VYMEZENÍ DÍLA

1. Úvodní ustanovení

Předmětem projektu je nasazení systému pro zajištění bezpečnosti mobilních zařízení v prostředí Dopravního podniku hl. m. Prahy, akciová společnost (dále jen „**DPP**“).
V rámci tohoto poptávkového řízení DPP poptává návrh řešení a následnou implementaci systému pro zajištění bezpečnosti mobilních zařízení, který by vyhovoval požadavkům uvedeným v této Příloze č. 1.

1.1. Cíle projektu:

- výrazné povýšení úrovně zabezpečení mobilních zařízení,
- zavedení aktivního přístupu k ochraně mobilních zařízení a jejich obsahu,
- povýšení mobilních zařízení na plnohodnotný pracovní nástroj,
- zavedení způsobů ochrany citlivého obsahu a dat ukládaných v mobilních zařízeních,
- zvýšení pracovní flexibility zaměstnanců,
- zvýšení úrovně služeb poskytovaných jednotkou IT,
- snížení nákladů na nákup mobilních zařízení umožněním využití konceptu BYOD.

2. Popis současného stavu

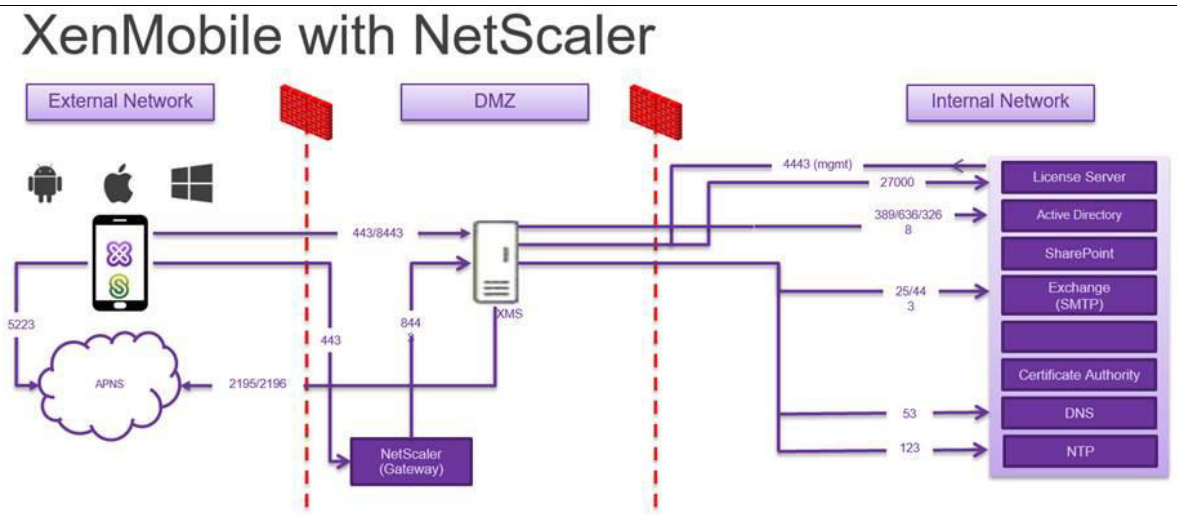
V současné době DPP neprovozuje žádný systém pro zajištění bezpečnosti mobilních zařízení.

3. Požadavky na řešení

3.1. Všeobecné požadavky:

- přehledné administrátorské rozhraní,
- oddělené soukromé a podnikové prostředí (podpora BYOD),
- ochrana podnikového obsahu a dat v zařízení (šifrování),
- možnost poskytnutí aplikací, podnikových aplikací a jejich zabezpečení (publikací na zařízení),
- jednoduchý enrollment na zařízení (ideálně více možností enrollmentu),
- možnost zabezpečeného aktivního přístupu do podnikové sítě (šifrovaná VPN),
- multiplatformní podporu a vyhovující cenový model,
- provozování systému na vlastní infrastruktuře (on premise),
- jednoduchou implementaci do podnikového prostředí a stávající infrastruktury,
- zachování uživatelského soukromí,
- integrace s již funkčními službami v DPP (AD/LDAP, CA, Exchange, VPN atd.),
- jednorázová platba za pořízení licence SW (Perpetual licenční model),
- možnost oddělené správy (delegování např. operátora),
- single Sign-On (SSO) pro pohodlí uživatelů (přes všechny podnikové aplikace a poskytnuté prostředky),
- možnost vzdáleného odstranění podnikových dat a poskytnutých aplikací,
- možnost vzdáleného uzamčení ztraceného/odcizeného zařízení,
- možnost lokalizace ztraceného/odcizeného zařízení na vyžádání uživatele,
- možnost řízení přístupu a manipulace s podnikovými daty a poskytnutými zdroji (prvky „Mobile Content Management“, „Mobile Application Management“ řešení),
- možnost práce s podnikovými daty a obsahem přímo na zařízení (vlastní aplikace nebo integrace s nainstalovanými aplikacemi).

