INTERWAY

Príloha č. 1 – Opis predmetu zákazky

Implementácia a poskytovanie služieb Personálneho Autorizačného Systému ÚPSVR (P.A.S.)

Cenová ponuka a Návrh technického riešenia

Október 2015

10

Obsah

1 Východiská pre návrh riešenia

1.1 Zámer a cieľ riešenia

V zmysle zákonov 275/2006 o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov ako aj zákona č. 122/2013 o ochrane osobných údajov v znení neskorších predpisov a na základe štúdie uskutočniteľnosti vznikla potreba riešiť zosúladenie prístupu k nosným informačným systémom. Spoločnosti InterWay si kladie za cieľ ponúknuť a následne zabezpečiť dodávku uceleného riešenia pre naplnenie požiadaviek zadania zo stručného opisu zákazky „Personálny autorizačný systém ÚPSVAR" (č. 18218 – MSS, Vestník ÚVO č. 174/2015 - 03.09.2015).

1.2 Predmet realizácie projektu

Predmetom zákazky je implementácia a poskytovanie služieb Personálneho Autorizačného Systému (P.A.S.) ako aj podporných a konzultačných služieb pre potreby riadenia bezpečnosti v oblasti autentifikácie a riadenia prístupu používateľov v súlade s platnou legislatívou podľa nasledovného členenia:

a) Dodávka služieb spojených s riadením bezpečnosti a analýzy metodiky pre projekt P.A.S., bude pokrývať:

- Služby koncepcie riadenia bezpečnosti v oblasti autentizácie a riadenia prístupu používateľov.
- Služby analýzy prostredia a klasifikácie informačných aktív
- Služby metodiky riadenia informačnej bezpečnosti a aktualizácie smerníc v oblasti autentizácie a riadenia prístupu používateľov.

b) Dodávka služieb a implementácie služieb softvérového riešenia pre projekt P.A.S., ktoré budú obsahovať:

- Služby vo forme Informačných systémov s príslušnými licenciami potrebnými na prevádzkovanie dodaných SW komponentov ako služby
- Služby implementácie (inštalácia, konfigurácia a prípadné úpravy) dodaných služieb IS
- Služby podpory integrácie prostredníctvom zverejnenia rozhraní tých IS služieb, ktoré budú využívať IS organizácie v pôsobnosti ÚPSVAR

c) Dodávka hardvéru, softvérových licencií ako služieb infraštruktúry pre P.A.S., ktorá musí pokrývať:

- Potreby softvérového riešenia v oblasti štandardných SW licencií, serverov, diskového priestoru, sieťovej infraštruktúry, monitorovania, technickej podpory a príslušných implementačných prác, potrebných pre realizáciu služieb PKI, ako aj služieb fyzických prístupov a prístupov do IS.
- Služby bezpečnostnej infraštruktúry a riešenia na všetkých vrstvách.

d) Dodávka služieb pre:

- Inštaláciu a konfiguráciu informačných systémov organizácií v pôsobnosti ÚPSVAR s pre komunikáciu s ostatnými IS cez rozhrania a bezpečný komunikačný kanál,

e) Služby projektového riadenia v súlade s metodológiou PRINCE 2 zahrňujúce aj služby monitoringu projektu, riadenia dodávok služieb a finančné riadenie.

f) Poskytnutie záruky na služby v trvaní:

- 24 mesiacov na HW komponenty
- 12 mesiacov na poskytovanie služby

g) Vypracovanie komplexnej dokumentácie riešenia:

- Spracovanie a odovzdanie nasledovných manuálov/príručiek:
  - Užívateľská dokumentácia (príručka),
  - Administrátorská dokumentácia (príručka),
  - Technická dokumentácia,
  - Prevádzková dokumentácia.

h) Vypracovanie základných smerníc a metodických pokynov v spolupráci s obstarávateľom (zodpovednými osobami ÚPSVR).

1.3 Cieľová skupina používateľov projektu P.A.S

Výstupy projektu budú využívať zamestnanci úradov práce v počte 8886.

- Z toho 95% karty s čipom (s PC)
- 5% karty bez čipu (bez PC)
- 10% z počtu 8886 budú návštevnícke karty a rezerva

2. Koncepcia riešenia, rozsah a termíny dodávky

Ako už bolo uvedené predmetom navrhovaného riešenia je vybudovanie systému Služieb P.A.S. V rámci vytvorenia P.A.S. bude vytvorený samotný systém ako aj metodická podpora pre jeho uvedenie do prevádzky. Pre samotné vytvorenie služieb systému budú vykonané nasledovné činnosti:

- Analýza a návrh riešenia,
- Architektúra
- Design
- Špecifikácia požiadaviek na služby IKT
- Implementácia
- Testovanie
- Akceptácia
- Deploy – nasadenie
- Podpora produkčnej prevádzky

Popis jednotlivých činností je uvedený v nasledujúcich kapitolách. Pre zabezpečenie fungovania P.A.S budú dodané potrebné služby softvérového vybavenie ako aj potrebné služby hardvérového vybavenia, ktoré budú potrebné pre funkčnosť riešenia a sú špecifikované v ďalších kapitolách alebo budú doplnené na základe výsledkov analýzy prostredia, ktorá je nutnou podmienkou úspešnej realizácie. Pre potreby zabezpečenia služieb bude potrebná súčinnosť obstarávateľa ako aj zabezpečenie súčinnosti s UPSVR a zabezpečenie súčinnosti s Ministerstvom práce sociálnych vecí a rodiny SR, ktoré v súčasnosti prevádzkuje niektoré funkčné celky pre UPSVR.

2.1 Činnosti a postup realizácie riešenia

2.1.1 Analýza a návrh riešenia

Analýza bude vychádzať z podkladov, ktoré poskytne obstarávateľ a tieto budú ďalej rozpracované do úrovne potrebnej pre realizáciu riešenia. V rámci analýzy budú zohľadnené aj spresnenia, ktoré vzniknú v čase realizácie projektu z titulu prípadných :

- nových požiadaviek legislatívy
- nových požiadaviek na rozhrania s relevantnými systémami
- nových požiadaviek vyplývajúcich z technického návrhu projektu P.A.S,
- nových požiadaviek vyplývajúcich z návrhu bezpečnosti prevádzky projektu P.A.S
- nových požiadaviek na P.A.S definovaných obstarávateľom.

Výsledky analýzy budú zosumarizované do výstupov:

- Detailná funkčná špecifikácia
- Technická architektúra
- Plán nasadenia do pilotnej a produkčnej prevádzky služieb P.A.S

2.1.2 Architektúra

Architektúra P.A.S bude obsahovať návrh a popis jednotlivých technických komponentov služby P.A.S, spôsoby komunikácie, integrácie a bezpečnostnej stránky riešenia. Bude slúžiť aj ako podklad pre prípravu, inštaláciu a konfiguráciu technickej infraštruktúry P.A.S do pilotnej a produkčnej prevádzky.

2.1.3 Design

Realizácia Designu a vývoja riešenia má prierezový charakter. V rámci dodávky riešenia vývoj prebieha v súlade so štandardnou a všeobecne akceptovateľnou metodikou SDLC (Software Development Life Cycle). Cieľom metodiky je zaistiť kontrolované riadenie aktivít v rámci všetkých fáz projektu, a to tak smerom k zadávateľovi ako aj od realizačného tímu podľa potrebnej súčinnosti.

