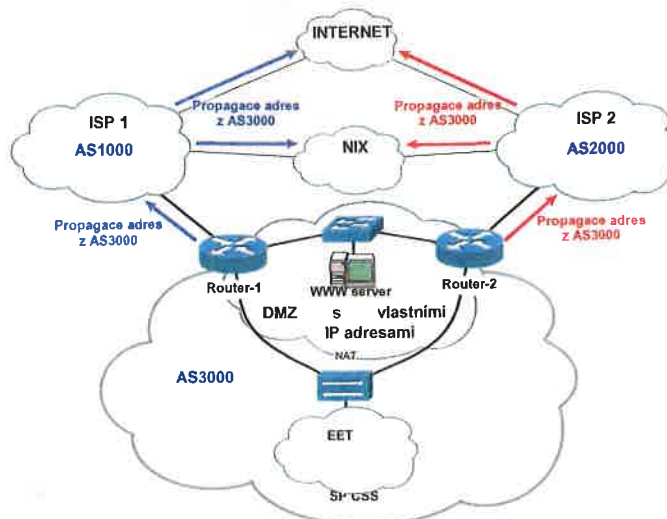
Obrázek 40 : Schéma toku dat při výpadku zahraniční konektivity ISP

Při použití této varianty je potřeba velice dobře vybírat poskytovatele, z jehož adresního prostoru budou adresy použity. Je velice žádoucí aby tento ISP měl zálohovanou konektivitu do internetu i do NIXu přes více směrovačů. Potom nebezpečí nedostupnosti serveru klesá na minimum.

V případě potřeby je možné požádat o „provider independent“ adresy, které umožní rychle změnit poskytovatele bez nutnosti přeadresování. Při přechodu stačí pouze změnit záznamy v databázích RIPE.

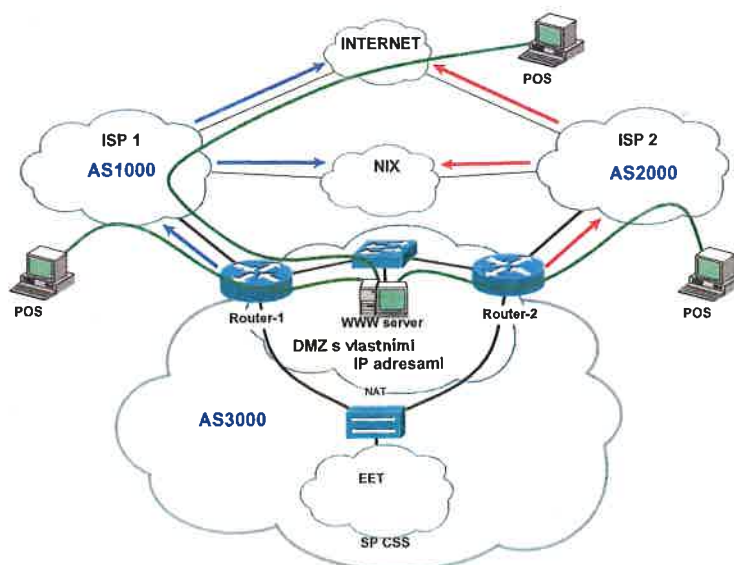
Připojení s vlastním autonomním systémem

Z hlediska technického se jeví varianta s vlastním autonomním systémem jako nejlepší. Tato varianta řeší všechny nevýhody předchozích variant. Směrovací informace jsou propagovány od všech ISP, se kterými je toto domluveno. Za všech okolností jsou dodrženy doporučení RIPE a není zapotřebí jiné nastavení směrování než je uvedeno v databázích RIPE.

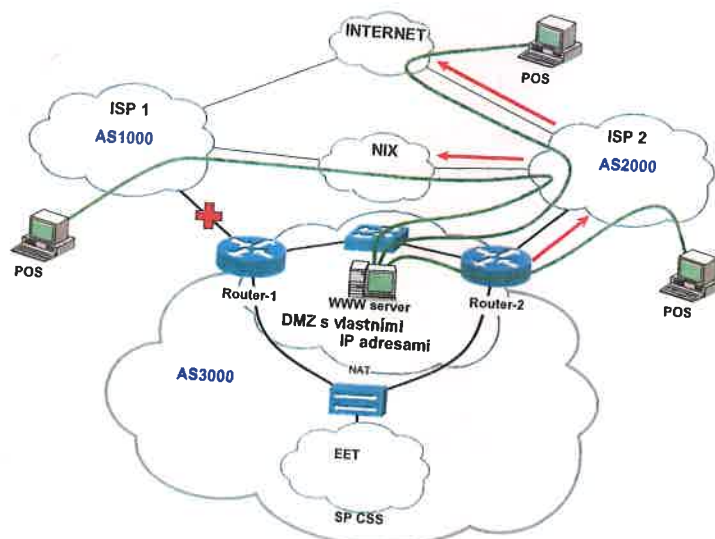


Obrázek 41 : Schéma zapojení s vlastním AS

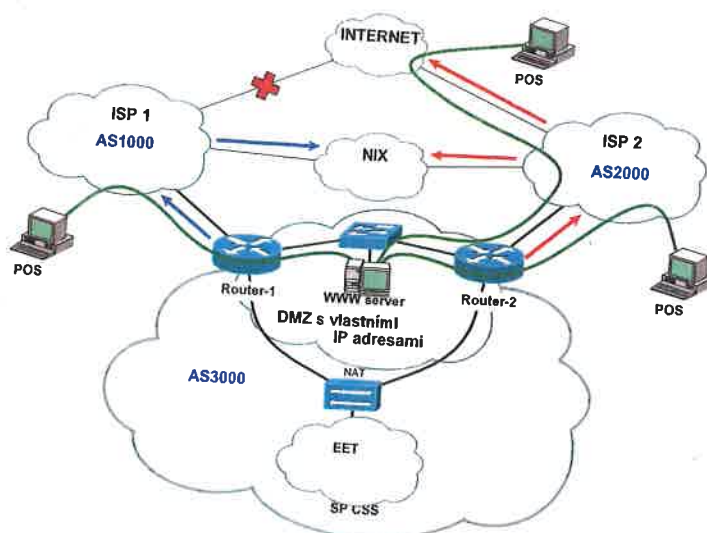
Za libovolného stavu je pro směrování provozu mezi POSem a EET hledána nejvýhodnější cesta (Obrázek 42, Obrázek 43 a Obrázek 44). Ani v případě ztráty zahraniční konektivity ISP nedojde k nedostupnosti služby EET.



Obrázek 42 : Schéma toku dat za normálního stavu sítě



Obrázek 43 : Schéma toku dat při výpadku linky k ISP



Obrázek 44 : Schéma toku dat při výpadku zahraniční konektivity ISP

Pro provozování vlastního AS je nutné podat žádost na RIPE NCC (Réseaux IP Européens Network Coordination Centre).

Tato varianta je z hlediska dodržování pravidel nesprávnější. Přináší však i některé problémy.

U menších sítí jsou přiděleny rozsahy adres jejichž samostatné směrování je doporučováno. Bohužel velcí poskytovatelé, především v USA, tato doporučení občas nerespektují a mohou nastat problémy s dostupností do těchto sítí.

Hraniční směrovače by měly mít plné směrovací tabulky. To klade vysoké nároky na paměť a výkon směrovačů. S rostoucími nároky roste cena zařízení.

Je nutné dosáhnout maximální stability hraničních směrovačů. Různé nestability mohou vést k přetěžování směrovačů. Proto má většina ISP nakonfigurovanou ochranu proti „nestabilním sítím“ a v případě několikeré změny směrovacích informací v krátkém čase přestane, na nastavenou dobu, přijímat směrovací informace z těchto sítí. Po tuto dobu budou problémy s dostupností některých sítí.

Analýza rizik

Cílem řízení rizik je identifikace a specifikace jednotlivých rizik projektu včetně posouzení jejich dopadů a celkové závažnosti a vymezení vhodných opatření na prevenci daného rizika nebo omezení následků při reálném uplatnění daného rizika. Na základě identifikace a specifikace jsou následně vybraná opatření plánována v rámci projektu.

Některá identifikovaná rizika mohou být záměrně akceptována bez jakýchkoli opatření (nebo jen s omezenými opatřeními) s ohledem na přílišnou (danému riziku neadekvátní) náročnost některých opatření (zejména nároky na časové, finanční a lidské zdroje).

Řízení rizik projektu provádí průběžně Vedení řešitelských týmů a konsoliduje Vedení projektového týmu. Tuto činnost koordinuje projektový manažer tak, aby se plně prošetřila možná rizika. Zjištěná závažná rizika, jejich dopady a návrhy na jejich řešení či omezení jsou neprodleně předkládána a eskalována k posouzení a případnému rozhodnutí ŘK projektu.

Identifikace a vyhodnocení rizik a opatření přijatá pro jejich následnou eliminaci jsou obsahem následujících subkapitol.

První fází analýzy rizik je identifikace potenciálních rizik, která spočívá v zjištění a následné evidenci významných rizik. Následnou druhou fází analýzy představuje vyhodnocení identifikovaných rizik, které je prováděno na základě hodnocení míry dopadu a pravděpodobnosti výskytu rizika.

Identifikace rizik

Jedním z významných aspektů řízení rizik je identifikace (definice) potenciálních rizik, která lze dle svého charakteru rozdělit do předem definovaných klasifikačních skupin:

- A. právní rizika;
- B. finanční rizika;
- C. technická rizika;
- D. personální rizika;
- E. provozní rizika;
- F. bezpečnostní rizika;
- G. projektová rizika.

Následující tabulky představují výsledný seznam identifikovaných potenciálních rizik, která mohou nastat v průběhu přípravy či realizace předkládaného projektu, ale i v průběhu běžného provozu celkového projektu. Pro zvýšení přehlednosti byla jednotlivá rizika označena kódem (např. A.1, B.3, apod.).

Právní rizika		
Kód	Riziko	Dopad
A.1	Nedodržení právních norem ČR, EU.	Zpoždění projektu z důvodu nápravy stavu nebo protiprávnost části projektu a možné náhrady škody.
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	Snížení nebo absence přínosů z důvodu nevymožitelnosti povinností poplatníků nebo kompromitace projektu samotného.
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	Alternativní řešení technických a jiných projektových potřeb za zvýšenou cenu, nebo nevymožitelnost náhrady škody a sankcí.

Finanční rizika		
Kód	Riziko	Dopad
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	Nemožnost vyhodnotit projekt z finanční stránky, částečná kompromitace projektu.
B.2	Navýšení cen technologií, služeb a prací a dalších vstupů.	Zvýšení celkových nákladů projektu a zároveň zvýšení nároků na financování projektu v realizační fázi projektu.
B.3	Růst provozních nákladů v provozní fázi projektu.	Zvýšení provozní náročnosti.

Technická rizika		
Kód	Riziko	Dopad
C.1	Výběr nekvalitního dodavatele.	Ohrožení kvality výstupu projektu a prodloužení doby realizace. Riziko zvýšených nákladů (dodatečných) na nápravu stavu.
C.2	Výběr nevhodné technologie.	Ohrožení kvality výstupu projektu nebo projektu vůbec, prodloužení doby realizace. Riziko zvýšených nákladů (dodatečných) na nápravu stavu.
C.3	Riziko související se zařízením (pře/poddimezovaná kapacita / výkon)	Kompromitace projektu, neschopnost plnit legislativní povinnosti za strany státu.

Personální rizika		
Kód	Riziko	Dopad
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	Neefektivní fungování projektového týmu. Ohrožení přípravy a realizace projektu či běžného provozu.
D.2	Nedostatečný vnitřní kontrolní systém.	Neefektivní fungování projektového týmu. Ohrožení realizace projektu či běžného provozu.
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	Ohrožení běžného provozu.
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	Nedostatečně kvalitní personální zajištění fungování.
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	Ohrožení projektu, nebo běžného provozu. Zvýšené náklady na projekt nebo provoz.
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	Zvýšené náklady na projekt nebo provoz. Ohrožení kvalitativní úrovně projektu.

Provozní rizika		
Kód	Riziko	Dopad
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	Ohrožení běžného provozu.
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	Ohrožení běžného provozu.
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	Zvýšené náklady na provoz. Ohrožení kvalitativní úrovně provozu.