Všeobecné požadavky
***Odpověď**: Plně pokrývá požadavky*
přehledné administrátorské rozhraní Veškeré komponenty jsou administrované prostřednictvím přehledného grafického rozhraní ve formě samostatně instalované administrativní aplikace. Administrace session uživatelů a základní troubleshooting prostředí je možné provádět prostřednictvím webové aplikace **oddělené soukromé a podnikové prostředí (podpora BYOD)** Bude zajištěno implementací Citrix XenMobile Mobile Application Management (MAM). MAM zajišťuje oddělení prostředí pro chráněné podnikové aplikace od privátního prostředí uživatele MAM lze nasadit i bez MDM a vynutit bezpečnostní politiky na úrovni aplikací ne jen celého zařízení **ochrana podnikového obsahu a dat v zařízení (šifrování)** Je využita technologie šifrování samotného mobilního zařízení, XenMobile MAM umožňuje použít i vlastní AES 256-bit šifrování **možnost poskytnutí aplikací, podnikových aplikací a jejich zabezpečení (publikací na zařízení)** Citrix XenMobile Advanced umožňuje komplexní řešení správy podnikové mobility, do kterého patří: Jednotná správa koncových bodů Správa mobilních zařízení Správa mobilních aplikací Zabezpečení síťové brány **jednoduchý enrollment na zařízení (ideálně více možností enrollmentu)** řešení Citrix XenMobile nabízí více možností enrollmentu, enrollment přes SMS, mail, per user unikátní URL pozvánky **možnost zabezpečeného aktivního přístupu do podnikové sítě (šifrovaná VPN)** Spojení mobilního zařízení s podnikovou sítí je šifrováno pomocí VPN. Pokud je to potřeba, je této VPN nadřazena per-app micro VPN, kterou je možno navazovat per aplikace pro separaci síťového provozu mezi aplikacemi **multiplatformní podporu a vyhovující cenový model** Dominantní mobilní platformy iOS a Android jsou plně podporovány, nasazení pro Windows Phone má omezení **provozování systému na vlastní infrastruktuře (on premise)** Servery (XMS a NetScaler) budou nainstalovány v prostředí pod plnou kontrolou zákazníka. Žádná z komponent nevyužívá režim provozování typu SaaS nebo Cloud Viz. Obr. Dále budou oba servery na definovaných portech přístupné do internetu, tak aby byla umožněna komunikace mobilních zařízení.



jednoduchou implementaci do podnikového prostředí a stávající infrastruktury

Podporovány jsou hlavní virtualizační platformy (VMware, Hyper-V, XenServer..), implementace XenMobile serveru je provedeno pomocí šablony pro danou platformu

zachování uživatelského soukromí

V zařízení je možno oddělit podnikovou část od privátní

Všechny aplikace XenMobile jsou zabezpečené a kontejnerizované prostřednictvím technologie Citrix MDX.

integrace s již funkčními službami v DPP (AD/LDAP, CA, Exchange, VPN atd.)