2.1.4 Špecifikácia požiadaviek na služby IKT (HW, SW)

Na základe Opisu predmetu zákazky bude potrebné obstarávateľom zabezpečiť poskytnutie infraštruktúry:

- Zabezpečenie zodpovedajúcej organizačnej štruktúry a personálu pre realizáciu infraštruktúry.
- Zabezpečenie súčinnosti tretích strán.
- Zabezpečenie priestorov a podpornej infraštruktúry priestorov (akými sú napr.: chladenie, napájanie, UPS) pre potreby uskladnenia, implementácie a prevádzky infraštruktúry.
- Zabezpečenie elektrickej a štruktúrovanej kabeláže pre potreby implementácie a prevádzky infraštruktúry podľa požiadaviek definovaných uchádzačom.
- Zabezpečenie vykonania zodpovedajúcich stavebných úprav ak je to potrebné pre realizáciu diela. V prípade vyplynutia potreby pre získanie povolení pre realizáciu týchto stavebných úprav je za získanie týchto povolení zodpovedný obstarávateľ.
- Zabezpečenie realizácie požadovaných opatrení pre realizáciu mechanizmov fyzickej a objektovej bezpečnosti ak to je nevyhnutné pre realizáciu diela.
- Zabezpečenie služieb komunikačnej infraštruktúry pre pripojenie s externými subjektmi a pre pripojenie do internetu.
- Zabezpečenie prevádzky HW a SW vybavenia podľa schváleného dizajnu a v dohodnutých termínoch dodávky služieb HW a SW.
- Zabezpečenie prístupu k nosným IS obstarávateľa
- V oblasti integrácie s existujúcim riešením:
    - Poskytnutie podkladov popisujúcich existujúce riešenie.
    - Zabezpečenie implementácie produktov, ktoré sú mimo rozsahu projektu a nie sú známe uchádzačovi a ich konfiguráciu podľa schválených požiadaviek.

Bude potrebné obstarávateľom zabezpečiť poskytnutie nasledujúceho prostredia s inštanciami zdrojových systémov

- Vývojové - pre vývoj a prototypy integrácie,
- Testovacie - pre E2E testy a bugfixing,
- Integračné - voči verziám zdrojových systémov zodpovedajúcich produkčnému nasadenie, tzv. pre-produkcie.

V oblasti bezpečnosti bude potrebné obstarávateľom zabezpečiť:

- Zabezpečenie bezpečnostných požiadaviek na externé systémy definovaných v tomto dokumente v kapitole Bezpečnostné požiadavky na externé systémy.
- Zabezpečenie zodpovedajúcej organizačnej štruktúry a personálneho zabezpečenia personálu pre realizáciu bezpečnostných mechanizmov.
- Zabezpečenie účinnosti a vynútiteľnosti princípov bezpečnosti, procesov riadenia a prevádzky bezpečnosti vrátane vyvíjaných komponentov a súvisiacich IS tak, aby nezničovali úroveň bezpečnosti.
- Zabezpečenie súčinnosti tretích strán.
- Realizácia bezpečnostných požiadaviek voči tretím stranám je na obstarávateľovi a príslušných subjektoch.

- V oblasti integrácie s existujúcim riešením:
    - Poskytnutie informácií a podkladov popisujúcich existujúce riešenie.
    - Zabezpečenie implementácie produktov, ktoré sú mimo rozsahu projektu P.A.S. a nie sú známe uchádzačovi podľa schválených požiadaviek.

2.1.5 Implementácia

Aktivita implementácia komponentov začína prípravnými prácami na začiatku realizácie projektu a skončí pred nasadením, migráciou údajov a stabilizáciou riešenia. Výstupom aktivity bude realizácie jednotlivých komponentov služieb P.A.S. V rámci tejto činnosti budú vyvinuté resp. nakonfigurované jednotlivé moduly P.A.S podľa špecifikácií vypracovaných v činnosti „Analýza a návrh riešenia".

2.1.6 Testovanie

V rámci tejto činnosti spolu s obstarávateľom otestujeme funkčnosť riešenia P.A.S. Pôjde najmä o preverenie interakcií a správnosť integrácie komponentov softvéru, preverenie, že všetky požiadavky boli správne implementované, identifikovanie chýb a zaistenie ich odstránenia pred nasadením systému do pilotnej a produkčnej prevádzky.

2.1.7 Akceptácia

Akceptácia prebieha dohodnutým postupom, pričom obstarávateľ protokolárne akceptuje projekt alebo službu. Protokoly budú obsahovať záznam o testovaní za účasti Dodávateľa a Objednávateľa. V popise akceptačného protokolu bude uvedený predmet akceptácie, potvrdenie správnosti funkcionality akceptovanej služby alebo komponentu.

2.1.6 Deploy - nasadenie

V rámci tejto činnosti bude P.A.S. postupne nasadzovaný do pilotnej a produkčnej prevádzky. Pri nasadení do pilotnej aj produkčnej prevádzky vykonáme inštaláciu a konfiguráciu aplikačného programového vybavenia. Pilotná prevádzka P.A.S bude prebiehať na produkčnom prostredí P.A. Zabezpečíme podporu a potrebnú metodiku počas celého trvania takto definovanej pilotnej prevádzky. V rámci pilotnej prevádzky počítame aj s možnosťou identifikácie a následného riešenia možných chýb a problémov. Pilotná prevádzka bude končiť vyhodnotením a v prípade potreby prijatím potrebných opatrení. Po úspešnom ukončení pilotnej prevádzky a vykonaní príslušných opatrení bude systém zavedený do produkčnej prevádzky.

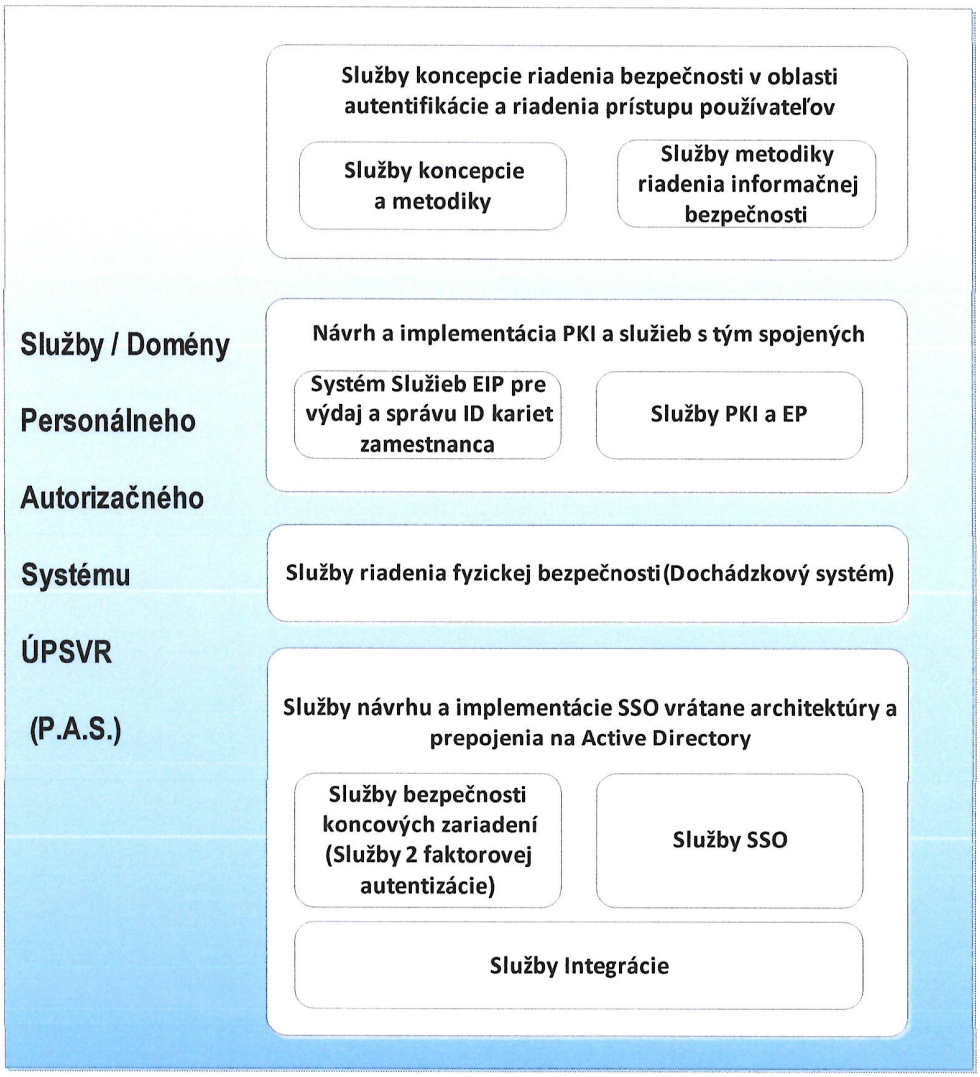
2.1.7 Podpora produkčnej prevádzky

V rámci tejto činnosti budeme podporovať prevádzku systému P.A.S Požadovaný rozsah podpory:

- Riešenie technických a bezpečnostných incidentov,
- Prispôsobenie systému, optimalizačné úpravy a poskytnutie konzultácií na základe zákazníckych požiadaviek v dohodnutom rozsahu
- Aplikácia opravných patchov

2.2 Funkčné domény pre projekt P.A.S.

Na základe výstupov z analýzy a pri poskytnutej súčinnosti spoločnosť InterWay pokryje všetky nižšie uvedené domény riešenia v rámci dodávok služieb projektu P.A.S.