Bezpečnostní rizika		
Kód	Riziko	Dopad
F.1	Krádež technologií nebo jejich poničení.	Znemožnění provozování dané technologie, resp. nutnost její opravy.
F.2	Teroristický útok (včetně kybernetického útoku).	Ohrožení běžného provozu. Nebezpečí poničení technologií a systému. Možné ohrožení z hlediska reputace a důvěryhodnosti projektu.
F.3	Bezpečnostní rizika	Kompromitace bezpečnostních prvků; narušení bezpečnosti v oblasti dostupnosti, důvěrnosti nebo integrity dat.
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákonu o ochraně utajovaných skutečností.	Kompromitace bezpečnostních prvků; kompromitace projektu, změny projektu a zvýšené náklady. Škody značného rozsahu v případě prozrazení utajovaných skutečností.

Projektová rizika		
Kód	Riziko	Dopad
G.1	Nedostatky v projektové dokumentaci.	Může dojít k celkovému zpoždění realizace.
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částečné přebírání výstupů dodavatele)	Může dojít k akceptaci nekvalitního díla a služeb nebo jejich částí.
G.3	Dodatečné změny v projektu.	Dodatečné změny by mohly významně ovlivnit dobu realizace projektu a ohrozit jeho realizaci.
G.4	Špatná koordinace dodavatelských prací.	Zpoždění zahájení provozu. Riziko snížení kvality dodaných prací/služeb/technologií.
G.5	Zpochybnění validity projektu	Kompromitace projektu a nesplnění cílů projektu.
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	Zpochybnění realizátora projektu, případné opakování soutěží, nebo zpoždění projektu.
G.7	Nedodržení termínu realizace.	Zpoždění zahájení provozu. Nedosažení plánovaných přínosů. Neshoda s legislativou.

Hodnocení rizik

Druhou fází analýzy rizik je její **vyhodnocení**, které spočívá v určení **míry dopadu „D“** rizika a **pravděpodobnosti výskytu „P“** rizika. Obě veličiny jsou hodnoceny v kvalitativních bodových škálách (stupnicích) s definovaným významem jednotlivých bodů škály. Míra dopadu (vlivu) rizika „D“ a pravděpodobnost výskytu rizika „P“ jsou hodnoceny dle stupnice uvedené v následující tabulce:

Hodnota	Dopad	Pravděpodobnost výskytu	Míra dopadu/ pravděpodobnosti
1	Téměř neznatelný	Téměř nemožná	Velmi malá
2	Drobný	Výjimečně možná	Malá
3	Významný	Běžně možná	Střední
4	Velmi významný	Pravděpodobná	Vysoká
5	Nepřijatelný	Hraničící s jistotou	Velmi vysoká

Z hlediska efektivity řízení rizik je nutné pro každé riziko stanovit jeho význam (interpretovatelný jednou konkrétní hodnotou), který zahrnuje jak míru dopadu rizika, tak i pravděpodobnost jeho výskytu. Z tohoto důvodu byl pro každé riziko stanoven stupeň **významnosti rizika „V“**, který je definován jako součin bodového ohodnocení dopadu rizika „D“ a pravděpodobnosti výskytu rizika „P“.

$$V = D \times P$$

Významnost rizika „V“ lze na základě dosažitelných hodnot klasifikovat dle do 3 skupin (viz stupnice dle následující tabulky). Distribuce dosažených hodnot významnosti rizika „V“ u všech definovaných rizik je v grafické podobě zpracována formou mapy rizik (viz kapitola „Mapa rizik“).

Stupeň významnosti	Hodnota
Běžné	1 – 4
Závažné	5 – 11
Kritické	12 – 25

Pro úspěšné řízení rizik je nejdůležitější zaměřit se na rizika nejzávažnější (rizika spadající do kategorie „Kritická rizika“), která je nutné co nejdříve eliminovat nebo alespoň minimalizovat.

Cílem této podkapitoly tedy bylo vytvoření tzv. **katalogu rizik**, ve kterém jsou uvedeny hodnoty pro míru dopadu, pravděpodobnost výskytu a významnost rizik.

Následující tabulka představuje výsledný katalog rizik – souhrn potenciálních rizik, která mohou nastat v průběhu přípravy a realizace předkládaného projektu, ale i v průběhu běžného provozu.

Kód rizika	Riziko	Míra dopadu	Míra pravděp. výskytu	Stupeň významnosti
Právní rizika				
A.1	Nedodržení právních norem ČR, EU.	5	1	5
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	5	1	3
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	3	2	6
Finanční rizika				
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	1	3	3
B.2	Navyšování cen technologií, služeb a prací a dalších vstupů.	2	3	6
B.3	Růst provozních nákladů v provozní fázi projektu.	3	3	9
Technická rizika				
C.1	Výběr nekvalitního dodavatele.	3	3	9
C.2	Výběr nevhodné technologie.	4	4	16
C.3	Riziko související se zařízením (pře/poddimenzovaná kapacita / výkon)	4	3	12

Kód rizika	Riziko	Míra dopadu	Míra pravděp. výskytu	Stupeň významnosti
Personální rizika				
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	2	3	6
D.2	Nedostatečný vnitřní kontrolní systém.	2	2	4
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	2	5	10
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	2	2	4
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	2	4	8
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	2	5	10
Provozní rizika				
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	3	1	3
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	2	2	4
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	1	5	5
Bezpečnostní rizika				
F.1	Krádež technologií nebo jejich poničení.	3	1	3
F.2	Teroristický útok (včetně kybernetického útoku).	5	2	10
F.3	Bezpečnostní rizika	3	5	15
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákona o ochraně utajovaných skutečností.	5	2	10
Projektová rizika				
G.1	Nedostatky v projektové dokumentaci.	1	3	3
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částkové přebírání výstupů dodavatele)	4	3	12
G.3	Dodatečné změny v projektu.	3	5	15
G.4	Špatná koordinace dodavatelských prací.	3	3	9
G.5	Zpochybnění validity projektu	3	2	6
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	1	2	2
G.7	Nedodržení termínu realizace.	5	2	10

Mapa rizik

Mapa rizik slouží ke grafickému znázornění katalogu rizik – míry dopadu „D“, pravděpodobnosti výskytu „P“ a stupně významnosti „V“ identifikovaných rizik. Mapa rizik je promítnuta v následující tabulce, ve které je zobrazeno rozložení jednotlivých rizik do definovaných kategorií významnosti rizik. Nejvíce identifikovaných rizik spadá do kategorie „Běžná rizika“. Přesto bude kladen důraz na eliminaci všech identifikovaných rizik, protože mohou v případě vzájemného souběhu negativně ovlivnit projekt.

Mapa rizik		Pravděpodobnost				
		Téměř nemožná	Výjimečně možná	Běžně možná	Pravděpodobná	Hraničící s jistotou
		1	2	3	4	5
Dopad	Nepřijatelný	A.1 A.2	F.2 F.4 G.7			
	Velmi významný			C.3 G.2	C.2	
	Významný	E.1 F.1	A.3 G.5	B.3 C.1 G.4		G.3 F.3
	Drobný		D.2 D.4 E.2	B.2 D.1	D.5 D.6	D.3
	Téměř neznamenný		G.6	B.1 G.1		E.3

Eliminace rizik

Na analýzu rizik navazují opatření, jejichž cílem je úplná eliminace potenciálních rizik nebo alespoň jejich minimalizace do podoby, která již projekt zásadně neovlivní a neohrozí jeho průběh. Taktika řízení rizik spočívá ve výběru nejvhodnějšího postupu pro zvládnutí příslušného rizika. Zvládnutí rizika spočívá obecně ve snižování jeho dopadu anebo jeho pravděpodobnosti výskytu. Pro kritická rizika se stanovují tzv. generické taktiky k jejich zvládnutí výběrem jedné z dále uvedených metod:

- **vyloučení rizika** – zákaz vybraných rizikových aktivit a procesů;
- **snížení rizika** – snížení velikosti dopadu např. pojištěním rizika;
- **přenos rizika** – redukce rizika snížením pravděpodobnosti nežádoucích událostí;
- **přijetí rizika** – akceptace rizika na stávající úrovni bez dalších aktivit.

Volba základní taktiky vychází z disponibilních možností, jakými vůbec lze v principu snížit dopad a pravděpodobnost konkrétního rizika.

Smyslem základních taktik je především uvědomění si základního směru (resp. možnosti) pro snižování významnosti rizika (tj. směru zamýšleného posunu pozice rizika v mapě rizik a to prostřednictvím snižování jeho pravděpodobnosti anebo dopadu s cílem posunout „pozici“ rizika v mapě rizik co nejvíce k počátku).

Pro eliminaci identifikovaných rizik byla vždy zvolena vhodná taktika zvládnutí rizika, která vedla ke stanovení konkrétního opatření. Tato opatření jsou specifikována v následující tabulce „Opatření navržená pro eliminaci rizik projektu“:

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Právní rizika		
A.1	Nedodržení právních norem ČR, EU.	Podrobná analýza legislativy a specifikace požadavků legislativy v úvodní fázi projektu.
A.2	Neschopnost udržet legislativní shodu systému nebo jeho částí	Průběžný monitoring změn legislativy v průběhu projektu a implementace změnového managementu.
A.3	Nevhodné smluvní podmínky, např. autorské právo, sankce, náhrada škody atd.	Návrh smluvních podmínek ze strany zadavatele a jejich ověření více právníky.
Finanční rizika		
B.1	Nedostatečné údaje pro vyhodnocení předpokladů návratnosti	Implementace metriky a systému pro vyhodnocování finančních dopadů projektu.
B.2	Navýšení cen technologií, služeb a prací a dalších vstupů.	Smluvní fixace cen za služby, standardizace technologií a otevřenost technologií, autorských práv a detailní dokumentace systémů.
B.3	Růst provozních nákladů v provozní fázi projektu.	Standardizace provozu, implementace systému řízení kvalitativní úrovně služeb provozu.

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Technická rizika		
C.1	Výběr nekvalitního dodavatele.	Při výběrových řízeních bude kladen důraz na kvalitu uchazečů (realizované projekty, reference od zákazníků apod.) a nabízenou cenu. Žadatel má bohaté zkušenosti s prováděním výběrových řízení.
C.2	Výběr nevhodné technologie.	Určení kvalitativních kritérií technologií a testování technologií před / v průběhu jejich obstarání.
C.3	Riziko související se zařízením (pře/poddimezovaná kapacita / výkon)	Dimenzování podle zátěžových testů, opce na zvýšení / snížení kapacit technologií.
Personální rizika		
D.1	Nedostatečná delegace kompetencí v projektovém týmu.	Uplatnění standardní metodiky řízení projektů a definování kompetencí v projektovém týmu.
D.2	Nedostatečný vnitřní kontrolní systém.	Implementace kontrolního systému s vnějším prvkem pro nezávislost kontroly.
D.3	Nedostatek kvalifikované a kvalitní pracovní síly v provozní fázi.	Zahrnutí získání know-how pracovníků spolu s ověřením jejich znalostí do realizační fáze projektu.
D.4	Fluktuace zaměstnanců zapojených do provozu projektu.	Uplatnění struktury znalostí v týmu s redundantním výskytem znalostí.
D.5	Závislost na specifických zaměstnancích / zaměstnancích dodavatele.	Kvalitní dokumentace s podrobným popisem všech částí systémů a infrastruktury, obstarání paralelního rámce pro poskytování služeb z vnějšího prostředí, rotace pracovníků více poskytovatelů.
D.6	Nedostatečné znalosti nebo potřeba specifického know-how.	Zmapování znalostní báze a identifikace mezer v znalostech, zavedení plánu transferu / obstarání specifického know-how.
Provozní rizika		
E.1	Neschopnost koordinace rozvoje systému v požadovaném čase a rozsahu	Standardizace provozu, implementace systému řízení kvalitativní úrovně služeb provozu včetně systému řízení změn.
E.2	Nenaplnění dodavatelských smluv v provozní fázi projektu.	Standardizace provozu, implementace kontrolních mechanismů a smluvní dohoda s náhradním poskytovatelem služeb.
E.3	Riziko spjaté s nastavením smluvního vztahu údržby a provozu systému (závislost na dodavateli)	Standardizace provozu, implementace kontrolních mechanismů a smluvní dohoda s náhradním poskytovatelem služeb.