XenMobile umožňuje integraci všech standardních služeb, včetně ověřování v AD, publikaci Exchange atp.

jednorázová platba za pořízení licence SW (Perpetual licenční model)

ano

možnost oddělené správy (delegování např. operátora)

ano je plně podporován role-based model přidělování práv

single Sign-On (SSO) pro pohodlí uživatelů (přes všechny podnikové aplikace a poskytnuté prostředky)

platforma podporuje SSO ověřování uživatelů

možnost vzdáleného odstranění podnikových dat a poskytnutých aplikací

Citrix XenMobile prostřednictvím MDM umožňuje zamknout, smazat nebo selektivně smazat celé zařízení, MAM navíc umožňuje mazat, zamknout, odstranit data na úrovni jednotlivých aplikací v chráněném kontejneru

možnost vzdáleného uzamčení ztraceného/odcizeného zařízení

Citrix XenMobile umožňuje vzdáleně uzamknout zařízení

možnost lokalizace ztraceného/odcizeného zařízení na vyžádání uživatele

Citrix XenMobile umožňuje lokalizovat poslední známou polohu zařízení

možnost řízení přístupu a manipulace s podnikovými daty a poskytnutými zdroji (prvky „Mobile Content Management“, „Mobile Application Management“ řešení)

Je podporováno pro aplikace běžící v MDX chráněném kontejneru

možnost práce s podnikovými daty a obsahem přímo na zařízení (vlastní aplikace nebo integrace s nainstalovanými aplikacemi). Všechny aplikace XenMobile jsou zabezpečené a kontejnerizované prostřednictvím technologie Citrix MDX. *Uchazeč detailně popíše jakým způsobem řešení splňuje uvedený/é požadavek/ky a jak bude požadovaná funkcionalita implementována v navrženém řešení v prostředí DPP.*

3.2. Technologické požadavky

Technologické požadavky
***Odpověď**: Plně pokrývá požadavky*
Požadované komponenty v rámci řešení: **Citrix XenMobile Advanced (1 licence)** Ano bude dodáno v licenčním modelu per-device včetně 1roku podpory od výrobce **Citrix NetScaler VPX200 Enterprise Edition (2 licence)** Ano, budou dodány v rámci řešení, včetně 1rok podpora od výrobce **Požadované parametry** **Zabezpečené separátní prostředí pro podniková data, aplikace a poskytnuté zdroje** Bude zajištěno implementací Citrix XenMobile Mobile Application Management (MAM). MAM zajišťuje oddělení prostředí pro chráněné podnikové aplikace od privátního prostředí uživatele **Zabezpečený komunikační kanál se stávající podnikovou infrastrukturou (aktivní šifrování VPN)** Pro aplikace v chráněném kontejneru je k dispozici šifrovaný VPN tunel do infrastruktury **Propojitelnost se stávajícími službami (Exchange, SharePoint, síťová úložiště, aplikace apod.)** Ano Citrix Xen Mobile Advance umožňuje integraci se službami Exchange a Sharepoint, **možnost využití propojení s podnikovým adresářem na koncovém zařízení (zobrazení kontaktů, identifikace volajícího)** Je podporována synchronizace kontaktů **možnost zpřístupnění vlastních aplikací a systémů na koncovém zařízení v rámci řešení** Je možno aplikace instalovat jak přímo na OS mobilního zařízení tak do chráněného kontejneru **aktivní šifrování v rámci odděleného úložiště pro podniková data a zdroje a to jak v klidovém režimu (uložený obsah a data), tak v aktivním režimu (šifrování přenosu a komunikace)** Ano, je podporováno **možnost bezpečného odstranění podnikových dat, informací a poskytnutých zdrojů při ztrátě nebo kompromitaci koncového zařízení** Lze vyvolat jak samotným uživatelem, tak administrátorem řešení **možnost řízení oběhu dokumentů (interní a externí), nastavení přístupových práv na úrovni dokumentu nebo skupiny dokumentů, kompletní správa životního cyklu dokumentů a možnost**

vytvoření pravidel pro manipulaci s dokumenty a prevenci ztráty dat (regulovaný tisk a pořizování snímků obrazovky, vodoznaky, zamezení aplikací třetí strany apod.). Citrix XenMobile je možno integrovat s DLP a IRM řešeními přes interface protokolu ICAP **Škálovatelnost systému** **horizontální škálovatelnost – v rámci nároků provozu a vývoje** Je podporována **vertikální škálovatelnost – v rámci nároků provozu a vývoje.** Je podporována *Uchazeč detailně popíše jakým způsobem řešení splňuje uvedený/é požadavek/ky a jak bude požadovaná funkcionalita implementována v navrženém řešení v prostředí DPP.*

3.2.1. Požadované komponenty v rámci řešení:

- Citrix XenMobile Advanced (1 licence),
- Citrix NetScaler VPX200 Enterprise Edition (2 licence).