2.3 Termíny dodávky

Predpokladaný rámcový časový harmonogram projektu PA je znázornený v nasledovnej tabuľke, pričom projekt bude rozdelený do 5 fáz - samostatných fakturačných cyklov, kedy sa predpokladá že budú odovzdané dodávky aktivít, ktoré sú v danej fáze označené znakom „X" a ktoré sú popísané v rámci textu tohto dokumentu.

Fáza	Fáza č.1	Fáza č.2	Fáza č.3	Fáza č.4	Fáza č.5
Služby koncepcie a metodiky					
Koncepcia riadenia bezpečnosti	X				
Analýza prostredia a klasifikácia informačných aktív	X				
Metodika riadenia informačnej bezpečnosti a aktualizácia smerníc		X			
Služby PKI a EP					
Služby Implementácia PKI v prostredí ÚPSVR					
Analýza	X				
Architektúra	X				
Design	X				
Dodanie potrebných licencií a HW	X				
Implementácia		X			
Testovanie		X			
Akceptácia		X			
Deploy		X			
Služby riadenia fyzickej bezpečnosti					
Služby riadenia dochádzky					
Analýza	X				
Architektúra	X				
Design		X			
Dodanie potrebných licencií a HW		X			
Implementácia			X		
Testovanie			X		
Akceptácia			X		
Deploy				X	
Bezpečnosť koncových zariadení					
Služby 2 faktorovej autentifikácie					
Analýza	X				
Architektúra		X			
Design			X		
Dodanie potrebných licencií a HW			X		
Implementácia			X		
Testovanie			X		
Akceptácia				X	
Deploy				X	
Služby Systému EIP					
Analýza		X			
Architektúra		X			
Dodanie potrebných licencií a HW		X			

Design		X			
Implementácia			X*	X*	X*
Testovanie			X*	X*	X*
Akceptácia			X*	X*	X*
Deploy			X*	X*	X*

X* - jednotlivé IS v rámci 3. iterácií

T – Dátum podpisu zmluvy

Ako je uvedené v tabuľke predpokladáme zosúladenie termínov jednotlivých fáz podľa požiadaviek obstarávateľa s ohľadom na ukončenie výberového procesu a s ohľadom na podpis zmluvy. Podľa tohto zosúladenia bude vytvorený Plán nasadenia do pilotnej a produkčnej prevádzky. Plán nasadenia P.A.S do pilotnej a produkčnej prevádzky, bude aj obsahovať:

- Detailný časový rámec implementácie P.A.S,
- Spôsob zavedenia testovacej, pilotnej a produkčnej prevádzky.

3. Návrh riešenia P.A.S.

3.1. Dodávka služieb spojených s riadením bezpečnosti a analýzy metodiky pre projekt P.A.S.

Dáta tvoria veľmi dôležitú časť infraštruktúry každej organizácie a patria k tomu najcennejšiemu, čo spoločnosť vlastní.

Okrem ekonomických faktorov sú tu aj zákonné normy a nariadenia, ako napr. zákon o ochrane osobných údajov, ktoré robia firmy zodpovednými za spôsob, ako narábajú s dátami a vytvárajú tlak na zvyšovanie bezpečnosti informačných systémov a dát.

Strata, krádež, či zneužitie dát môže spôsobiť nielen značnú finančnú ujmu, ale aj ujmu na povesti a naštrbenie dôvery obchodných partnerov a klientov. Aby sa predišlo podobným udalostiam, je dôležité implementovať pravidlá v zmysle platnej legislatívy a noriem, ktoré zaručia ich bezpečnosť počas celého životného cyklu.

Koncepcia a metodiky budú v súlade: so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a jeho novelami, so štandardami podľa Výnosu č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy, ako aj s novelou výnosu č. 276/2014 Z. z., ktorou sa novelizuje výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. so zákonom č. 122/2013 Z. z. o ochrane osobných údajov v znení zákona č. 84/2014 Z. z.. so štandardami z oblasti riadenia bezpečnosti podľa noriem radu ISO 27000.

V zmysle požiadaviek budú vypracované nasledovné dokumenty:

- analýza prostredia a klasifikácie informačných aktív.
- metodika riadenia informačnej bezpečnosti a aktualizácie smerníc v oblasti autentizácie a riadenia prístupu používateľov. a poskytnuté služby:
- služby PKI
- služby implementácie EP v identifikovaných systémoch

3.1.1 Analýza prostredia a klasifikácia informačných aktív

V rámci tejto časti bude vykonané preštudovanie a hĺbková analýza prostredia, dokumentácie, postupov a zásad existujúcich v súčasnej dobe s cieľom porozumieť procesom v rámci ÚPSVaR, identifikovať rozsah existujúceho súladu s požiadavkami bezpečnosti.

Výstup etapy:

- Hĺbková analýza súčasného stavu informačných a komunikačných systémov z pohľadu bezpečnosti, ktorej súčasťou budú:
- Identifikácia a klasifikácia informačných aktív dôležité (kritické) informačné aktíva budú mať určených vlastníkov a ich zodpovednosť za aktíva podľa stanovenej klasifikácie s dôrazom zodpovednosti za referenčné dáta odporúčania na klasifikáciu informačných aktív, vlastníkov, dôležitosti a dôsledky prípadne dopady v prípade straty alebo nedostupnosti návrh spôsobu ochrany aktív (v závislosti od ich významu)
- Návrh správy informačných aktív s evidenciou a riadením prístupu k informačným aktívam
- Klasifikačná schéma (schéma klasifikácie informácií)
- Identifikácia a klasifikácia informácií v pôsobnosti ÚPSVR

- Jednoznačné definovanie vlastníka identifikovaných informačných aktív a v rámci nich definovanie jednotlivých informácií
- Definovanie úrovne ochrany pre jednotlivé skupiny klasifikovaných informácií

3.1.2 Metodika riadenia informačnej bezpečnosti a aktualizácia smerníc

V rámci tejto etapy bude spracovaná metodika podporujúca zavedenie a riadenie informačnej bezpečnosti v podmienkach ÚPSVaR.

Tá bude obsahovať sadu dokumentov, ktorá bude pokrývať jednotlivé požiadavky Výnosu, resp. normy STN ISO/IEC 27001:2014.