Kód rizika	Riziko	Opatření vedoucí k eliminaci
Bezpečnostní rizika		
F.1	Krádež technologií nebo jejich poničení.	Zajištění maximální úrovně ostrahy jak z hlediska personálního zabezpečení, tak i moderních zabezpečovacích systémů. Umístění technologií do přiměřeného prostoru datacentera.
F.2	Teroristický útok (včetně kybernetického útoku).	Uplatnění metodiky / standardu pro řízení bezpečnostních rizik a řízení bezpečnosti. Technická opatření pro eliminaci útoků.
F.3	Bezpečnostní rizika	Uplatnění metodiky / standardu pro řízení bezpečnostních rizik a řízení bezpečnosti. Technická opatření pro zabezpečení dostupnosti, integrity a důvěrnosti dat.
F.4	Nedodržení povinností vyplývajících z legislativy, zejména zákona o ochraně utajovaných skutečností.	Postupování ve shodě se zákonem a příslušnými předpisy.
Projektová rizika		
G.1	Nedostatky v projektové dokumentaci.	Uplatnění standardní metodiky řízení projektů a kvalitativních kritérií na dokumentaci.
G.2	Neschopnost expertního zhodnocení kvality dodaných služeb (částkové přebírání výstupů dodavatele)	Definice kvalitativních úrovní, jejich oponentura třetí stranou a kontrola / audit jejich uplatnění v průběhu projektu.
G.3	Dodatečné změny v projektu.	Uplatnění standardní metodiky řízení projektů a změnového řízení.
G.4	Špatná koordinace dodavatelských prací.	Uplatnění standardní metodiky řízení projektů a kontrolních mechanismů postupu.
G.5	Zpochybnění validity projektu	Podpora prostřednictvím podporné komunikace s okolím projektu a příprava krizové komunikace - scénářů krizové komunikace.
G.6	Škody z nedostatečné soutěže anebo škody spojené s reputací na základě medializovaného zpochybnění nezávislého výběru dodavatele	Uplatnění principů transparentnosti a zákonných pravidel pro podporu soutěže v projektu nebo jeho částech.
G.7	Nedodržení termínu realizace.	Za dodržování termínu realizace (příp. etap) bude zodpovědný dodavatel, případně porušení sjednaného harmonogramu bude řešeno smluvní pokutou.

Projektové řízení a projektový tým

Pro realizaci Projektu EET je kladen velký důraz na úspěšné zvládnutí vhodných metod a nástrojů. Dobré a vžitě praktiky projektového řízení se opírají především o následující zdroje:

- Norma ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.
- Mezinárodní metodika Project Management Body of Knowledge.
- Metodiky, doporučení a Prince2.

Metodologie řízení projektu se skládá z následujících klíčových procesních oblastí, jež je nutné zásadním způsobem zvládat:

- Procesy vztahující se ke zdrojům.
- Procesy vztahující se k pracovníkům (řízení lidských zdrojů v rámci projektu).
- Procesy vztahující se k řízení vzájemných závislostí (řízení integrace projektu).
- Procesy vztahující se k záměru (řízení rozsahu prací projektu).
- Procesy vztahující se k časovým lhůtám (řízení času v rámci projektu).
- Procesy vztahující se k nákladům (řízení nákladů projektu).
- Procesy vztahující se ke komunikaci (řízení komunikace v rámci projektu).
- Procesy vztahující se k rizikům (řízení rizik projektu).
- Procesy vztahující se k nakupování (řízení obstarávání v rámci projektu).
- Procesy vztahující se ke zlepšování (řízení jakosti v rámci projektu).

Metodika řízení projektu je založena na definici organizace projektu a nastavení procesů projektového řízení. Metodika je navržena tak, aby poskytovala metodickou podporu a metodické nástroje pro:

- Řízení projektu tak, aby bylo efektivním způsobem dosaženo stanovených cílů projektu.
- Kontrolu plnění smluvních závazků a podmínek plynoucích ze Smluvních vztahů:
 - kvality, včasnosti a úplnosti plnění závazků smluvních stran,
 - identifikace případného neplnění smluvních závazků smluvními stranami,
 - identifikace zřejmých, jednoznačných a rychle aplikovatelných termínovaných postupů vedoucích k odstranění překážek plnění Smluvních závazků a k případné reflexi těchto postupů do znění Smluvní dokumentace.

Koncepce metodiky řízení projektu včetně organizace projektu vychází z následující základních prosazovaných zásad:

- **Racionálně navržená struktura orgánů řízení projektu**

Organizační struktura projektu zahrnuje pouze nutné řídicí orgány, jejichž struktura je minimalizována tak, aby mohly řádně plnit jim svěřené řídicí funkce. Struktura řídicích orgánů je navržena hierarchicky tak, aby se na příslušné úrovni řízení projektu nakládalo pouze s adekvátními a na nižších úrovních dostatečně předpracovanými informacemi a tak, aby probíhaly pouze řídicí činnosti, které jsou adekvátní dané úrovni řízení.

- **Racionálně navržené rozhodovací procesy**

Rozhodovací procesy jsou navrženy takovým způsobem, aby byl minimalizován počet nutných kroků vedoucích ke konečnému rozhodování, ovšem při zachování kvality rozhodovacího procesu. V rámci rozhodovacích procesů je uplatněna zásada individuální rozhodovací odpovědnosti a zásada „rozhoduje jeden“ (ať již ve smyslu řídicího orgánu jako celku, tak jednotlivých účastníků projektu).

• Prosazování cílené adresné odpovědnosti

V rámci projektu je jednoznačně určena odpovědnost jednotlivých účastníků. Jednotlivé úkoly jsou předávány k řešení těm účastníkům projektu, kteří mají předpoklady a potřebné zdroje k jejich vykonání. Provádění jednotlivých činností (plnění úkolů včetně kvality plnění) je důsledně sledováno.

• Zajištění účelnosti a efektivity metodiky řízení projektu

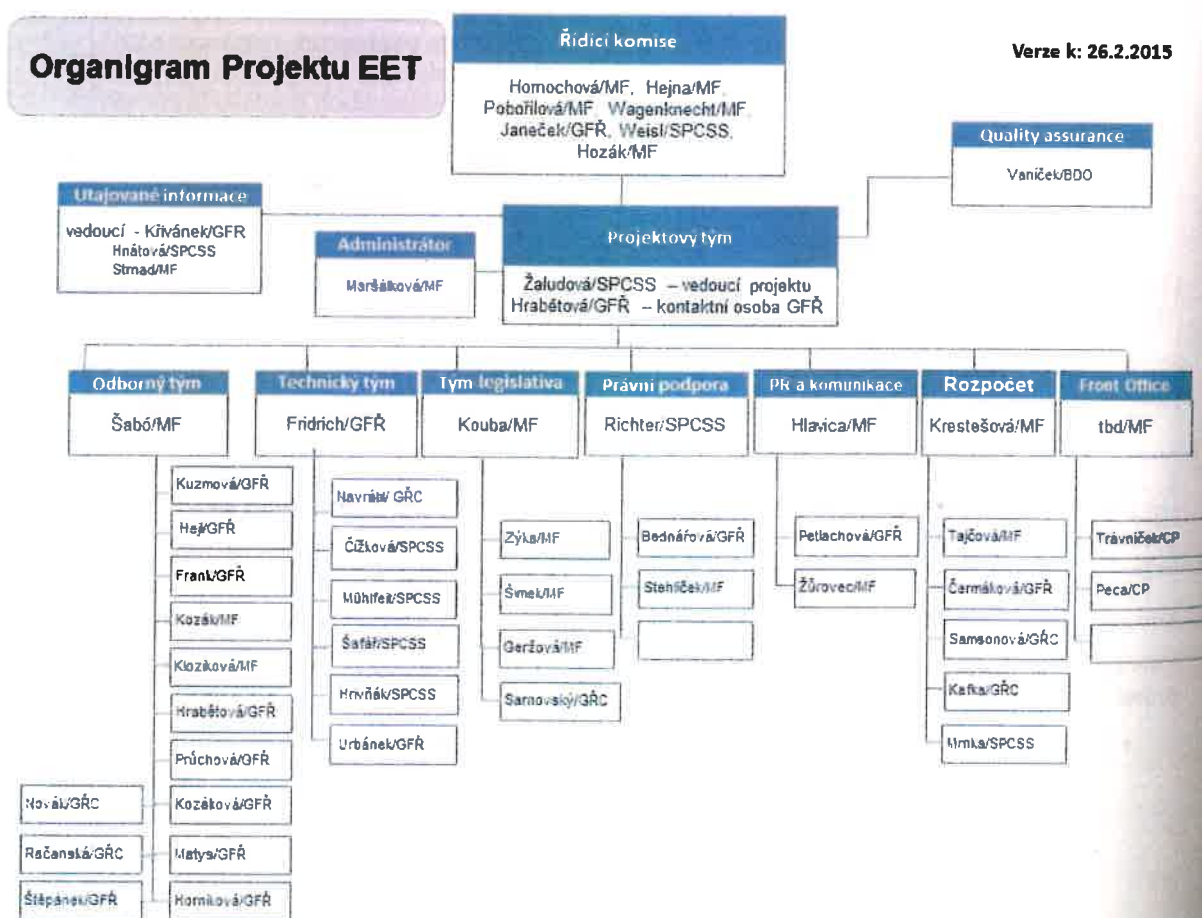
Metodika řízení projektu není chápána staticky. V průběhu projektu, se může částečně měnit, a to vždy tak, aby vždy odpovídala aktuálnímu stavu projektu a byla účinná a efektivní při řešení aktuálních potřeb projektu včetně těch, které mohou plynout ze změny priorit projektového řízení. Soulad aktuální podoby metodiky se stavem a potřebami projektu je průběžně sledován.

Organizace Projektu

V této kapitole jsou popsány **orgány** Projektu EET z hlediska jejich **struktury a vzájemných vazeb**.

Orgány projektu

Organizační struktura Projektu EET je **graficky znázorněna** na schématu níže.



Obrázek 45: Organizační struktura projektu

Řídící komise a sponzor Projektu

Sponzor Projektu EET

Sponzorem projektu je statutární zástupce organizace, který je vybaven rozhodovací pravomocí a bude se zasazovat za realizaci projektu. Sponzor projektu především rozhoduje o způsobu financování projektu, provádí strategická rozhodnutí, která mají vliv na směřování projektu a řeší případné spory a problémy, které se nepodaří vyřešit na nižších úrovních. Sponzor projektu odpovídá především za:

- Oficiální zaštitění celého projektu.
- Řešení velkých změn projektu.
- Schvaluje výstupy projektu.

Sponzorem projektu je Ministr financí ČR.

Řídící komise

Řídící komise projektu (ŘK) má celkem **sedm členů**, předsedou komise je statutární zástupce GŘC. Jeho členy jsou zaměstnanci nejvyššího vedení MFČR a GŘC:

- Simona Hornochová
- Miroslav Hejna
- Michaela Pobořilová
- Lukáš Wagenknecht
- Martin Janeček (předseda)
- Hanuš Weisl
- Roman Hozák

Mezi hlavní úkoly ŘK patří především:

- Schvalování hlavních výstupů Projektu EET, tj. zejména Základní listiny Projektu EET, apod.
- Projednávání aktuálního stavu hlavních aktivit Projektu EET a přijímání případných zásadních rozhodnutí týkajících se Projektu, zejména schvalování podstatných změn.
- Řešení rizik a přijímání opatření k jejich eliminaci, respektive odstranění.
- Schvalování personálních změn projektového týmu a řešitelských týmů.

Řídící komise se bude v plném složení scházet minimálně **jednou za měsíc**, v případě potřeby častěji. Jednání ŘK se bude za účelem informování o aktuálním stavu Projektu účastnit rovněž projektový manažer. Projektový manažer nebude mít hlasovací právo. Konkrétní mechanismy jednání a schvalování na úrovni ŘK budou upraveny v Základní listině Projektu EET.

Seznam projektových rolí a jejich základní specifikace:

Role	Specifikace role
Zainteresovaná smluvní strana projektu	Zainteresovanou smluvní stranou se rozumí subjekt, který je v projektu přímo zastoupen a nějakým způsobem projekt přímo ovlivňuje. V tomto případě MFČR, GŘC, GŘC, SPCSS.
Člen řídicí komise	Člen řídicí komise odpovídá spolu s ostatními členy řídicí komise za dohled nad plněním celkového rámce projektu, zejména dohleduje projektové vedení. Člen řídicí komise se podílí na rozhodování zásadních otázek a stavů projektu, které jsou mu k rozhodnutí předkládány z úrovně vedení projektu. Člen řídicí komise plní úkoly uložené mu rozhodnutím řídicí komise.