3.2.2. Požadované parametry

- zabezpečené separátní prostředí pro podniková data, aplikace a poskytnuté zdroje
- zabezpečený komunikační kanál se stávající podnikovou infrastrukturou (aktivní šifrování VPN)
- propojitelnost se stávajícími službami (Exchange, SharePoint, síťová úložiště, aplikace apod.)
- možnost využití propojení s podnikovým adresářem na koncovém zařízení (zobrazení kontaktů, identifikace volajícího)
- možnost zpřístupnění vlastních aplikací a systémů na koncovém zařízení v rámci řešení
- aktivní šifrování v rámci odděleného úložiště pro podniková data a zdroje a to jak v klidovém režimu (uložený obsah a data), tak v aktivním režimu (šifrování přenosu a komunikace)
- možnost bezpečného odstranění podnikových dat, informací a poskytnutých zdrojů při ztrátě nebo kompromitaci koncového zařízení
- možnost řízení oběhu dokumentů (interní a externí), nastavení přístupových práv na úrovni dokumentu nebo skupiny dokumentů, kompletní správa životního cyklu dokumentů a možnost vytvoření pravidel pro manipulaci s dokumenty a prevenci ztráty dat (regulovaný tisk a pořizování snímků obrazovky, vodoznaky, zamezení aplikací třetí strany apod.).

3.2.3. Škálovatelnost systému

- horizontální škálovatelnost – v rámci nároků provozu a vývoje
- vertikální škálovatelnost – v rámci nároků provozu a vývoje.

3.3. Funkční požadavky

Funkční požadavky
***Odpověď**: Plně pokrývá požadavky*
Uživatelské role a přístup **možnost několika způsobů enrollmentu zařízení (zavedení do systému přes e-mailový odkaz, SMS odkaz**

zaslaný na koncové zařízení atd.)

Enrollment je možný prostřednictvím SMS, mail, per user unikátní URL pozvánky

single Sign-On přístup k podnikovým informacím, datům a poskytnutým zdrojům

SSO je poskytováno pro microVPN spojení, webové aplikace v rámci intranetu, secure mailového clienta a případně aplikace. SSO pro všechny http, HTTPS zdroje z intranetu

možnost definování několika úrovní uživatelských rolí a přístupů v rámci řešení

Řešení umožňuje definování více rolí: full admin, restricted admin, read only admin, aplication admin, user, custom

Monitoring zařízení

- **možnost vzdálené správy (vzdálené uzamčení koncového zařízení, bezpečné vymazání podnikových dat a aplikací spolu s poskytnutými zdroji, na vyžádání uživatele možnost provedení lokalizace koncového zařízení) a kontroly koncového zařízení - ověření úrovně zabezpečení, kontrola nastavení systému zařízení, kontrola konzistence mobilního OS na koncovém zařízení apod.**

- **ověření souladu koncového zařízení s nastavenou bezpečnostní politikou - nestandardní/nepovolené mobilní OS, nepovolené zvýšení oprávnění koncového uživatele (jailbrake, root), povolená instalace aplikací mimo oficiální distribuční cesty, nainstalované potenciálně nebezpečné aplikace, nedostatečně chráněný přístup k vlastnímu mobilnímu OS (slabý nebo žádný zámek obrazovky)**

- **zobrazení stavu koncového zařízení - typ mobilního OS, chování zařízení z hlediska nastavených politik a definovaných pravidel, enrollment status zařízení (aktivní, čeká na potvrzení, smazané apod.), statistiky koncového zařízení**

- **zobrazení stavu zabezpečení koncového zařízení – aktuální stav zabezpečení a kontroly koncového zařízení, nalezené hrozby a řešené problémy, hlášení problémů a hrozeb**

Odpověď na body v kapitole **Monitoring zařízení**.: XenMobile nabízí dynamické přidělování práv v závislosti na zjištěném stavu zařízení (instalovaný sw, politiky, atp..) a generování reportů. XenMobile provádí při přihlášení a v průběhu provozu v definovaných intervalech inventarizaci zařízení a reaguje na zjištěný stav automatickými akcemi, např. uzamčením zařízení

GUI rozhraní administrátora a uživatele

- **přehledné uživatelské rozhraní s možností základního konfigurování a úpravy zobrazení, včetně přidání dodatečných nebo oblíbených položek**