Výstup etapy:

- Metodika riadenia informačnej bezpečnosti obsahujúci:
- Definovanie pozície manažéra informačnej bezpečnosti, jej právomocí a zaradenie v štruktúre organizácie
- Zavedenia kryptografických prostriedkov na zabezpečenie ochrany dôvernosti údajov pre prípad potreby prenosu údajov, ktoré obsahujú citlivé dáta nezabezpečenou počítačovou sieťou
- *Definovanie bezpečnostných požiadaviek na jednotlivé chránené typy aktív*
- Popis dotknutých systémov a ich bezpečnostného okolia
- Popis akceptovateľnej miery rizika pre jednotlivé aktíva
- Rozsah vzdelávania používateľov v oblasti informačnej bezpečnosti
- Návod na kontrolu efektivity a auditu bezpečnostných opatrení

Prílohy ako samostatné dokumenty k Metodike:

- Návrh postupov na určenie vlastníkov, ktorý zodpovedajú za implementáciu a dodržiavanie primeranej úrovne bezpečnosti každého informačného aktíva
- Návrh postupov formalizovaného schvaľovania inštaláciu prostriedkov IT
- Návrh postupov na vykonávanie overovania reálnej použiteľnosti záložných médií
- Návrh postupu ako zaradiť do procesu pripomienkového konania, v prípade príprav zmlúv s tretími stranami, odbor vnútornej kontroly a bezpečnostného manažéra
- Návrh postupov pre dôvernú a bezpečnú likvidáciu starej alebo nepoužiteľnej výpočtovej techniky, médií, či nosičov dát

3.2 Služby koncepcie riadenia bezpečnosti v oblasti autentifikácie a riadenia prístupu používateľov

3.2.1 Služby PKI

V rámci tejto časti sa predpokladá implementácia prostriedkov PKI infraštruktúry v procesoch autentizácie a el. podpisovania. V rámci tejto časti budú realizované nasledovné kroky:

- Služba zriadenia PKI, služba viacúčelových smart kariet a čítačiek, služba správy digitálnych certifikátov, služba integrácie na adresárové služby prevádzkovateľa.

3.2.1.1 Služba zriadenia PKI

V rámci zriadenia služieb PKI sa predpokladá najmä nasledovný rozsah prác:

- Dodanie HW a SW vybavenie pre prevádzku lokálnych registračných autorít na každom z 46 úradov v pôsobnosti ÚPSVR,

- Vypracovanie a dodanie používateľskej príručky pre operátorov Registračných autorít a samostatnej dokumentácie pre držiteľov certifikátov – zamestnancov ÚPSVR, vyškolenie určených pracovníkov ÚPSVR na funkciu operátor registračnej autority v rozsahu dvoch 8 hodinových školení,
- Vybudované registračné autority budú využívať služby komerčnej certifikačnej autority, ktorá v plnej miere spĺňa všetky definované legislatívne požiadavky na prevádzku certifikačnej autority potvrdené schválením Národným bezpečnostným úradom SR.
- Súčasťou tejto etapy bude aj spracovanie samostatného dokumentu „Certification Practices Statement", ktorý jednoznačne pre potreby ÚPSVR definuje:
- Overenie identity žiadateľa o digitálny certifikát, kroky pre CA ako vytvárať, udržiavať a prenášať certifikáty, popis zabezpečenia kľúčového páru, popis dát, ktoré sú obsiahnuté v digitálnom certifikáte, spôsob revokácie vydaných certifikátov.
- Samostatnou súčasťou dodávky služby bude návrh a vypracovanie procesov, ktoré budú definovať:
    - aké informácie sú nutné a akým spôsobom budú odovzdané pri vydávaní certifikátu vo forme Certifikačných požiadaviek (Certificate requests),
    - postupy pre revokáciu certifikátov,
    - postupy pre zverejnenie informácií o revokácii,
    - postupy vydávania následných certifikátov.

3.2.1.2 Služba viacúčelových smart kariet a čítačiek

V rámci tejto časti budú dodané smart karty a odpovedajúce čítačky pre 9.000 zamestnancov ÚPSVR. Smart karty budú spĺňať nasledovné požiadavky:

Dodávka hybridných kariet, ktorá umožňuje silnú autentizáciu a logické a fyzické kontroly prístupu, možnosť využiť ako zamestnanecký ID preukaz (možnosť potlače), podpora pre heterogénne prostredia OS:

- Windows 7 / Windows 8/ Windows 8.1,
- Windows Server 2003 , 2008 a 2012.

Podpora štandardov PKI ako napr.:

- ISO 7816 1-4,
- PCSC / CCID,
- CryptoAPI / MSCAPI,
- PKCS11,
- X.509 Certificates.

Integrovaný kontaktný čip s podporou napr.:

- Java Card OS,
- Global Platform Specification,
- Crypto Co-Processor,
- Number of 1024 Bit Digital Certificates1 min. 10,
- Number of 2048 Bit Digital Certificates1 min. 10,
- EEPROM Storage.

Podpora vybranej bezkontaktnej technológie napr.:

- HID iCLASS,

- MIFARE Classic,
- MIFARE DESFire EV1.

Podpora aplikácií:

- MS Windows® Domain Log-On
- MS Outlook (kryptovanie a podpisovanie).
- MS Windows Key Storage API.
- Single Sign-On
- VPN (SSL / IPSEC)

Podpisovanie dokumentov

3.2.1.3 Služba správy digitálnych certifikátov

V rámci tejto časti dodávateľ zabezpečí prevádzku systémov certifikačnej autority a dohľad nad prevádzkou vybudovaných registračných autorít v správe ÚPSVR. To zahŕňa najmä monitoring prevádzkovanej siete registračných autorít a súvisiaca softvérová podpora programového vybavenia registračných autorít v rozsahu 16 hodín mesačne.

Súčasťou tejto časti je aj služba dodania max. 8.500 ks digitálnych certifikátov na 4 ročné obdobie pre dotknutých používateľov.

Osobitne bude v rámci tejto časti poskytnutá služba Distribučného Systému Certifikátov (CDS) repozitára, pre distribúciu certifikátov používateľom a organizáciám. Táto služba bude pokrývať nasledovné úlohy:

- Certifikácia platnosti verejných kľúčov podpisom verejných kľúčov, revokovanie „vypršaných" alebo stratených kľúčov, publikovanie verejných kľúčov.

3.2.2. Služby implementácie EP v identifikovaných systémoch

V rámci tejto časti bude zabezpečená automatická distribúcia certifikátov vydávaných v rámci služby správy digitálnych certifikátov na prevádzkované autentizačné systémy pre prihlasovanie používateľov do prostredia informačných systémov ÚPSVR.

Dodávka služby bude pozostávať najmä z analýzy existujúceho prostredia, návrhu integračného zámeru, testovania a nasadenia navrhovaného riešenia v prostredí prevádzkovateľa systémov.

3.3 Služby riadenia fyzickej bezpečnosti (Dochádzkový systém)

3.3.1 Všeobecný popis návrhu riešenia služby

Pre realizáciu časti zadania zameranej na služby riadenia dochádzky navrhujeme zavedenie centrálneho systému evidencie dochádzky pre celé prostredie Obstarávateľa. Na základe hĺbkovej analýzy, ktorá je nutnou podmienkou úspešnej realizácie, prostredia a požiadaviek bude spresnená a ďalej detailizovaná koncepcia návrhu **centralizovaného riešenia s jednou databázou pre celú SR**, alebo **centralizované riešenie podľa krajov**.

Logická schéma oboch riešení je znázornená na obrázkoch nižšie. V súlade s požiadavkou obstarávateľa využiť existujúce riešenia navrhujeme ako centrálny systém evidencie dochádzky použiť jeden aktuálne používaných systémov riadenia dochádzky .

Programové vybavenie bude nainštalované na centrálny server dostupný zo všetkých lokalít UPSVR a bude prevádzkované mimo dátového centra MPSVR. V tomto variante bude služba riadenia dochádzky poskytovaná ako riešenie typu cloud. Služba bude obsiahne aktuálne potrebný počet licencií pre celkový počet používateľov ako aj licencie potrebné pre pripojenie všetkých čítacích jednotiek.