Vedoucí projektu/ projektového týmu	Vedoucí projektu odpovídá za vedení jemu podřízeného projektového týmu, zejména zadává úkoly a sleduje jejich plnění. Vedoucí projektu je hlavní odpovědnou osobou za projekt a je současně hlavní kontaktní osobou zajišťující komunikaci s ostatními řešitelskými projektovými týmy a řídicí komisí.
Kontaktní osoba projektového týmu	Kontaktní osoba projektového týmu je hlavní odpovědnou osobou za projekt za danou zainteresovanou smluvní stranu. Zajišťuje komunikaci za svou smluvní stranu napříč mezi všemi projektovými týmy.
Členové projektového týmu	Členové projektového týmu jsou vedoucí jednotlivých řešitelských týmů a administrátor projektu. Předkládají projektovému vedoucímu výstupy za své řešitelské týmy. Jedná se o výkonnou složku projektu.
Administrátor projektu	Administrátor projektu zajišťuje některé běžné agendy projektu (např. zápisy z jednání řídicí komise, zápisy z jednání projektového týmu, atp.) a zprostředkovává a zastřešuje další organizační požadavky plynoucí z projektového týmu.
Vedoucí řešitelského projektového týmu	Vedoucí řešitelského projektového týmu je zodpovědný za vedení jeho týmu. Organizuje schůzky svého týmu, zadává úkoly členům svého týmu, kontroluje plnění těchto úkolů, předkládá a zodpovídá za výstupy svého týmu směrem k projektovému vedoucímu. Každý vedoucí řešitelského týmu má povinnost delegovat svého zástupce, v případě nutnosti zastoupení při jednáních projektového týmu.
Člen řešitelského projektového	Člen řešitelského projektového týmu řádně a včas plní úkoly uložené nadřízeným vedoucím odborného týmu nebo jím pověřenou osobou. Každý člen řešitelského projektového týmu je zejména povinen neprodleně informovat nadřízeného vedoucího, nebo vedoucího projektu o skutečnostech, které mohou ohrozit projekt či naopak napomoci jeho realizaci.

Kompetence jednotlivých projektových týmů

Řídicí komise Projektu EET (dále také „ŘKO“)

Řídicí komise Projektu EET (dále jen ŘKO) je vrcholový řídicí orgán Projektu EET, který rozhoduje o zásadních otázkách ovlivňujících směr a průběh realizace Projektu EET.

Člen ŘKO musí být vybaven potřebnými kompetencemi rozhodovat v zásadních otázkách Projektu EET, musí mít možnost alokovat potřebné projektové zdroje a musí mít možnost prosadit rozhodnutí v rámci příslušné smluvní strany.

Řídicí komise Projektu je složena ze zástupců MFČR, GŘŘ a SPCSS.

Na jednání ŘKO mohou být na žádost zástupců MFČR, GŘŘ či zástupců SPCSS přizváni s poradním hlasem další externí odborníci nebo zástupci dalších stran participujících na realizaci Projektu.

ŘKO se schází dle potřeby tak, aby byla zabezpečena dostatečná kvalita sledování Projektu. V případě nutnosti rychlého a zásadního rozhodnutí se Řídicí komise Projektu sejde v prvním možném termínu na vyžádání kterýmkoliv jejím stálým členem.

ŘKO svolává vedoucí projektu, pokud není domluveno jinak.

Kompetence ŘKO:

- Jmenuje členy ostatních týmů na návrh vedoucího projektu.
- Informuje vedení Ministerstva financí ČR o průběhu projektu; kontroluje stav a průběh projektu a vydává rozhodnutí za účelem podpory plnění cílů projektu.
- Rozhoduje o návrhu na změnu projektu (rozsah plnění, harmonogram, cena) včetně případných změn smlouvy.
- Řeší krizové situace projektu a rozhoduje o mimořádných opatřeních k jejich odstranění.

- Potvrzuje jednotlivá plnění projektu a schvaluje zahájení a ukončení projektu.
- Řídí a schvaluje součinnosti, které budou poskytnuty v rámci projektu (včetně třetích stran).
- Je eskalačním orgánem, který řeší případné spory, jež se nepodařilo vyřešit v rámci ostatních projektových týmů.

Quality assurance (QA)

Garant kvality dohlíží na všechny procesy, od návrhu, realizaci až po dokumentaci projektu. Cílem QA je dohlédnout na procesy projektu, tak aby byl projekt dokončen dle zadání a v požadovaném čase a kvalitě. Garant kvality (z BDO) je nominován dočasně a to do 27.2. 2015.

Projektový tým (PT)

Projektový tým, řeší aktuální problémy při přípravě a provozu Služeb, koordinuje činnost řešitelských týmů, které se podílejí na přípravě a realizaci služeb.

PT projednává a předkládá návrhy na optimalizaci a změnu, zpracovává zprávy o průběhu Projektu, identifikuje možná rizika, iniciuje jednání na mitigaci rizik.

PT schvaluje dokumenty, jež jsou součástí plnění, schvaluje dílčí harmonogramy jednotlivých etap Projektu.

Tým je složen ze zástupců SPCSS, MFČR a GŘŘ a případně zástupců třetích stran.

Kompetence Projektového týmu

- Definuje a hodnotí požadavky na systém EET, určuje priority ve spolupráci s ostatními týmy.
- Předkládá výstupy Řídící komisi.
- Řídí a monitoruje kvalitu v průběhu všech etap projektu.
- Připravuje a projednává návrhy postupů k mitigaci rizik.
- Odpovídá za vedení aktuálního Registru rizik.
- Předkládá podklady Řídící komisi a poradě vedení (ZPV)

Odborný tým (OT)

Kompetence Odborného týmu:

- Specifikuje zadání - věcný popis fungování systému elektronické evidence tržeb z hlediska povinných subjektů a z hlediska správce daně, včetně souvisejících kontrolních postupů a udělování sankcí.
- Navrhuje a upravuje procesní postupy ve vztahu k zavedení EET ve spolupráci s ostatními týmy.
- Provádí věcné hodnocení vůči Chorvatskému modelu. Komunikuje s odbornými subjekty ze zahraničí.
- Spolupracuje také s ostatními týmy, zejména s týmem legislativy a technickým týmem, s týmem PR komunikuje propagační stránku projektu.
- Podílí se na vytvoření zadávací dokumentace pro projekt EET.
- Zodpovídá za formální i obsahovou správnost specifikace zadání

Technický tým (TT)

Kompetence Technického týmu:

- Vytváří funkční a technickou specifikaci pro zadání projektu EET.

- Provádí sběr požadavků od odborného a legislativního týmu a převádí věcné požadavky do technického řešení.
- Formalizuje požadavky a komunikuje požadavky s ostatními týmy.
- Připravuje návrh technického řešení EET.
- Připravuje podklady pro zadávací dokumentaci projektu EET.
- Zodpovídá za správnost vytvořené funkční a technické specifikace

Tým legislativa (TL)

Kompetence Týmu legislativa:

- Odpovídá za přenesení věcného řešení do legislativního textu, tj. při požadavku na regulaci, tým zváží, zda je ji třeba provádět zákonem, vyhláškou či postačí řešení v rovině metodické či správní. Pokud bude daný požadavek regulován zákonem či vyhláškou, pak je odpovědný za formulaci daného ustanovení do předmětného právního předpisu.
- Vyhodnocuje požadavky ostatních týmů zejména s ohledem na nutnost regulace zákonem, vyhláškou atd.
- Navrhuje formulace ustanovení zákona.
- Odpovídá za realizaci legislativního procesu přípravy zákona o EET, tj. realizace připomínkových řízení a procesů v rámci vlády a Parlamentu České republiky (tj. zajištění potřebné součinnosti ze strany předkladatele)
- Vede harmonogram legislativního procesu
- Zodpovídá za legislativní zachycení věcného řešení.

Tým právní a administrativní podpora (PP)

Kompetence Týmu právní a administrativní podpora:

- Právní a administrativní podpora projektu, tj. organizuje přípravu pro zadání veřejných zakázek na realizaci EET včetně vedení dokumentace.
- Podílí se na vytvoření zadávací dokumentace pro projekt.
- Připravuje a vede harmonogram zadání veřejných zakázek.
- Komunikuje s dotčenými orgány (ÚOHS ...).
- Zodpovídá za smluvní zajištění systému EET ve všech fázích projektu

Tým PR a komunikace (PR)

Kompetence Týmu PR a komunikace:

- Příprava strategického plánu komunikace, segmentace cílové skupiny, volba nástrojů, precizace hlavních sdělení, časový plán
- Příprava obsahu kampaně (název projektu, Corporate identity projektu, argumentář, tonalita sdělení)
- Sběr mediálně důležitých témat a informací z jednání týmů.
- Hodnotí získané informace z hlediska nutné komunikace směrem k veřejnosti či jiným zájmovým skupinám.
- Zpracovává manuál krizové dokumentace.
- Provádí analýzu mediálního obsahu.
- Navrhuje témata, která je nutné sdílet. Navrhuje postupy sdílení.
- Podporuje klíčové zaměstnance MFČR při prezentacích EET a veřejném vystupování

- Zodpovídá za komunikaci s médii a třetími stranami na podporu v médiích (on-line komunikace včetně zvláštní webové stránky)

Tým Rozpočet/controlling (RO)

Kompetence Týmu Rozpočet a controlling:

- Nastavuje a řídí rozpočet projektu a kontroluje jeho plnění ve 2 rovinách (rozpočet a controlling)
- Plánování zdrojů a řízení nákladů projektu (rozpočet)
- Příprava podkladů pro plánování zdrojů, rozpočtu a řízení nákladů projektu,
- Plánování zdrojů - určování, jaké zdroje (pracovníci, vybavení) a v jakých množstvích by měly být použity pro provedení projektových a provozních činností.
- Odhadování nákladů - stanovení přibližných nákladů potřebných k dokončení projektových a provozních činností.
- Rozpočtování nákladů – zpracování a rozdělování celkových odhadovaných nákladů mezi jednotlivé etapy projektu a provozu.
- Operativní řízení nákladů - operativní řízení změn rozpočtu projektu.
- Návrh, nastavení a zavedení systému controllingu projektu v za účelem pravidelného informování o stavu čerpání a rezerv finančních a dalších prostředků,
- Pravidelné zpracovávání výkazů čerpání rozpočtu a porovnání plánu a skutečnosti.
- Zodpovídá za řádné plnění rozpočtu

Tým Front Office (FO)

Kompetence Týmu Front Office:

- Komunikuje se zástupci a Ministerstva vnitra (ISDS, Czechpoint) a České pošty za účelem přípravy a realizace obslužných procesů EET prostřednictvím služeb ISDS (datové schránky) a kontaktních míst České pošty a Czechpoint.
- Zodpovídá za řádné a včasné zajištění procesů EET spojených s obsluhou povinných subjektů na kontaktních místech (FÚ, Česká pošta, Czech point) a prostřednictvím ISDS.

Tým Utajované informace (UI)

Tým Utajované informace (UI) je složen z bezpečnostních ředitelů GFŘ a SPCSS a zástupce ředitele Odboru Bezpečnost a krizové řízení MFČR.

Kompetence Týmu Utajované informace:

- Komunikuje ve spolupráci s právním týmem s dotčenými orgány (NBÚ).
- Zodpovídá za realizaci veškeré agendy spojené s nakládáním se stávajícími utajovanými informacemi v rámci projektu EET i s těmi co vzniknou v průběhu realizace, jakož i dalšími bezpečnostními aspekty EET.
- Vede seznam poskytnutých utajovaných informací (utajovaných dokumentů), které v rámci projektu EET vznikly.
- Vede seznam pracovníků (členů projektových týmů) s přístupem k předmětným utajovaným informacím a provádí jejich poučení.
- Kontroluje nakládání s utajovanými informacemi v rámci projektu EET.

Řízení Projektu

Následující kapitoly popisují hlavní principy řízení Projektu. Detailní a aktuální specifikace řízení Projektu EET bude uvedena v **Základní listině Projektu**, která bude zpracována bezprostředně po schválení tohoto dokumentu.

Základní listina Projektu bude jasně **definovat aktivity řízení a implementace** Projektu EET, odpovědnosti a termíny plnění. Za zpracování Základní listiny Projektu a její případné změny odpovídá projektový manažer a schvaluje ji Řídící komise Projektu.