- **přehledná konzole administrátora - aplikace pro správu/webové rozhraní, možnost vytváření statistik a reportů, přehledné výstupy ze systému**

Odpověď na body v kapitole **GUI rozhraní administrátora a uživatele**: Konzole pro správu prostředí je přístupna z webového prohlížeče v HTML 5 kódu a splňuje požadované funkce

Výkon a provoz systému

- **návrh a implementace řešení s ohledem na možnosti stávající infrastruktury a podmínky provozu DPP**
- **realizované řešení s minimálním dopadem na výkonnost a odezvy koncového zařízení, bez nadměrného vytěžování lokálních zdrojů koncového zařízení (a to i při běhu analytických nástrojů a provádění kontroly nasazeným bezpečnostním řešením)**

XenMobile Server bude instalován jako virtuální appliance s následujícími parametry:

- 4vCPUs
- 8GB RAM
- 50GB disk space

XMS dále vyžaduje MS SQL databázi verze 2012 nebo novější, případně je možno využít embedded PostgreSQL databázi (není doporučeno do produkčního prostředí)

Integrace na další systémy

- **Active Directory/LDAP**
- **Certifikační autorita DPP**
- **Exchange server DPP**
- **Interní systémy Objednatele (SharePoint, Intranet, síťová datová úložiště apod.)**
- **Integrace navrženého řešení do stávající infrastruktury DPP.**

Řešení umožňuje integraci se všemi zmíněnými aplikacemi zadavatele

Uchazeč detailně popíše jakým způsobem řešení splňuje uvedený/é požadavek/ky a jak bude požadovaná funkcionalita implementována v navrženém řešení v prostředí DPP.

3.3.1. Uživatelské role a přístup

- možnost několika způsobů enrollmentu zařízení (zavedení do systému přes e-mailový odkaz, SMS odkaz zaslaný na koncové zařízení atd.),
- single Sign-On přístup k podnikovým informacím, datům a poskytnutým zdrojům,
- možnost definování několika úrovní uživatelských rolí a přístupů v rámci řešení.

3.3.2. Monitoring zařízení

- možnost vzdálené správy (vzdálené uzamčení koncového zařízení, bezpečné vymazání podnikových dat a aplikací spolu s poskytnutými zdroji, na vyžádání uživatele možnost provedení lokalizace koncového zařízení) a kontroly koncového zařízení - ověření úrovně zabezpečení, kontrola nastavení systému zařízení, kontrola konzistence mobilního OS na koncovém zařízení apod.,

- ověření souladu koncového zařízení s nastavenou bezpečnostní politikou - nestandardní/nepovolené mobilní OS, nepovolené zvýšení oprávnění koncového uživatele (jailbrake, root), povolená instalace aplikací mimo oficiální distribuční cesty, nainstalované potenciálně nebezpečné aplikace, nedostatečně chráněný přístup k vlastnímu mobilnímu OS (slabý nebo žádný zámek obrazovky),
- zobrazení stavu koncového zařízení - typ mobilního OS, chování zařízení z hlediska nastavených politik a definovaných pravidel, enrollment status zařízení (aktivní, čeká na potvrzení, smazané apod.), statistiky koncového zařízení,
- zobrazení stavu zabezpečení koncového zařízení – aktuální stav zabezpečení a kontroly koncového zařízení, nalezené hrozby a řešené problémy, hlášení problémů a hrozeb.

3.3.3. GUI rozhraní administrátora a uživatele

- přehledné uživatelské rozhraní s možností základního konfigurování a úpravy zobrazení, včetně přidání dodatečných nebo oblíbených položek,
- přehledná konzole administrátora - aplikace pro správu/webové rozhraní, možnost vytváření statistik a reportů, přehledné výstupy ze systému.

3.3.4. Výkon a provoz systému

- návrh a implementace řešení s ohledem na možnosti stávající infrastruktury a podmínky provozu DPP,
- realizované řešení s minimálním dopadem na výkonnost a odezvy koncového zařízení, bez nadměrného vytěžování lokálních zdrojů koncového zařízení (a to i při běhu analytických nástrojů a provádění kontroly nasazeným bezpečnostním řešením).