Do aplikácie sa budú užívatelia prihlasovať cez web klienta s možnosťami funkcionality:

- **Používatelia** a spracovatelia informácií dochádzkového systému budú môcť pristupovať k údajom o dochádzke na základe oprávnení s rôznymi úrovňami povolení. Zamestnanci si budú môcť skontrolovať správnosť svojho značenia dochádzky a získať informáciu o odpracovanom čase prostredníctvom web klienta na svojom PC.
- **Prezeratelia** budú môcť sledovať dochádzku im priradených zamestnancov, bez možnosti editácie dochádzkových listov.
- **Spracovatelia** budú mať možnosť ručnej editácie dochádzkových listov (napr. nahratie dovolenky, PN – ky, služobnej cesty, doplnenie chýbajúceho značenia a pod.). Spracovatelia zároveň budú musieť editovať a uzatvárať dochádzkové listy za účelom potvrdenia ich správnosti.

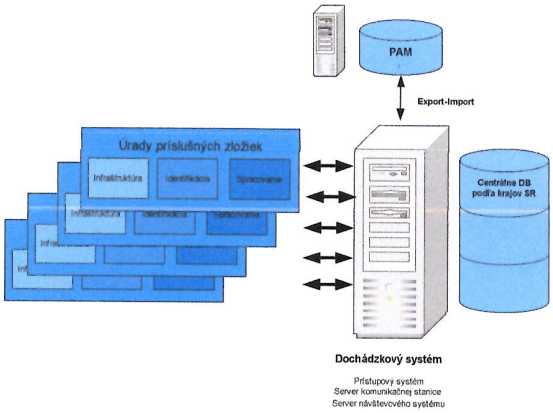
Uzatvorenie a kontrola dochádzkových listov môže byť viacstupňová. Po uzatvorení a odsúhlasení dochádzkových listov bude vyexportovaný súbor pre výpočet miezd do PaM. Súbor bude možné odosielať dávkovo po organizačných zložkách. Údaje o zamestnancoch budú importované do dochádzkového systému s externého zdroja údajov.

Značenie dochádzky budú zamestnanci realizovať na dodaných dochádzkových čítacích jednotkách. Poznačené udalostí bude aplikácia Prístupový systém pomocou Komunikačnej stanice vyčítavať z čítacích jednotiek a exportovať ich do dochádzkového systému v službe cloud. V dochádzkovom systéme budú jednotlivé prechody spracované a podľa nich vypočítavané dĺžky odpracovanej doby prerušení, prípadných príplatkov atď.

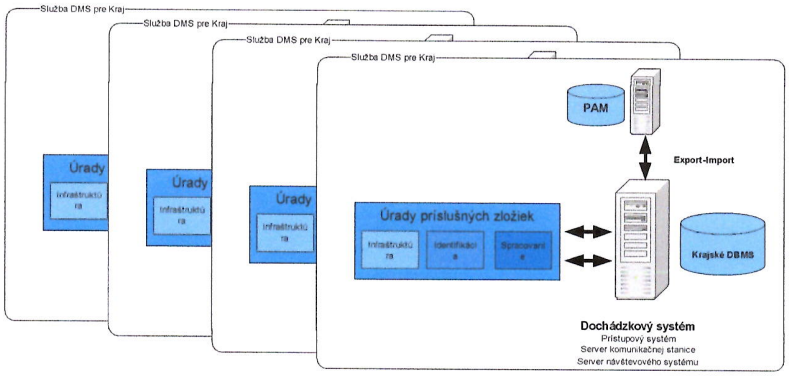
Komunikácia medzi serverom dochádzkového systému a čítacími jednotkami bude realizovaná cez TCP/IP protokol. Komunikačný prevodník v čítacej jednotke bude mat pridelenú vlastnú IP adresu. V prípade zlyhania komunikácie medzi jednotlivými objektami a serverom budú čítacie jednotky jednotlivé prechody ukladať do svojej pamäte a odošlú sa na server po obnovení komunikácie.

- Umiestnenie čítacích jednotiek v jednotlivých objektoch bude realizované na základe analýzy.
- Navrhovaná služba riadenia dochádzky umožňuje evidenciu dochádzky do 9 000 zamestnancov.
- Popis webových služieb a prepojení na externé systémy bude súčasťou analýzy.

Schéma zapojenia centralizovaného riešenia služieb dochádzkového systému s jednou databázou pre celú SR



Riešenie služieb dochádzkového systému s centralizáciou podľa krajov



3.3.2 Stručný popis služieb aplikačného softvéru pre dochádzkový systém

3.3.2.1 Služby komunikačnej stanice

Komunikačná stanica je základným modulom pre komunikáciu s čítacími jednotkami. Je nainštalovaná na komunikačnom počítači alebo severy a zabezpečuje nasledovné funkcie:

- Riadenie komunikácie sčítacími jednotkami,
- ON-LINE monitorovanie stavu čítacích jednotiek s grafickým znázornením ich stavu (uzavretie a uzamknutie),
- Vzdialené ovládanie čítacích jednotiek (otvorenie elektrických zámkov na riadených dverách, zablokovanie ovládaných čítacích jednotiek, ...),
- Zápis údajov do databázy (ON LINE údaje),
- Zápis údajov do textových logovacích súborov s možnosťou vytvoriť pre každú čítaciu jednotku samostatný súbor,
- Poskytovanie informácií pre držiteľov kariet pre zobrazenie na čítacích jednotkách (10 správ po 20 znakov),
- Poskytovanie komunikačných prostriedkov pre Prístupový systém WIS/K, ktorý komunikuje s čítacími jednotkami,

- Smerovanie ON LINE informácií pre nádstavbový monitorovací systém.

Služba komunikačnej stanice môže pracovať ako služba operačného systému. Je schopná *komunikovať prostredníctvom sériových portov a so vzdialenými čítacími jednotkami aj protokolom* TCP/IP. Je možné vytvoriť sieť komunikačných staníc, ktoré môžu byť nainštalované na viacerých počítačoch a sú medzi sebou prepojené prostredníctvom LAN/WAN siete.

3.3.2.2 Služby prístupového systému

Prístupový systém je ľahko konfigurovateľné programové vybavenie, ktoré je svojimi vlastnosťami a cenou schopné plniť požiadavky veľkých, stredných aj malých spoločností a organizácií.

Služby prístupového systému umožňujú a zabezpečujú najmä:

- Priamy on-line prenos dát na riadiace PC a ich ukladanie do databázy a logovacích súborov,
- Získané údaje môže exportovať do nadstavbových aplikácií.
- Viacnásobné zálohovanie systému proti strate informácií
- Modulárna štruktúra umožňujúca rozšírenie systému
- Správa bezkontaktných kariet (pridelenie karty zamestnancovi, evidencia zamestnancov),
- Správa čítacích jednotiek
- Záznam a vyhodnocovanie poznačených prechodov zamestnancov,

3.3.2.3 Služby cloudového dochádzkového systém

Dochádzkový systém cloudového typu umožňuje centralizované spracovanie dochádzky a slúži na kompletnú evidenciu, spracovanie a vyhodnotenie dochádzky zamestnancov. Zabezpečuje kontrolu príchodov a odchodov z pracoviska, vyhodnocuje rôzne druhy prerušenia pracovnej doby. Jeho výstup po mesačnej uzávierke je podkladom pre výpočet miezd. Umožňuje širokú parametrizáciu a prispôsobivosť voči potrebám používateľa, ktoré priamo vychádzajú zo Zákonníka práce, Zákone o mzde, Zákone o plate ako aj zo špecifických požiadaviek vyplývajúcich z kolektívnych zmlúv a rôznych typov smerníc o vyhodnocovaní a evidencii pracovného času.