Základem metodiky řízení projektu je vyvážený a vzájemně provázaný systém procesů a postupů, jehož cílem je efektivní dosažení stanovených cílů v plánovaném rozsahu a s využitím plánovaných zdrojů. Tento systém zahrnuje následující procesní okruhy popsané dále v následujících podkapitolách:

- Řízení rizik.
- Řízení dodavatelů.
- Řízení změn.
- Kontrolu postupu projektu.
- Řízení problémů.
- Akceptační postupy.
- Komunikační strategie.
- Řízení kvality.
- Správa dokumentace.

Řízení rizik

- Hlavní **odpovědnost za řízení rizik** (monitorování a realizaci opatření k eliminaci / odstranění rizika) nese projektový manažer (PM).
- **Nástrojem pro řízení rizik** je Katalog rizik. Rizika uvedená v Katalogu budou předmětem monitorování a řízení na úrovni projektového týmu, respektive řešitelského týmu, který odpovídá za jeho eliminaci / odstranění.
- Za **identifikaci** případných dalších rizik Projektu EET jsou odpovědni všichni členové řešitelských týmů. O identifikovaném riziku, včetně návrhu nápravného opatření, je každý člen povinen informovat příslušného vedoucího týmu.
- Vedoucí řešitelského týmu **ohodnotí riziko** z hlediska jeho významnosti (tj. pravděpodobnost a dopad) a schválí navržené nápravné opatření. Pokud jde o riziko střední / vysoké významnosti, eskaluje jej na PM, který jej zařadí na nejbližší jednání projektového týmu.
- Projektový tým nově **identifikovaná rizika**, jejich významnost a návrh opatření projedná a rozhodne o začlenění do Katalogu rizik. Každému novému riziku PT následně přidělí osobu odpovědnou za sledování rizika a realizaci nápravného opatření. Nápravná opatření ve formě nepodstatných změn schvaluje PM, ve formě podstatných změn pak ŘK.
- Monitorování a řízení rizik je vždy **předmětem jednání ŘK**.

Řízení dodavatelů

- Za řízení dodavatelů odpovídá vedoucí projektového týmu. Na přípravě veřejných zakázek se budou podílet jednotlivé řešitelské týmy, každý za svojí oblast. Odpovědnost zahrnuje nastavení a kontrolu smluvních vztahů.
- Odpovědnost za **řízení změn** v rámci Projektu EET nese projektový manažer (PM).
- „**Podstatné**“ změny v Projektu na základě návrhu PM schvaluje ŘK. „**Nepodstatné**“ změny v projektu schvaluje PM a informuje na nejbližším jednání ŘK.

Řízení problémů

Cílem řízení problémů je včasná identifikace a řízené řešení faktorů (problémů), které ohrožují úspěšné dosažení cílů projektu (zejména pak lokálně jeho řádný průběh).

Na rozdíl od změny, která je řízenou (byť dodatečnou) změnou předmětu projektu či způsobu jeho realizace, může být problémem jakákoli skutečnost související s projektem, která má na jeho průběh a výsledek negativní vliv menšího i většího rozsahu.

Řešení problémů probíhá primárně uvnitř projektových týmů v pravomoci příslušného vedoucího řešitelského týmu. Vedoucí řešitelského týmu informují o problémech svého vedoucího řešitelského týmu a jejich řešení ostatní členy vedení řešitelského týmu. V případě zásadních problémů, které přesahují pravomoci vedení řešitelského týmu jsou tyto přenášeny na vedení projektového týmu a případně až na ŘK projektu.

Řešení některých problémů může vyústit do požadavku na změnu.

Identifikace problému

Kdokoliv z projektového týmu projektu může identifikovat problém. V tomto případě zašle hlášení problému (popis problému, jeho příčin, dopadů a možných řešení) elektronickou cestou nadřízenému vedoucímu řešitelského týmu.

Příslušný vedoucí řešitelského týmu potvrdí ohlašovateli elektronickou cestou přijetí hlášení problému.

Rozhodnutí o řešení problému

Vedoucí řešitelského týmu posoudí přijatý problém a je-li to třeba k řešení, konzultuje jej s vedením projektového týmu. Vyžaduje-li to situace, může být problém spolu s návrhy řešení a dalšími relevantními podklady předán vedení projektu případně následně řídicí radě projektu. Následně rozhodne o způsobu řešení problému jedním z následujících způsobů:

- **Odložení problému:** neshledá-li potřebu řešit hlášený problém, pak jej uzavře.
- **Operativní řešení problému:** rozhodne-li o operativním řešení problému, pak stanoví způsob řešení včetně předpokládaných termínů a zdrojů a pověří příslušné členy řešitelského týmu úkoly a sleduje jejich plnění. Po operativním vyřešení problému uzavře tento problém s tím, že o uzavření informuje vedení projektového týmu a případně ŘK (jestliže došlo k eskalaci problému na dané úrovni).
- **Návrh na změnu:** shledá-li potřebu řešit problém formou změnového požadavku, pak připraví příslušný změnový požadavek.

Řešení problému

Problémy vedení řešitelských týmů a vedení projektového týmu sleduje nejméně s týdenní periodicitou a podle potřeby přijímá příslušná opatření. Informace o problémech a jejich řešení jsou dle závažnosti a úrovně eskalace zaznamenávány v rámci zápisů z jednání řešitelských týmů, vedení projektového týmu a ŘK.

Principy akceptace

- Akceptační řízení je činnost, která začíná protokolárním **předáním předmětu dílčího** plnění (etapy, fáze) a během které vedoucí projektového týmu a jednotlivými dodavateli ověřují, zda předaný předmět plnění odpovídá smluvním vztahům, a to prostřednictvím akceptačních kritérií a v dohodnutých lhůtách.
- Akceptační protokoly – v souladu s odevzdanými výstupy dodavatelů zajišťují vedoucí řešitelských týmů jejich vypracování a podepsání dotčenými stranami.

Reporting a monitoring

- Za průběžný monitoring Projektu na úrovni jednotlivých řešitelských týmu odpovídá **příslušný vedoucí**. Za monitoring na úrovni celého Projektu odpovídá projektový manažer. Aktuální stav realizovaných aktivit je předmětem pravidelných jednání projektového týmu. Projektový manažer pravidelně informuje o stavu Projektu ŘK.
- Etapové a **závěrečná monitorovací zpráva** – předkládá se poskytovateli po ukončení etap, respektive celkovém ukončení Projektu EET. Za zpracování zpráv odpovídá projektovému manažer, který zprávu předloží ke schválení ŘK. Po schválení je zpráva předána k podpisu statutárnímu zástupci.
- Všichni členové týmu budou povinni zpracovávat měsíční **pracovní výkazy**, které budou specifikovat počet hodin účelně strávených na realizaci Projektu (v souladu s popisem práce na Projektu) a realizovanou aktivitu. Výkaz práce je schvalován nadřízeným člena týmu.
- **Za řízení rozpočtu** Projektu a jeho aktuální čerpání odpovídá vedoucí řešitelského rozpočtu a controlling. Řízení rozpočtu je předmětem jednání na úrovni projektového týmu. Změny rozpočtu schvaluje vždy projektový manažer. Tzv. podstatné změny rozpočtu musí být schváleny ŘK.

Komunikace v rámci projektu

Řídící komise

- Řídící komise Projektu se schází **minimálně jednou za měsíc**, v případě potřeby častěji. Na prvním jednání ŘK si členové zvolí předsedu.
- Jednání ŘK svolává **předseda ŘK** na podnět PM minimálně 1x za měsíc, respektive v případě eskalovaného problému. Agendu připravuje a zápis pořizuje PM Projektu EET.
- ŘK je **pravidelně informován** o aktuálním stavu a dalším vývoji v Projektu EET.
- V případě rozhodování hlasováním rozhoduje **prostá většina** hlasů, sponzor má právo veta, PM má hlas pouze poradní. Pro účely hlasování musí být přítomni členové ŘK, nebo jimi určení náhradníci. Pro zefektivnění realizace Projektu EET Základní listina Projektu dále specifikuje případy, kdy je možné hlasování / schvalování „per rollam“.
- Ze všech jednání ŘK jsou pořizovány **písemné zápisy**, které jsou archivovány v souladu s pravidly archivace.

Projektový tým

- Projektový tým se schází zpravidla **jednou za týden**, v případě potřeby častěji. Nastavení frekvence jednání bude předmětem úpravy v Základní listině Projektu.
- Jednání týmu **svolává PM**, agendu připravuje asistent PM.
- Účelem jednání projektového týmu je **zejména monitoring** stavu Projektu EET, **koordinace prací a činností řešitelských týmů**, řízení rizik, koordinace s ostatními projekty, které mají vazbu na Projekt EET, řízení změn apod.
- Ze všech jednání projektového týmu pořizuje asistent PM písemné zápisy, které jsou archivovány v souladu s pravidly archivace.

Řešitelské týmy

- Řešitelské týmy se schází zpravidla **jednou za týden**, v případě potřeby častěji. Nastavení frekvence jednání bude předmětem úpravy v Základní listině Projektu.
- Jednání týmu svolávají příslušní vedoucí řešitelských týmů.
- Účelem jednání řešitelského týmu je zejména **monitoring stavu Projektu** na úrovni týmu, **koordinace prací a činností** v rámci týmu, monitoring dodavatelských vztahů, řízení rizik, koordinace s ostatními řešitelskými týmy, apod.
- Ze všech jednání řešitelského týmu jsou pořizovány **písemné zápisy**, které jsou archivovány v souladu s pravidly archivace.

Schvalování výstupů

- ŘK schvaluje **změny v projektovém týmu**, podstatné změny v Projektu EET a monitorovací zprávy.
- PM **schvaluje výstupy** Projektu EET na úrovni projektového týmu (tzn. akceptační kritéria dílčích etap, akceptační protokoly z řešitelských týmů, nepodstatné změny v Projektu EET, návrhy podstatných změn v Projektu EET).
- Vedoucí řešitelských týmů schvalují **výstupy dodavatelů** dodané v rámci jimi věcně řízené oblasti.

Řízení kvality

Principy řízení kvality

Zajištění kvality jednotlivých klíčových výstupů projektu a projektu samotného patří mezi povinnosti vedoucích řešitelských týmů a je dohledováno manažerem kvality projektu z hlediska dodržování metodiky řízení projektu a souladu se smluvním rámcem stanoveným smlouvou o dílo. Zajišťování kvality výstupů projektu vychází ze dvou principů:

- **Zdokonalování kvality projektových postupů.**
- **Kontroly kvality klíčových výstupů projektu.**

PM společně s manažerem kvality vypracovávají plán zajišťování kvality projektu. Mezi nástroje k zajištění kontroly kvality patří:

- Osvědčený projektový postup, jehož použití je na závěr projektu (a případně i v jeho průběhu) posuzováno a který je soustavně zdokonalován.
- Pokud na úkolu pracuje více zdrojů, je stanoveno, který z nich za splnění úkolu zodpovídá a role/úloha ostatních zdrojů.
- Projektový postup obsahuje na závěr jednotlivých kroků úkoly spočívající v posouzení zpracovaných výstupů, přičemž podle možností jsou k těmto úkolům přiřazeny zdroje, které nezpracovávaly posuzované výstupy.
- Vytvoření katalogu požadavků na systém a ověření, že splnění těchto požadavků je ověřitelné.
- Zapojení uživatelů do kontroly kvality (posuzování návrhů uživatelského rozhraní, akceptační testování).
- Provedená posouzení kvality produktů jsou dokumentována (kdo kontroloval, co kontroloval, s jakým výsledkem).
- Produkty, u kterých byly zjištěny nedostatky, jsou zadány k úpravě a odstranění a těchto nedostatků je kontrolováno.
- Určování příčin zjištěných chyb a zapracování preventivních činností do projektového postupu.
- Při zadání úkolu jen vždy specifikován požadovaný výstup a kritéria pro posouzení jeho kvality, specifikaci kritérií kvality stanovuje PM nebo jím pověřený zdroj (zejména o produktech výkonné části projektu).
- Před zahájením testování je zpracovávána specifikace testovacích případů pro jednotlivé úrovně testování.

Kontroly kvality

V rámci řízení kvality se uplatňují vedle sebe pravidelné (povinné) a nepravidelné (nepovinné) kontroly kvality.