3.3.5. Integrace na další systémy

- Active Directory/LDAP,
- Certifikační autorita DPP,
- Exchange server DPP,
- Interní systémy Objednatele (SharePoint, Intranet, síťová datová úložiště apod.),
- Integrace navrženého řešení do stávající infrastruktury DPP.

3.4. Ostatní požadavky

Ostatní požadavky
***Odpověď**: Plně pokrývá požadavky*
Použitý HW a SW HW pro pilotní provoz o Implementace řešení bude provedena v režimu on-premis na serverovém HW DPP, o Alokované HW prostředky v prostředí DPP: ▪ *XenMobile Advanced* – 4vCPU, 8GB RAM, 50GB HDD, ▪ *NetScaler VPX200 EE* – 2vCPU, 2GB RAM, 20GB HDD (počítáno na jednu instanci, pro výsledné řešení HW x2), ▪ *SQL databáze* – 2vCPU, 4GB RAM, cca 20GB HDD. SW pro pilotní provoz o Komplementární řešení bezpečnosti mobilních zařízení prostřednictvím *Citrix XenMobile Advanced,*

- 2x *Citrix NetScaler VPX200 Enterprise Edition.*

Bude použit licenční model per-device. Dostupný hardware je plně dostačující pro plánované nasazení XenMobile řešení a bude takto použito

Popis architektury řešení

podpora provozu na nejrozšířenějších mobilních platformách (Android, iOS, Windows), včetně prvků zabezpečení a šifrování,

Ano vše je podporováno

pilotní provoz řešení bude probíhat v rámci vybrané testovací skupiny koncových zařízení dle vyhodnocení vhodnosti nasazení.

Ano

Rozsah implementace

implementace požadovaného řešení bude provedena Zhotovitelem

Ano

DPP bude na implementaci úzce spolupracovat a to především z důvodu získání detailních informací, které s implementací řešení souvisí, jelikož běžná správa/údržba řešení bude po nasazení řešení na pracovnících DPP

Zaměstnancům zadavatele bude umožněna účast během implementačních prací

zaškolení administrátorů – nastavení a ovládání administrátorského rozhraní, nastavení uživatelské části SW, provozní scénáře a běžná správa/údržba dodaného řešení.

Bude realizováno v rozsahu max. 6 administrátorů

Pilotní projekt

řešení pro pilotní provoz by mělo být koncipováno pro 100 koncových zařízení (licence typu per device),

- celková doba trvání pilotního provozu je plánována na dobu 1 roku,
- k vyhodnocení pilotního provozu dojde po 6 měsících uvedení pilotního provozu tak, aby mohlo být následně rozhodnuto, zda se bude plánovat rozšíření projektu a následný přechod do rutinního provozu po ukončení pilotního provozu,
- v rámci vyhodnocení pilotního provozu bude pracovníky DPP zpracována závěrečná zpráva jako podklad pro následné rozhodnutí o dalším pokračování projektu,
- v případě rozšíření projektu a následném přechodu do rutinního provozu bude požadováno vytvoření a provedení Disaster Recovery scenářů.

Požadovaná dokumentace

- Cílový koncept,
- Instalační dokumentace (včetně schématu navrženého řešení),
- Administrátorský manuál,
- Uživatelský manuál (používání a konfigurace komponent na koncovém zařízení).

Odpověď na body v kapitole **Pilotní projekt a Požadovaná dokumentace**: Pilotní projekt je plánován pro 100 koncových zařízení pokrytých pořízenou licencí na dobu jednoho roku. V rámci projektu bude dodána veškerá požadovaná dokumentace.

Požadavky na součinnost

Požadavky na součinnost DPP v rámci projektu – uvede potenciální Zhotovitel ve své nabídce.

Zhotovitel pro realizaci pilotního projektu od zadavatele očekává:

dodání servisních účtů

zajištění databáze MS SQL verze 2012 nebo novější

certifikáty vydané certifikační autoritou zadavatele

ssl certifikáty vydané veřejnou certifikační autoritou

vytvoření potřebných virtuálních serverů

dodání potřebných IP adres

dodání active directory skupin pro administrativní přístupy do systému

Uchazeč detailně popíše jakým způsobem řešení splňuje uvedený/é požadavek/ky a jak bude požadovaná funkcionalita implementována v navrženém řešení v prostředí DPP.