Cloudový dochádzkový systém umožňuje najmä:

- Evidenciu zamestnancov (pridávanie, oprava, rušenie, archív zamestnancov, tlač zostáv),
- Prideľovanie kariet zamestnancom,
- Výpočet aktuálnej odpracovanej doby (dni, hodiny),
- Výpočet odpracovanej doby za týždeň (PPT),
- Výpočet mesačnej odpracovanej doby,
- Zaznamenávanie, výpočet a rozdelenie druhov prerušenia pracovnej doby (základné aj doplnkové prerušenia.
- Počítanie prerušení - vplyv prerušenia na pracovnú dobu) je možné v systéme ľahko nakonfigurovať,
- Hromadné zadávanie prítomností (vedúci pracovníci) a neprítomností do dochádzkových listov,
- Automatické generovanie záznamov pri dlhodobých neprítomnostiach (nemoc, OČR, dovolenka, ...),

- Možnosť označiť vybraných zamestnancov, ktorých dochádzkový list sa nespracováva podľa údajov zaznamenaných na čítacích jednotkách,
- Registráciu a rozdelenie druhu odpracovanej doby podľa smien (viaczmenné prevádzky),
- *Počítanie salda k danému dňu a jeho prevod do ďalších mesiacov,*
- Automatické generovanie základných druhov príplatkov za prácu (II. a III. zmena, sobota, nedeľa, sviatok),
- Automatické generovanie doplnkových druhov príplatkov za prácu (bonus, pohotovosť, riziko, ...),
- Výstupné zostavy s možnosťou výstupu na tlačiareň (dochádzkové listy, evidenčné listy dochádzky za organizáciu,
- Zoznam zamestnancov, výkazy o prerušeniach a príplatkoch...),
- Archivovanie dochádzkových listov po mesiacoch s možnosťou ich opätovného prezerania a tlače,
- Generovanie prevodového súbory pre systémy PaM,
- Plus ďalšie funkcie, ktoré sú potrebné pre spracovanie a vyhodnotenie dochádzky *zamestnancov.*

Služba čítacej jednotky bude slúžia na snímanie bezkontaktných kariet s ich následným zaznamenaním do vnútornej pamäte. Budú vybavené riadiacou jednotkou s operačným systémom Linux.

3.4 Služby návrhu a implementácie SSO vrátane architektúry a prepojenia na Active Directory

3.4.1 Služby bezpečnosti koncových zariadení (Služby 2 faktorovej autentizácie)

Rozsah implementácie služieb 2 faktorovej autentizácie sa v projekte P.A.S. bude obmedzený na prihlásenie sa používateľov prostredníctvom MS Windows koncových zariadení do existujúcej Microsoft AD domény pomocou čipovej smart karty a PINu.

Vychádzame zo skutočnosti, že použitie čipovej karty pre overenie užívateľa považuje Microsoft za najsilnejšiu formu overovania pre Windows Server v prostredí služby Active Directory systému Windows.

Na základe hĺbkovej analýzy navrhneme a implementujeme nasledovné služby pre potreby 2FA:

- So službami enrolovania Smart Card Certifikátov MS AD
- Manažmentom vydávania Smart Card Certifikátov pre potreby MS AD
- Enrolovanie Smart Card Certifikátov pre potreby MS AD
- Služby pre prihlasovanie používateľov prostredníctvom MS Windows koncových zariadení do domény pomocou čipovej smart karty a PINu a prostredníctvom adresárovej infraštruktúry (AD).

3.4.2 Služby SSO

Zavedením služby SSO namiesto súčasného množstva prihlasovacích údajov si používateľ bude pamätať len jeden a zvyšok vybaví služba SSO. Je preto potrebné zabezpečiť napojenie na systém

identifikácie a autentifikácie používateľa (a autorizácie činností). Pre SSO bude vyvorená vysoko dostupná konfigurácia, napojená na aplikácie UPSVR, ktoré to umožnia. Služba SSO sa stane bránou automatického prihlásenia do jednotlivých, spojených a aj nezávislých systémov ÚPSVR. Pre riešenie SSO služby navrhujeme technologické riešenie s ohľadom na súčasný stav infraštruktúry.

Pri dodávke riešenia a služieb budeme rešpektovať už existujúci systém IDM, ktorý je aktuálne zavedený do prevádzky a integrovaný s AD a so službami a systémami spolupracujúcimi s existujúcim prostredím a AD.

Na fyzickú realizáciu navrhujeme využiť služby riešenia Enterprise Single Sign-On Suite Plus (ESSO Suite) , ktoré predstavuje flexibilnú a prispôsobiteľnú škálovateľnú infraštruktúru správy identít. Poskytuje funkcie ako je:

- Podpora jediného prihlásenia (SSO) do prakticky pre ľubovoľnú aplikáciu bez potreby jej úpravy
- Resetovanie hesla na strane Windows klienta
- Centralizované nastavovanie poverení, pravidiel a ich zmena
- Podpora pre prostredie pracoviska typu kiosk
- Zabezpečená autentifikácia a komplexný audit.

Podporuje väčšinu dnešných aplikácií. ESSO Suite je navrhnutá ako funkcia SSO a resetovania hesla pre Windows, Web, Java, a Mainframe / terminálových aplikácií bežiacich na ľubovoľnom operačnom systéme na ktoré sa pristupuje z systému Windows. Pre SSO nie potrebné úpravy na cieľových systémoch. Poskytuje tiež medzi-platformové riešenie jednotného prihlásenia pre webové aplikácie, vrátane SaaS. Esso Suite znižuje celkové náklady na vlastníctvo TCO tým, že využíva existujúcu infraštruktúru, ako sú adresárové servre AD a databázy a nevyžaduje žiadne modifikácie na cieľových systémoch. Plne prispôsobený inštalačný balík MSI môže byť ľahko vytvorený a široko nasadený na počítačoch koncových užívateľov, čo eliminuje potrebu individuálnej konfigurácie na každom počítači.

Väčšina funkcií SSO je spravovaná pomocou klientskych komponentov, vrátane identifikácie a reakcie na žiadosti aplikácií o kredity, presadzovanie politík a správu autentifikácie. Niektoré moduly SSO využívajú serverové funkcie len na správu a uchovávanie údajov.

SSO ukladá údaje v centrálnych repozitároch ako sú: Microsoft Active Directory, LDAP adresátové služby, databázy Oracle a aj väčšina ostatných riešení pre SQL databázy.

Využívanie existujúcej infraštruktúry, ochrany proti zlyhaniu a zálohovania automaticky podporuje ochranu centrálne uchovávaných SSO údajov, ako sú užívateľské kredity, bezpečnostné politiky a aplikačné vzory.

Klientske konfiguračné údaje ako napríklad politika správy hesiel, politika administratívnych zmien, autentifikačná politika ako aj aplikačné poverenia sa riadia z administratívnych konzol zahrnutých v každom SSO module a sú zosynchronizované s repozitárom. Poskytuje sa tak účinný spôsob, akým môže správca presadzovať špecifické celopodnikové pravidlá a bezpečnostné politiky.

SSO aplikácie používajú štandardizované technológie v oblasti vykonávania ich funkčnosti:

- Kryptovanie užívateľských dát MS-CAPI norma AES
- Prístup údajom cez Active Directory/AD-LDS, LDAP a SQL
- Prepojenie na čipové karty prostredníctvom MS-CAPI a PKCS #11 rozhrania

- Prepojenie s externými a zabudovaných skenermi odtlačkov prstov prostredníctvom BioAPI/BSP
- Integrácia so systémami riadenia identity s použitím SPML
- Konfigurácia uchovávanie údajov prostredníctvom XML

Funkcie navrhovanej služby SSO

- Poskytuje funkčnosť služby automatického jednotného prihlásenia pre Windows, Web, Java, Mainframe/terminálovo orientované aplikácie ku ktorým sa pristupuje z Windows pracovnej stanice. ESSO Logon Manager monitoruje relácie-session automaticky zisťuje požiadavky na prihlásenia do aplikácií a automatické dokončenie prihlásenia vždy, keď je to možné.
- Koncoví používatelia majú ľahký prístup do aplikácií, či už sú prihlásení na podnikovej sieti, alebo cestujú mimo kancelárie, alebo vyžívajú zdieľanie pracovnej stanice.
- Služba ESSO-LM – Login Manger dokáže akceptovať primárnu autentifikáciu používateľa v rámci relácie priamo od prihlásenia do Windows, ako aj s väčšinou priemyselne akceptovaných tokenov, čipové karty, proximity karty a s pridaním ESSO-UAM aj biometrické riešenia. ESSO-UAM môže nahradiť štandardné prihlasovacie Windows mechanizmy vrátane dvojfaktorovej autentifikácia na získanie dodatočnej bezpečnosti mimo session.
- Služba Prístupového portálu poskytuje formulárový prístup k SSO službe založenej na prihlasovanie do internetových Web aplikácií v rámci rôznych platforiem (počítač, tablet & smartfón) a operačných systémov. Táto služba zahŕňa súbor RESTful rozhraní, ktoré umožňuje bezpečný prístup k ESSO konfiguráciám aplikácií a uchovávaním oprávnení v úložisku. Prístupový Proxy komponent poskytuje ESSO spôsobilosť (formulárového jednotného prihlásenia a bezhlavičkovej autentifikácie) pre internetové Web aplikácie bez nutnosti uloženia akejkoľvek formy klientskeho komponentu na prístupovom zariadení.