Pravidelné kontroly

Pravidelné kontroly jsou prováděny v následujících termínech a rozsahu dle stanoveného schématu:

Dodržování projektového plánu	
Metoda:	Monitorování a sledování Plánu projektu. Informování o stavu projektu včetně hlášení výrazných projektových odchylek.
Odpovídá:	PM.
Četnost:	Kontinuálně, formálně minimálně jedenkrát týdně.
Cíl:	Dodržet všechny plánované milníky realizace.

Shoda výstupů se specifikací	
Metoda:	Ověření, zda výstup splňuje všechna kvalitativní a kvantitativní akceptační kritéria formou akceptace či dílčí kontroly.
Odpovídá:	PT a subjekty definované v Akceptačních kritériích.
Četnost:	Při akceptačním řízení.
Cíl:	Dodržet kritéria kvality realizace Projektu.

Projektová dokumentace	
Metoda:	Ověřit kompletnost projektové dokumentace dle požadavků Metodiky.
Odpovídá:	PT.
Četnost:	Průběžně minimálně jedenkrát týdně a při ukončení hlavních částí projektu.
Cíl:	Zajistit auditovatelnost realizace projektu.

Nepravidelné kontroly

Nepravidelné kontroly mohou být provedeny podle potřeby kdykoliv v průběhu projektu. Provedení kontroly iniciují PM nebo ŘK. Kontrolu kvality dokumentace, průběhu realizace a výstupů projektu provádí určený PM ve spolupráci s manažerem kvality projektu nebo manažer kvality sám a dle potřeby se účastní kterýkoliv účastník projektu. Pokud jsou při kontrole kvality shledány nedostatky, stanoví se přiměřené lhůty k jejich odstranění. Za odstranění těchto nedostatků odpovídá určení PM.

- **Kontrola vedení projektu**
Formální kontrola, které se účastní zástupci liniového řízení MFČR, GŘŘ, GŘC, SPCSS (včetně např. zástupců příslušných organizačních jednotek). Provedení kontroly je vedeno PM, výsledky kontroly jsou schváleny ŘK.
- **Kontrola Vedoucích řešitelských týmů**
Kontrola kvality, prováděná manažerem kvality.
- **Kontrola člena týmu**
Kontroly kvality na úrovni řešitelských týmů jsou prováděny formou pracovních jednání/workshopů či tzv. distribučním způsobem. Při těchto kontrolách, zpracovávají připomínky k předloženým výstupům ostatní členové PT, s odpovídajícími zkušenostmi a dovednostmi ve vztahu k revidovanému výstupu.
- **Kontrola sebe sama**
Autor a/nebo vlastník výstupu sám provádí kontrolu výsledků své práce, v průběhu realizace i před předáním.

Ověřování požadavků a návrhu

Součástí procedur zajištění kvality je také prosazování řádného ověřování požadavků a návrhu, jehož cílem je omezení projektových rizik, která plynou z realizace částí projektu na základě chybných či neúplných vstupních požadavků nebo na základě návrhu, který by stanovené požadavky nerespektoval.

Veškeré požadavky musí vycházet z primárních požadavků definovaných v základním dokumentu projektu s tím, že je pouze vhodně upřesňují či doplňují, musí být specifikovány a odsouhlaseny kvalifikovanými subjekty a dále prověřeny. Tento cíl je zajištěn řízeným procesem konzultací / interview aplikací následujících kroků:

- PM stanoví požadavky a strukturu konzultací / interview, zvolí vhodné osoby pro jednotlivé konzultace / interview (respondenty) a naplánuje konzultace / interview.
- Určení pracovníci provedou dle plánu jednotlivé konzultace / interview a zdokumentují je v podobě záznamů typu Zpráva / Zápis z jednání / Zápis interview, které jsou potvrzeny jednotlivými respondenty a prověřeny PM, případně dalšími jím určenými osobami.
- Je-li třeba, jsou po dohodě provedeny další doplňující konzultace / interview.

Veškeré návrhy částí díla musí vycházet z požadavků Smlouvy a z požadavků získaných v rámci konzultací / interview tak, aby splňovaly příslušné záměry projektu. Tohoto cíle je dosaženo řízeným procesem přípravy návrhu, v rámci kterého:

- Dodavatel musí písemně předkládat PT veškeré nové nebo zpřesňující návrhy řešení.
- PT musí zajistit řádné připomínkové řízení předložených návrhů a předat připomínky k zapracování.
- Po zapracování všech připomínek musí být návrh schválen na úrovni PT (případně na vyšší úrovni projektového týmu vyžaduje-li to jeho povaha).

Ověřování výstupů projektu

Cílem ověřování výstupů projektu je zajistit předání díla jak v jednotlivých částech tak vcelku v podobě a kvalitě, která je plně v souladu s požadavky základního dokumentu projektu a s požadavky a návrhy specifikovanými a odsouhlasenými v průběhu projektu.

Správa a dokumentace projektu

V této části Metodiky řízení projektu stanoví základní pravidla nakládání a správy dokumentace projektu.

Kategorie dokumentace

Dokumentace projektu je členěna na následně vymezené kategorie:

- **Řízená dokumentace projektu:**
Řízenou dokumentací projektu je veškerá dokumentace vyžadovaná smluvní dokumentací nebo metodikou řízení projektu, dokumentace sledovaná na úrovni vedoucích ŘT případně další dokumentace určená na úrovni PT. Jedná se nejen o výstupy projektu, ale také o důležitou podkladovou dokumentaci.
- **Pracovní dokumentace projektu:**
Pracovní dokumentací projektu je veškerá dokumentace či materiály zpracováváné účastníky projektu v rámci jim přidělených úkolů či přímo sloužící k plnění těchto úkolů včetně dokumentace jako jsou podklady.
- **Specifická dokumentace projektu:**
Specifickou dokumentací projektu je veškerá dokumentace či materiály zpracováváné v rámci projektu, se kterými, vzhledem k jejich charakteru, nelze nakládat výše uvedeným způsobem. Jedná se zejména o databáze, vytvářený programový kód a konfigurace.

Značení dokumentace

Pravidla značení dokumentace se vztahují na řízenou dokumentaci projektu s tím, že by měla být dodržována také pro zbývající typy dokumentace tam, kde je to možné. Značení (identifikace) jednotlivých dokumentů má základní strukturu **Identifikátor_Verze.Pripona**, kde jednotlivé části identifikace mají následující význam:

- **Identifikátor:** identifikační řetězec dokumentu ve tvaru **NavestiUpresneniDoplnek** tvořený:
 - **návěštím a upřesněním:** specifické řetězce, které charakterizují typ dokumentu,

- **doplňkem:** obecný text únosné délky dle uvážení autora dokumentu, který slouží ke zlepšení vypovídací hodnoty názvu souboru
- **Verze:** řetězec zajišťující přehled o verzování dokumentu na úrovni názvu dokumentu (pokud má verzování smysl). Verze je standardně uváděna ve tvaru vNN.NN (např. v01.02). V některých případech – např. pracovních meziverzí v rámci pracovní dokumentace lze užívat vhodná rozšíření (např. v01.02a).
- **Přípona:** řetězec dáný typem souboru a vázaný především na používané programové vybavení (např. doc, xls, txt).

V rámci identifikace dokumentů (návěští, upřesnění, doplněk) smí být užíváno výhradně:

- velkých a malých písmen bez diakritiky
- číslic 0 až 9
- speciálních znaků „_“ a „-“

Je-li předán podklad projektu s daným názvem (např. z externích zdrojů, pak je s ním nakládáno s jeho původní identifikací.

Podrobnější informace o značení jednotlivých hlavních typů dokumentů je uveden v následující tabulce:

Popis	Návěští	Upr̃esnění	Dopl̃ñek	Verze	Př̃íklad
Obecný dokument na který nepatří do žádné z dále uvedených skupin			DleUvážení	_vNN.NN	Obecný_dokument_v01.02
Šablona dokumentu	Sab		_DleUvážení	_vNN.NN	Sab_př̃íklad_v00.01
Zpráva o stavu projektu	ZoS	-XX		_vNN.NN	ZoS-03_v00.01
Zápis z jednání vedoucích projektu číslo NN ze dne dd.mm.rrrr	ZJ	-VP-XX_rrrrmmdd		_vNN.NN	ZJ-VP-06_20090202_v01.00
Zápis z jednání Řídící rady číslo NN ze dne dd.mm.rrrr	ZJ	-RR-XX_rrrrmmdd		_vNN.NN	ZJ-RR-02_20090202_v01.00
Zápis z jednání - ostatní číslo NN ze dne dd.mm.rrrr	ZJ	-Os_rrrrmmdd	_DleUvážení	_vNN.NN	ZJ-Os_20090202_Pom_v01.00
Zápis interview ze dne dd.mm.rrrr	ZIn	_rrrrmmdd	_DleUvážení	_vNN.NN	ZIn_20090202_Modul_v00.12
Zpráva ze dne dd.mm.rrrr	Zpr	_rrrrmmdd	_DleUvážení	_vNN.NN	Zpr_20090202_Info_v01.00
Změnový požadavek číslo Z-XXXXX	Z	-XXXXX		_vNN.NN	Z-00047_v01.02
Akceptační kritéria k akceptaci číslo XX	AK	-XX	_DleUvážení	_vNN.NN	AK-05_Ucetnictví_v00.25
Akceptační protokol k akceptaci číslo XX (dle akceptačních kritérií)	AP	-XX	_DleUvážení	_vNN.NN	AP-05_Ucetnictví_v01.00
Závěrečný akceptační protokol	AP-Z			_vNN.NN	APZ_v01.00

Tabulka 3: Značení jednotlivých hlavních typů dokumentů

Nakládání s dokumentací

Pro nakládání s dokumentací jsou stanovena dle vymezených kategorií dokumentace následující zásady:

- **Řízená dokumentace projektu:**
Řízená dokumentace projektu podléhá řízenému zpracování, verzování, předávání, uložení na určeném řízeném zdroji, zálohování, evidenci a řízení přístupu.
- **Pracovní dokumentace projektu:**

Pracovní dokumentace projektu podléhá pravidelnému ukládání na určeném zdroji pracovní dokumentace, zálohování a řízení přístupu.

Účastníci projektu odpovídají za údržbu své pracovní dokumentace na zdroji pracovní dokumentace v souladu s pokyny příslušného vedoucího projektového týmu v takovém stavu, aby tato dokumentace mohla být dále použita v případě nepřítomnosti účastníka nebo při poškození či ztrátě dokumentace na jiných zdrojích (např. lokální pracovní stanice).

- **Specifická dokumentace projektu:**

Specifická dokumentace projektu podléhá minimálně pravidelnému zálohování a řízení přístupu. Dále může být žádoucí verzování a další opatření. Veškerá opatření jsou určována a zajišťována specificky dle charakteru dokumentace určenými účastníky projektu.

Účtenková loterie

Jedním z podpůrných nástrojů může být účtenková loterie. Základním účelem loterie je zvýšení známosti systému EET mezi spotřebiteli a podpora občanů – spotřebitelů při implementaci projektu (zavedení elektronické evidence tržeb) a identifikace poplatníků.

Účtenková loterie nebyla v žádné zemi organizována na obdobné podmínky, zejména způsob fiskalizace. Východiska z jiných zemí však mohou posloužit jako ilustrační a pomoci identifikovat klíčové vlastnosti možné loterie v České republice.

V případě loterie na Tchaj-wan šlo de facto o číselnou loterii, kde byla losována výherní čísla (koncovky) čísel účtenek. Účtenky bylo potřebné zaregistrovat jenom v případě výhry. Výhry byly odstupňovány podle počtu čísel (čtyřčíslí bylo nejmenší a šestičíslí nejvyšší z hlediska výhry). Nevýhodou byla náhodnost a možnost obchodníků generovat čísla účtenek z falešných pokladnic s nepravděpodobnými koncovkami, např. všechny stejné číslo 9999 apod.

Loterie v Slovenské republice byla postavena na principu registrované účtenky, kde podstatným registračním a odlišovacím znakem byli čísla registračních pokladen. Registrované účtenky, resp. čísla pokladen, byly porovnávány vůči databázi registračních pokladen a v případě chybného / neexistujícího čísla nebylo možné účtenku zaregistrovat. Bylo možné nahlásit špatně vystavenou účtenku, to však už nebylo odměněno šancí získat nějakou výhru. Z těchto důvodů byly registrovány zejména účtenky z obchodních řetězců, které však nebyly cílovou skupinou pro odhalování podvodných pokladen.

Z výše uvedených zkušeností vyplývá, že je vhodné orientovat účtenkovou loterii na oblast odhalování špatně vystavených účtenek..