3.4.1. Použitý HW a SW

HW pro pilotní provoz

- Implementace řešení bude provedena v režimu on-premis na serverovém HW DPP,
- Alokované HW prostředky v prostředí DPP:
  - *XenMobile Advanced* – 4vCPU, 8GB RAM, 50GB HDD,
  - *NetScaler VPX200 EE* – 2vCPU, 2GB RAM, 20GB HDD (počítáno na jednu instanci, pro výsledné řešení HW x2),
  - *SQL databáze* – 2vCPU, 4GB RAM, cca 20GB HDD.

SW pro pilotní provoz

- Komplementární řešení bezpečnosti mobilních zařízení prostřednictvím *Citrix XenMobile Advanced,*
- 2x *Citrix NetScaler VPX200 Enterprise Edition.*

3.4.2. Popis architektury řešení

- podpora provozu na nejrozšířenějších mobilních platformách (Android, iOS, Windows), včetně prvků zabezpečení a šifrování,
- pilotní provoz řešení bude probíhat v rámci vybrané testovací skupiny koncových zařízení dle vyhodnocení vhodnosti nasazení.

3.4.3. Rozsah implementace

- implementace požadovaného řešení bude provedena Zhotovitelem
- DPP bude na implementaci úzce spolupracovat a to především z důvodu získání detailních informací, které s implementací řešení souvisí, jelikož běžná správa/údržba řešení bude po nasazení řešení na pracovnících DPP
- zaškolení administrátorů – nastavení a ovládání administrátorského rozhraní, nastavení uživatelské části SW, provozní scénáře a běžná správa/údržba dodaného řešení.

3.4.4. Pilotní projekt

- řešení pro pilotní provoz by mělo být koncipováno pro 100 koncových zařízení (licence typu per device),
- celková doba trvání pilotního provozu je plánována na dobu 1 roku,

- k vyhodnocení pilotního provozu dojde po 6 měsících uvedení pilotního provozu tak, aby mohlo být následně rozhodnuto, zda se bude plánovat rozšíření projektu a následný přechod do rutinního provozu po ukončení pilotního provozu,
- v rámci vyhodnocení pilotního provozu bude pracovníky DPP zpracována závěrečná zpráva jako podklad pro následné rozhodnutí o dalším pokračování projektu,
- v případě rozšíření projektu a následném přechodu do rutinního provozu bude požadováno vytvoření a provedení Disaster Recovery scenářů.

3.4.5. Požadovaná dokumentace

- Cílový koncept,
- Instalační dokumentace (včetně schématu navrženého řešení),
- Administrátorský manuál,
- Uživatelský manuál (používání a konfigurace komponent na koncovém zařízení).

3.4.6. Požadavky na součinnost

Požadavky na součinnost DPP v rámci projektu – uvede potenciální Zhotovitel ve své nabídce.

4. Harmonogram a postup nasazení

Podle zkušenosti DPP lze pilotní projekt realizovat v následujících fázích. Uveďte předpokládaný harmonogram nasazení řešení podle Vašich zkušeností.

Harmonogram
***Odpověď**: Plně pokrývá požadavky*

Vytvoření dokumentu „Cílový koncept“

Předmětem této fáze bude zpracování dokumentu Cílový koncept, jehož obsahem bude popis finálního technického řešení. Běžná struktura Cílového konceptu je uvedena v následujících bodech:

- Specifikace požadavků:
  - obecné, funkční, technické,
  - požadavky na součinnost DPP.
- Návrh řešení:
  - návrh použitých produktů,
  - Logický návrh řešení,
  - Fyzický návrh řešení.
- Základní definice testovacích/DRP scénářů,
- Definice akceptačních kritérií,
- Rizika a předpoklady.

Podmínkou přechodu do další fáze je akceptace Cílového konceptu DPP.

Cílový koncept bude zhotoven v rozsahu 2 člověkodní

Implementace řešení

Instalace a konfigurace řešení bude probíhat v místě a na infrastruktuře DPP. DPP zajistí v rámci součinnosti HW pro nasazení řešení dle specifikace v bodu 3.4.1. této **Přílohy č. 1**.

Implementace řešení je plánována v rozsahu 2 člověkodní

Vytvoření instalační dokumentace

V průběhu nasazení bude vytvářena dokumentace, popisující detailně změny a konfiguraci systému tak, aby finální verze odpovídala stavu projektu v okamžiku plné akceptace.