Komponenty riešenia služby SSO

- **ESSO Logon Manager (ESSO-LM) – Služby Login SSO manažér** – poskytuje funkčnosť služby jednotného prihlásenia

- **Access Portal – Služby prístupového portálu** - ktorý poskytuje prístup funkčnosti služby jednotného prihlásenia pre internetové Web aplikácie

- **ESSO Password Reset (ESSO-PR) – Služba zmeny hesla** – poskytuje samoobslužnú službu pre zmeny hesla

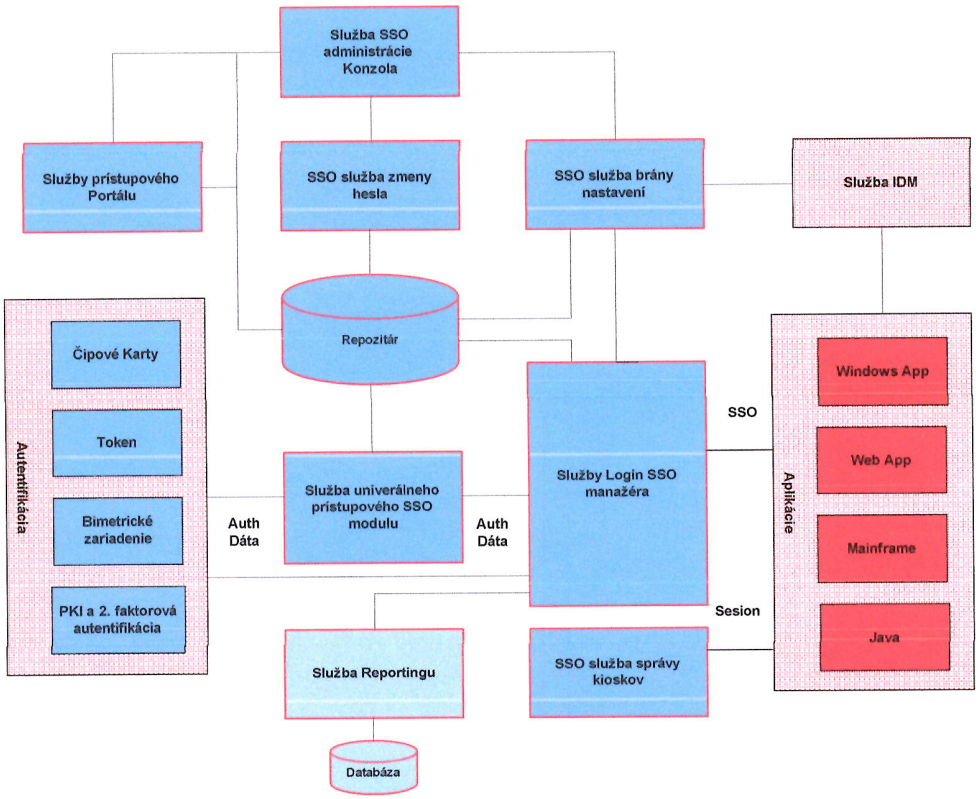
- **ESSO Provisioning Gateway (ESSO-PG) – Služba brány nastavení**– služba automaticky distribuuje údaje systémov do ESSO-LM klienta

- **ESSO Kiosk Manager (ESSO-KM) – Služba správy kioskov** – služba poskytuje riadenie a správy pre prostredie kiosku

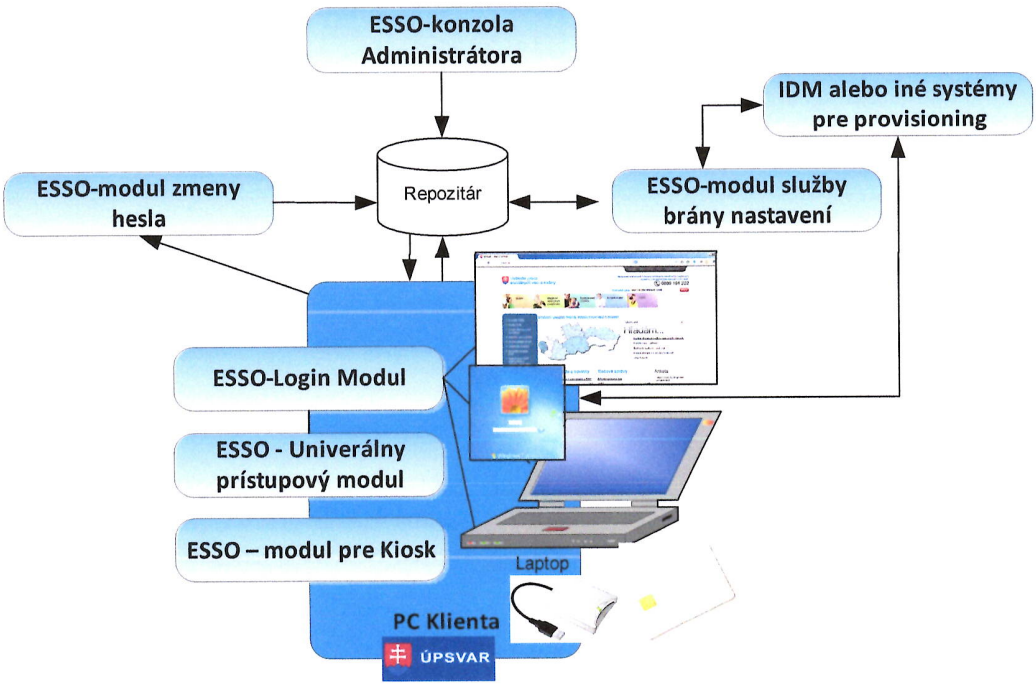
- **ESSO Universal Authentication Manager (ESSO-UAM) – Služba univerzálneho prístupového SSO modulu** - poskytuje silnú autentifikáciu vnútri a aj mimo Windows sessions.

- **ESSO Anywhere – Služba SSO kdekoľvek** – poskytuje možnosť nasadiť ESSO-LM inštalačné balíky na pracovné stanice, ktoré nie sú pripojené do siete

- **ESSO Reporting - Služba reportingu**– zachytáva udalosti a ukladá ich do vzdialenej databázy



Obrázok č. 1: Koncepčná architektúra riešenia SSO



Obrázok č. 2: Koncept nasadenia jednotlivých modulov systému SSO

3.4.3 Služby Integrácie

Uvedomujeme si, že jednou z kľúčových charakteristík projektu, je okrem iného, integrácia na *existujúce IS v rámci projektu* P.A.S..