Je možné předpokládat následující základní scénáře pro eventuální okruhy slosovatelných účtenek v rámci specifických „sub loterií“:

1. Účtenka je validní – obsahuje číslo účtenky poplatníka a i správný fiskální identifikační kód.
2. Účtenka může být validní, ale neobsahuje fiskální identifikační kód
3. Účtenka obsahuje nesprávný (falešný) fiskální identifikační kód
4. Účtenka obsahuje jiné nesprávné údaje (např. název poplatníka, datum, ičo nebo hodnotu DPH apod.)

Pozn.: Scénář nevydání účtenky vůbec není vzat v úvahu.

Ověření účtenky i její registrace by měla být co nejjednodušší. V naprosté většině případů bude postačovat jako první krok validace fiskálního identifikačního kódu. Po jeho validaci by měli být poskytnuty ověřovateli i doplňkové údaje jako jsou název poplatníka, nebo provozovny, datum a čas.

V případě negativního ověření, by měla být možnost registrace i této účtenky, minimálně pro kontrolní účely.

Právě účtenky, které nejsou validní, by mohly být zařazeny do slosování samostatně (čímž se dramaticky zvýší pravděpodobnost výhry) nebo uplatnit na ně nějaký bonus – žolíka.

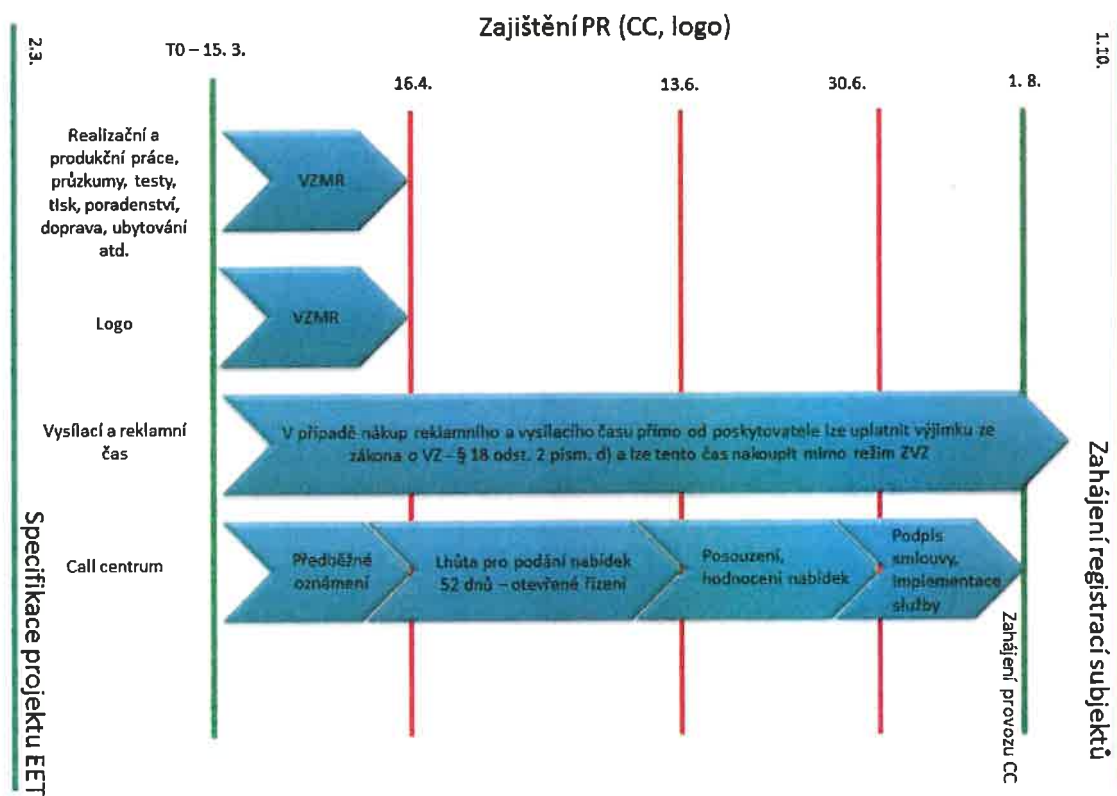
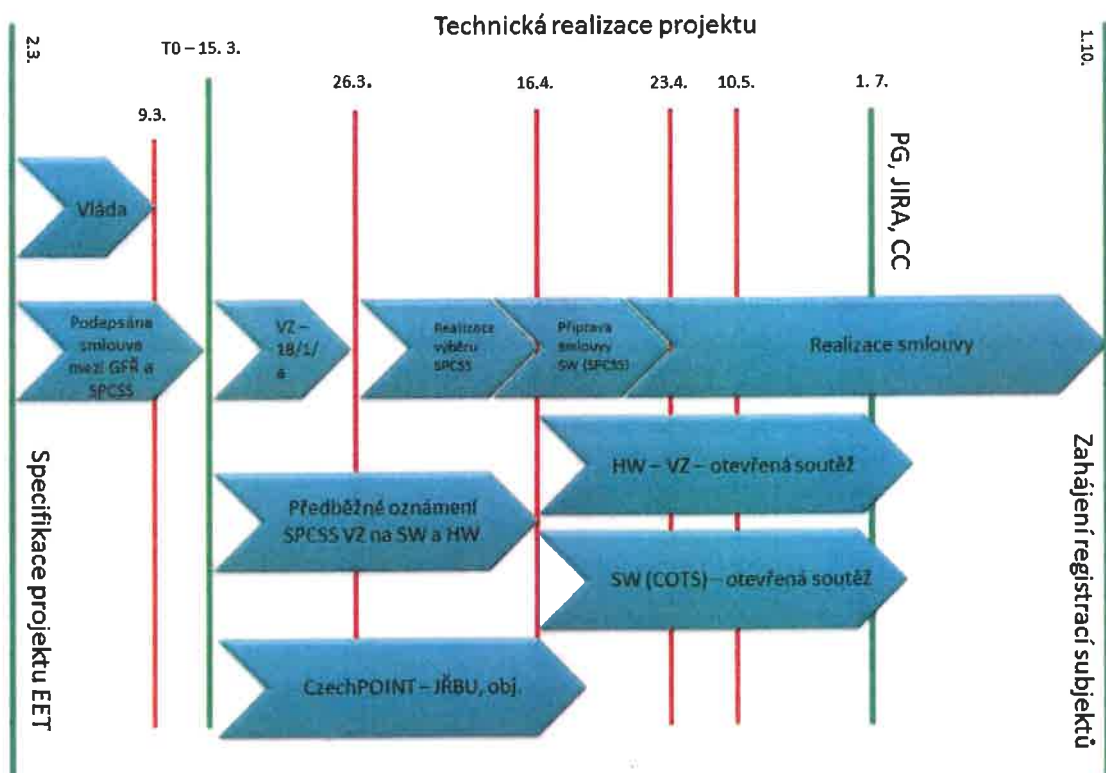
Např. účtenky, které nemají fiskální identifikační kód a budou slosovány, mohou mít několikanásobnou výhru. Nebo účtenky, které mají fiskální identifikační kód, ale není validní, tj. je falešný, by mohli být zařazeny do samostatného slosování.

Preferováním neúplných nebo nevalidních účtenek je možno dosáhnout zvýšeného zájmu na získání právě těchto účtenek a tím vyhledávání provozoven, které jsou více rizikové.

Je potřeba zvážit riziko falšování účtenek soutěžícími? Jde vlastně o jakýsi los, který ovšem nemá žádné ochranné prvky. Falšovat účtenky, kde je něco špatně nebo údaje chybí, je asi to nejjednodušší. Natisknu si libovolný počet účtenek, které nepůjdou žádným způsobem zkontrolovat (budou obsahovat falešné údaje, případně bude chybět údaj o obchodníkovi). Z pohledu výše uvedeného je ovšem taková účtenka vlastně nejcennější a mám šanci získat žolíka.

Účtenky, které nepůjdou ztotožnit s konkrétním dohledatelným obchodníkem, by neměly být do slosování zařazeny. Otázka je, zda a za jakých podmínek jsme schopni všechny účtenky kontrolovat.

Harmonogram projektu



Analýza přínosů a nákladů

Analýza přínosů a nákladů je strukturována jako jednoduchá projekce nákladů a přínosů v čase. Některé obvyklé aspekty jako hodnota projektu nebo projekce rizik v čase nebyly do analýzy zahrnuty.

Důvodem použití jednoduchého modelu byl zřejmý převis přínosů na d náklady, kde jsou přínosy řádově vyšší než náklady. Nejedná se tudíž o standardní projekt, u kterého by rozhodování o projektu záviselo na výsledku analýzy nákladů a přínosů.

Uvedení výčtu přínosů a také nákladů však považujeme za důležité z hlediska získání přehledu o přínosech a nákladech a jejich struktuře.

Přínosy

Identifikace přínosů

Identifikace přínosů počítá jenom s jedním přínosem a to zlepšením výběru daní. Ostatní efekty, jako např. kultivace podnikatelského prostředí, snižování negativních efektů šedé ekonomiky apod. nejsou kvantifikovány.

U hlavního přínosu, vyšších příjmů z daní, byla realizována kvantifikace přínosu dvěma metodami. S ohledem na charakter kvantifikace (kvantum jsou samotné peněžní prostředky), se jedná de facto o přímou monetizaci přínosů.

Kvantifikace byla prostřednictvím metod:

- Kvantifikací přínosu prostřednictvím snížení podílu šedé ekonomiky, a
- Kvantifikací přínosu prostřednictvím snížení odchylky ve výběru daní, tzv. VAT Gap.

Kvantifikace přes šedou ekonomiku

Friedrich Schneider: „Size and Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2013“

15,5% HDP¹¹ za rok 2013, což představuje 596 mld. Kč. Pokles šedé ekonomiky byl v letech 2003 – 2013 cca 6% ročně.

Rozsah šedé ekonomiky není rovnoměrný, ale v jednotlivých odvětvích se liší. Největší podíl (až 25 – 35% z celé produkce) je v sektoru stavebnictví a téměř žádný v hornictví, bankovních službách a distribuci elektřiny. Ostatní sektory jsou nad 10% z celkové produkci v sektorech.

Podle statistického úřadu čtyři sektory, u kterých je podíl šedé ekonomiky nadprůměrný, mají podíl více než 31% na celkovém HDP.

Stavebnictví	7,4%
Obchod, opravy motorových vozidel a spotřební zboží	11,8%
Pohostinství a ubytování	1,9%
Doprava, skladování, pošty a telekomunikace	10,5%

Dá se předpokládat, že **šedá ekonomika u těchto sektorů je více než 200 mld.**

Samozřejmě, potřeba vzít v úvahu i jiné odvětví, jako jsou služby, zemědělství, výroba - zejména spotřebního zboží atd. Z tohoto důvodu byla jako základ pro výpočet odhadnuta hodnota 400 mld. šedé ekonomiky zasažené projektem EET.

¹¹ 3 845,93 mld. Kč za rok 2013

Propočet předpokládaných příjmů prostřednictvím potlačení šedé ekonomiky je vztaženo na % snížení celkové šedé ekonomiky následovně:

Scénář	pesimistický	konzervativní	optimistický
% transferu šedé ekonomiky	1 %	3 %	5 %
přínos (navýšené daně)	4 mld. Kč	12 mld. Kč	20 mld. Kč

Kvantifikace VAT GAP

Byl použit propočet podle studie Evropské komise „Study to quantify and analyse the VAT Gap in the EU-27 Member States“¹²; konkrétně poměr („Household consumption VAT Liability“ k „Total VTTL“) a k „VAT Revenues“.

Jedná se tedy o předpokládaný podíl domácností na celkové daňové mezeře vypočtený jako podíl spotřeby domácností (61,7%) na daňové mezeře DPH (3,267 mld. Euro – 84,9 mld. Kč).

Samozřejmě, projekce dokonalého potlačení mezery je nereálná a v nejlepším státě EU (Holansko, Finsko) představuje 5%. Dosažení mediánu zemí EÚ (15%) je pro účely odhadu přiměřené jako maximální dosažitelná hodnota. Za rok 2012 byla hodnota daňové mezery DPH 22%. To zmanená, že v celkovém vyjádření by byla maximální dosažitelná hodnota 27 mld. Kč.