Našou snahou bude maximálne využitie integračných platforiem obstarávateľa na integráciu dotknutých. Predpokladáme, že na základe analýzy v oblasti integrácie navrhneme, vytvoríme a implementujeme nasledovné služby:

- Návrh integračných rozhraní potrebných pre realizáciu projektu P.A.S. na dotknutých existujúcich a nových IS
- Typy integračných rozhraní
- Návrhové vzory použité pre integráciu
- Interface agreementy
- Implementácia rozhraní na strane dodávaných IS
- Požiadavky na integračné rozhrania existujúcich IS
- Otestovanie
- Nasadenie

V prípade že sa na základe analýzy ukáže potrebné nasadenie novej integračnej platformy, vypracujeme návrh a zdôvodnenie použitia novej integračnej platformy pre P.A.S

3.5 Služby projektového riadenia v súlade s metodológiou PRINCE 2

V rámci aktivity sú vykonávané činnosti, ktoré súvisia s projektovým riadením zo strany spoločnosti InterWay, s riadením a koordináciou prác počas všetkých etáp realizácie projektu zo strany dodávateľa, riadením prostredia pre implementáciu projektu, riadením zmien a konfigurácie a s riadením požiadaviek. Na základe presne stanovených pravidiel bude projekt sledovaný po realizačnej aj finančnej stránke a následne budú prijímané rozhodnutia tak, aby sa zabezpečil hlavný cieľ realizácie projektu P.A.S. Riadenie projektu bude prebiehať v súlade s Metodickým pokynom MF SR 28999/2009-132 pre riadenie IT projektov v súlade s metodikou projektového riadenia Prince2. Cieľom uvedenej metodiky riadenia projektov je prehľadne etapizovať projekt do zvládnuteľných celkov a organizovane dodať definované výstupy požadované zákazníkom.

4 Splnenie požiadaviek na riešenie

4.1 Všeobecné požiadavky

Pri návrhu riešenia a realizácii P.A.S. budeme aplikovať riadenie enterprise architektúry (EA), čím vytvoríme priestor pre nastavenie štandardizovaných pravidiel, ktoré budú platiť všeobecne na celú architektúru P.A.S. v širšom časovom a organizačnom kontexte ako je projekt.

EA rámec budeme uplatňovať v častiach venujúcich sa architektúre v projekte P.A.S. Pri návrhu a riadení architektúry projektu P.A.S. budeme aplikovať architektonický rámec TOGAF 9.1 resp. jeho relevantné časti a pre oblasť modelovania UML a BPMN a notácie architektúry využijeme rámec ArchiMate 2.0 .

V doménach zameraných na SW bude riadenie projektových aktivít v súlade s výnosom MF SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy podľa Prílohy 4: Štandard pre riadenie informačno-technologických projektov a novelizácia výnosu MF 276/2014 o štandardoch pre informačné systémy.

Metodika bude doplnená o prispôsobené prvky Rational Unified Process (RUP) a v oblasti architektúry a tiež o vhodne aplikované disciplíny riadenia EA.

4.2 Legislatívne požiadavky

Pri návrhu riešenie bol zohľadnený fakt, že niektoré častí súčasného riešenia sú súčasťou informačného systému verejnej správy je pre obstarávateľa záväzný Výnos MF SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy a novelizácia výnosu MF 276/2014 o štandardoch pre informačné systémy.

Rovnako bude kladený dôraz na štandardizáciu navrhovaného riešenia pre poskytovanie predmetných služieb podľa medzinárodných štandardov tak, aby navrhované riešenie bolo v súlade s platnou legislatívou.

4.3 Integračné požiadavky

Zo zadania vyplýva, že jednou z kľúčových charakteristík projektu, je okrem iného, integrácia na existujúce IS v rámci projektu P.A.S. Rešpektujeme požiadavku na integráciu dotknutých IS a využitie existujúcich integračných platforiem obstarávateľa. V oblasti integrácie vypracujeme a budeme s ohľadom na výsledky analýzy implementovať nasledovné služby:

- Návrh integračných rozhraní potrebných pre realizáciu projektu P.A.S. na dotknutých existujúcich a nových IS
- Typy integračných rozhraní
- Návrhové vzory použité pre integráciu
- Interface agreementy
- Implementácia rozhraní na strane dodávaných IS
- Požiadavky na integračné rozhrania existujúcich IS
- Otestovanie
- Nasadenie

V prípade, že súčasne z analýzy vyplynie nasadenie novej integračnej platformy, vypracujeme návrh a zdôvodníme prípadné použitie novej integračnej platformy.

4.4 Technologické a bezpečnostné požiadavky

4.4.1 Administrácia systému

Pravidelná aktualizácia systému - Systém počíta s aktualizáciami, ktoré môžu byť spôsobené zmenami legislatívy, ktorá by mohla mať vplyv na beh systému. Webová admin konzola - Súčasťou systému SSO bude webová administrátorské konzola pre správu a monitorovanie časti riešenia SSO

4.4.2 Monitoring

Monitoring a vyhodnocovanie - P.A.S bude monitorovať a zaznamenávať všetky úkony používateľov ako aj činnosť samotného systému a zozbierané dáta bude prezentovať pre možnosti ďalšej analýzy.

Prevádzkové údaje - P.A.S bude zbierať a uchovávať detailné prevádzkové údaje. Prevádzkové údaje bude obsahovať informácie, ktoré umožnia prijatie rozhodnutí pre optimalizačné opatrenia

4.4.3 Dostupnosť a odolnosť systému proti výpadkom

Dostupnosť webového rozhrania - Architektúra P.A.S bude navrhnutá tak, aby aj v prípade výpadku časti infraštruktúry bol systém schopný poskytovať svoje služby

Dostupnosť systému - Dostupnosť systému pre všetkých používateľov bude 24/7 v systéme P.A.S

Požadovaná dostupnosť riešenia je pre: Služby PKI	99%
Služby manažmentu dochádzky	99%
Služby 2 faktorovej autentizácie	99%
Služby SSO	99%

4.4.4 Architektúra

Bude poskytovať všeobecný rámec so schopnosťou budovať systémy s rôznymi typológiami za účelom vyhovieť špecifickým požiadavkám a obmedzeniam. Viacúrovňová ochrana a rôzne aspekty bezpečnosti bude od začiatku časťou implementovanej architektúry. Bezpečnostný model bude flexibilný, umožňovať adaptovať rôzne súčasné a budúce bezpečnostné technológie.

4.4.5 Škálovateľnosť a výkonnosť

Riešenie P.A.S bude spĺňať výkonnostné požiadavky pri jednotlivých dodávaných častiach riešenia služieb a tiež aj pri riešení ako celku. Pre jednotlivé časti riešenia bude systém navrhnutý tak aby splnil požadovaný čas odozvy na menej ako 5 sekúnd. Kapacita spracovávaných požiadaviek bude 10 / 1 sekunda.

Výkonnosť - z dôvodu vysokého predpokladaného počtu používateľov a transakcií bude zabezpečené rozloženie záťaže s dôrazom na odozvu voči koncovým užívateľom.

Vysoká dostupnosť bude zabezpečená prostredníctvom clusteringu.

4.4.6 Bezpečnosť

Pre potreby naplnenia vysokej úrovne bezpečnosti sú bezpečnostné mechanizmy predstavované nielen klasickými technologickými prvkami ale aj prvkami integrovanými do vývoja softvéru a jeho funkcií ako aj netechnologickými prvkami umožňujúcimi systematické riadenie a prevádzkovanie na základe rizík. Doména bezpečnosti vykonáva funkciu dohľadu nad implementáciou bezpečnostných mechanizmov do produktov ostatných domén v súlade s bezpečnostnou architektúrou na úrovni stanovenia architektonických princípov. Jednotlivé domény dodávajú výstupné reporty o implementácii bezpečnostných mechanizmov.

4.5 Prevádzkové požiadavky

Cieľom prevádzky vo všeobecnosti je zabezpečiť bezproblémový chod P.A.S. počas celej jeho životnosti, ako aj minimalizovať prevádzkové náklady. Kľúčovým faktorom pre naplnenie tohto cieľa je nastavenie a zavedenie prevádzkových IT procesov v súlade s metodikou ITIL. Na základe analýzy pre dosiahnutie vyššie uvedených cieľov budú na základe existujúcich prevádzkových procesov návrh na doplnenie procesov o prvky P.A.S. a aktualizovaná dokumentácia