Dosažení této hodnoty jsme odhadli rozloženě v čase na následujících hodnotách v jednotlivých letech:

	2016	2017	2018	2019 - 2021	2022 - 2024
% z předpokládané maximální dosažené hodnoty	10%	25%	40%	50%	60%
suma	2,7 mld.	6,75 mld.	10,8 mld.	13,5 mld.	16,2 mld.

Z obou metod vychází střednědobě objem dosažitelných přínosů 10 – 15 mld. Kč. Pro účely projekce přínosů v čase a srovnání s náklady byla použita hodnota **12 mld. Kč**.

¹²http://ec.europa.eu/taxation_customs/resources/documents/common/publications/studies/vat-gap.pdf

Náklady

Iniciační náklady:

Rozpočet investiční fáze projektu

ELEKTRONICKÁ EVIDENCE TRŽEB

Náklady investiční fáze projektu

390 907 355 Kč

Termín realizace investiční fáze

1.1.2015 - 31.12.2015

Název položky	Odhadovaný náklad v Kč*	Organizace	Projektový tým	Způsob objednávky	Datum dodávky
Poradenství, konzultace	241 879	MF	Projektový	Přímá objednávka	1. 2. 2015
Poradenství PR a komunikace	1 500 000	MF	Projektový	Veřejná soutěž	2/15 -4/16
Externí právní poradenství, právní zastoupení	1 500 000	FS	Právní a admin. podpora	Veřejná soutěž	Trvale
Znalecké posudky	300 000	FS	Právní a admin. podpora	Veřejná soutěž	Trvale
Implementace pilot	7 086 776	SPCSS	Technický		7-12/2015
Správní poplatky, soudní poplatky	100 000	FS	Právní a admin. podpora	Rozpočet	Trvale
Kreativní agentura	2 000 000	FS	PR a komunikace	Veřejná soutěž	3/15 -9/16
Realizační a produkční práce	2 000 000	FS	PR a komunikace	VS a objednávka	4/15 - 9/16
Nákup medií přes agenturu	12 000 000	FS	PR a komunikace	Veřejná soutěž	8/15 - 9/16
Nákup medií napřímo	1 000 000	FS	PR a komunikace	Objednávka	8/15 - 9/16
Průzkumy a testy	500 000	FS	PR a komunikace	Objednávka	2/15 -12/16
Tisky a výroba 3D	1 000 000	FS	PR a komunikace	VS a objednávka	5/15 - 10/16
Ostatní náklady	500 000	FS	PR a komunikace	Objednávka	2/15 - 10/16
Osobní vozidla	3 500 000	FS	Odborný	VS, smlouvy	1. 1. 2016
Vzdělávání, vstupní příprava	175 000	FS	Odborný	VS, objednávka v limitu	1. 1. 2016
Ostatní věcné výdaje mimo programy	4 825 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Jednorázové výdaje ICT (vybavení nových zaměstnanců)	16 500 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Osobní vozidla	2 800 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Mobilní kanceláře	8 000 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Vystrojení	3 044 200	CS	Odborný	Pokryto rámcovými smlouvami	1. 1. 2016
Technické prostředky	818 500	CS	Odborný	Veřejná soutěž	1. 1. 2016
Informační technologie:	2 845 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
				Rámcová smlouva CS	1. 1. 2016
					1. 1. 2016

Z toho: 80 chytrých telefonů 40 notebooků 40 přenosných tiskáren + 8x multifunkční tiskárna do mobilní kanceláře				VS - centrální zadávání MF VS - centrální zadávání MF	1. 1. 2016
Vybavení pracoviště	960 000	CS	Odborný	VS - centrální zadávání MF	1. 1. 2016
Vybavení pracoviště	720 000	CS	Odborný	VS - centrální zadávání MF	1. 1. 2016
Vzdělávání, vstupní příprava	2 365 000	CS	Odborný	Bez VS	1. 1. 2016
Výzbroj	1 050 000	CS	Odborný	Veřejná soutěž	1. 1. 2016
Call centrum	2 000 000	FS	Front office		15. 10. 2015
Nastavení systémů ČP, procesní ICT	10 000 000	FS	Front office	Objednávka ČP	1. 6. 2015
Nastavení Call centra ČP Brno	1 500 000	FS	Front office	Objednávka ČP	1. 6. 2015
Personální náklady na 2FTE	2 400 000	FS	Front office	Objednávka ČP	1. 3. 2015
Mzdové náklady na 1 FTE	1 800 000	SPCSS	Front office	Existující smlouva	1. 3. 2015
Realizace komunikace (NIX)	24 200 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Certifikační autorita EET	14 520 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Frontend vrstva	63 283 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Aplikační a DB vrstva	8 228 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Storage a zálohování	145 200 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
ESB	4 235 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Service desk	1 210 000	SPCSS	Technický	Veřejná soutěž	1. 11. 2015
Aplikace EET (SW)	27 000 000	FS	Technický	Veřejná soutěž	1. 11. 2015
Úpravy ADIS	8 000 000	FS	Technický	JŘBÚ	1. 11. 2015
CELKEM	390 907 355				

*včetně DPH

Provozní náklady:

Rozpočet provozní fáze projektu

ELEKTRONICKÁ EVIDENCE TRŽEB

Náklady provozní fáze projektu

417 479 245 Kč

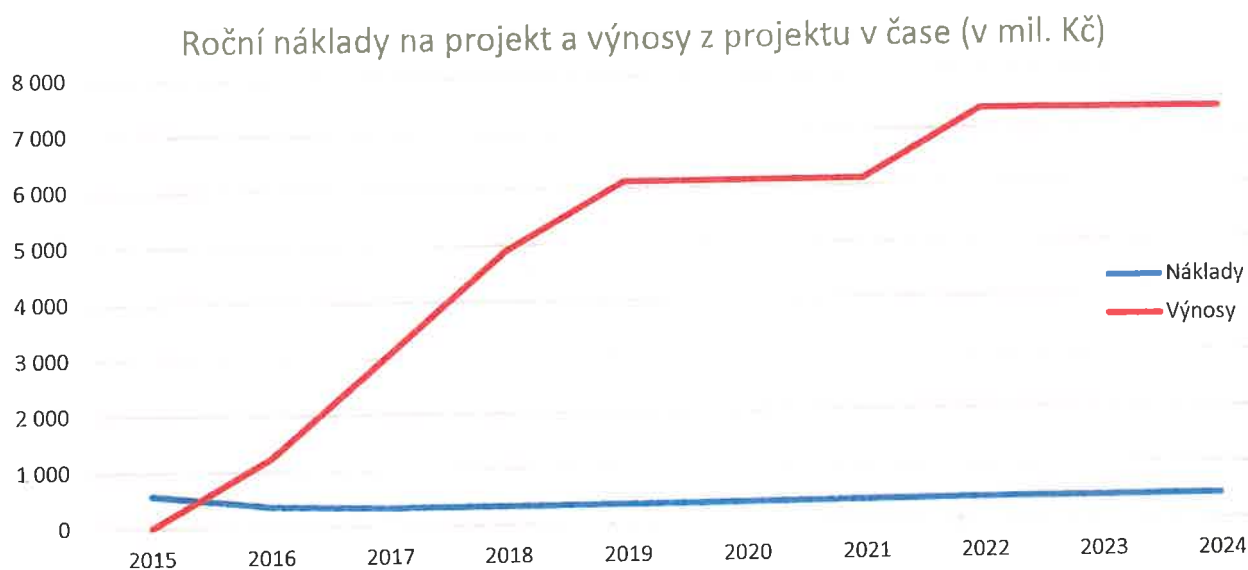
Termín realizace provozní fáze

1.1.2016 - 31.12.2016

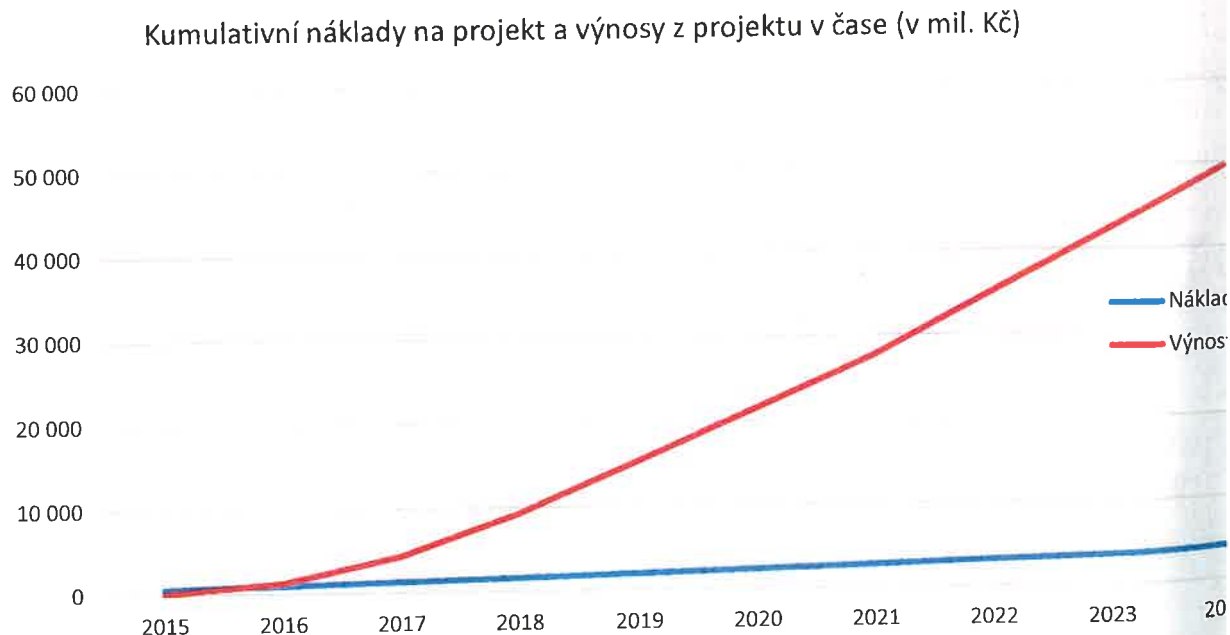
Název položky	Odhadovaný náklad v Kč*	Organizace	Projektový tým	Způsob objednávky	Datum dodávky
Poradenství PR a komunikace	500 000	MF	PR a komunikace	Veřejná soutěž	2/15 -4/16
Obnova vozidel	2 700 000	CS	Odborný	VS 1x za 4 roky	Trvale
Provoz vozidel	1 800 000	CS	Odborný	Navýšení rozpočtu	Trvale
Vystrojení obnova	806 235	CS	Odborný	Navýšení rozpočtu	Trvale
Obnova technických prostředků	163 700	CS	Odborný	Navýšení rozpočtu	Trvale
Ostatní provozní náklady	2 080 000	CS	Odborný	Navýšení rozpočtu	Trvale
Ostatní provozní náklady	800 000	CS	Odborný	Navýšení rozpočtu	Trvale
Mzdové náklady	64 779 276	CS	Odborný	Navýšení rozpočtu	kalendářní rok
Provoz systému souvisejících s EET v systémech ČP	1 000 000	FS	Front office	Navýšení rozpočtu	od 1. 1. 2016
Provoz technického callcentra ČP	600 000	FS	Front office	Objednávka ČP	od 1. 1. 2016
Provoz zákaznického callcentra ČP	2 400 000	FS	Front office	Objednávka ČP	od 1. 1. 2016
Kontrolní nákupy	10 000 000	CS	Odborný	Navýšení rozpočtu	trvale, kalendářní rok
Výdaje na platy včetně příslušenství	133 979 147	FS	Odborný	Navýšení rozpočtové položky	1. 1. 2016
Ostatní IT náklady	4 500 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
Kontrolní nákupy	20 000 000	FS	Odborný	Navýšení rozpočtu	trvale, kalendářní rok
Údržba/Obnova hardware	117 425 290	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Housing	6 845 251	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Service Desk	30 700 346	SPCSS	Technický	Veřejná soutěž	1. 1. 2016
Aplikace EET (SW)	5 400 000	FS	Technický	Veřejná soutěž	1. 11. 2015
PR	2 000 000	FS	PR a komunikace		Kalendářní rok
Ostatní provozní náklady	9 000 000	FS	Odborný	Objednávky, smlouvy	1. 1. 2016
CELKEM	417 479 245				

*včetně DPH

Návratnost projektu v čase



Obrázek 46: Roční náklady na projekt a výnosy z projektu v čase



Obrázek 47: Kumulativní náklady na projekt a výnosy z projektu v čase