Dokumentace bude vytvořena v rozsahu 2člověkodní

Školení

Zhotovitel je povinen provést administrátorské školení personálu DPP (do 6 administrátorů) podle definovaných požadavků. Toto školení může probíhat průběžně např. jako součást implementační fáze.

Školení personálu zadavatele je plánováno v rozsahu 3člověkodní

Akceptace

Na závěr projektu (tj. po dokončení předchozích fází) proběhne finální akceptace řešení. Akceptační kritéria budou definována v rámci Cílového konceptu. Výsledky akceptačních testů budou zadokumentovány a podepsány zástupci Zhotovitele i DPP.

Akceptace řešení je plánována v rozsahu 2člověkodní *Uchazeč připraví návrh harmonogramu projektu*

4.1. Vytvoření dokumentu „Cílový koncept“

Předmětem této fáze bude zpracování dokumentu Cílový koncept, jehož obsahem bude popis finálního technického řešení. Běžná struktura Cílového konceptu je uvedena v následujících bodech:

- Specifikace požadavků:
  - obecné, funkční, technické,
  - požadavky na součinnost DPP.
- Návrh řešení:
  - návrh použitých produktů,
  - Logický návrh řešení,
  - Fyzický návrh řešení.
- Základní definice testovacích/DRP scénářů,
- Definice akceptačních kritérií,
- Rizika a předpoklady.

Podmínkou přechodu do další fáze je akceptace Cílového konceptu DPP.

2MD

4.2. Implementace řešení

Instalace a konfigurace řešení bude probíhat v místě a na infrastruktuře DPP. DPP zajistí v rámci součinnosti HW pro nasazení řešení dle specifikace v bodu 3.4.1. této **Přílohy č. 1**.

2MD

4.3. Vytvoření instalační dokumentace

V průběhu nasazení bude vytvářena dokumentace, popisující detailně změny a konfiguraci systému tak, aby finální verze odpovídala stavu projektu v okamžiku plné akceptace.

1MD

4.4. Školení

Zhotovitel je povinen provést administrátorské školení personálu DPP (do 6 administrátorů) podle definovaných požadavků. Toto školení může probíhat průběžně např. jako součást implementační fáze.

3MD

4.5. Akceptace

Na závěr projektu (tj. po dokončení předchozích fází) proběhne finální akceptace řešení. Akceptační kritéria budou definována v rámci Cílového konceptu. Výsledky akceptačních testů budou zadokumentovány a podepsány zástupci Zhotovitele i DPP.

2MD

5. Podpora řešení

Uveďte rozsah a cenu podpory řešení dle níže uvedených požadavků.

Podpora řešení

Odpověď: *Plně pokrývá požadavky*

Podpora řešení od výrobce (software maintenance)

DPP v rámci realizace projektu požaduje ocenění software maintenance v režimu 8x5 na období 1 roku. Zhotovitel v rámci nabídky specifikuje detaily nabídnuté podpory (závažnosti incidentů, reakční doby apod.).

Ano, Citrix Xen Mobile software maintenance obsahuje nárok na technickou podporu od výrobce v režimu 24x7 po dobu 1roku

Uchazeč specifikuje navrhovanou úroveň podpory řešení s ohledem na níže uvedené požadavky a její cenu.

5.1. Podpora řešení od výrobce (software maintenance)

DPP v rámci realizace projektu požaduje ocenění software maintenance v režimu 8x5 na období 1 roku. Zhotovitel v rámci nabídky specifikuje detaily nabídnuté podpory (závažnosti incidentů, reakční doby apod.).

5.2. Podpora řešení od Zhotovitele

5.2.1. Paušální podpora

DPP požaduje ocenění servisní podpory poskytnuté Zhotovitelem s následujícími parametry:

- servisní podpora na 4 roky (platba bude probíhat měsíčně),
- režim podpory 8x5 s garantovanou dobou odezvy následující pracovní den (pro všechny druhy poruch) a garantovanou dobou neutralizace 1 pracovní den pro kritické poruchy, 3 pracovní dny pro vážné poruchy a 10 pracovních dnů pro poruchy s nízkou závažností,
- rozsah servisní podpory v objemu 1 člověkoden/měsíčně (s možností převodu v rámci kalendářního roku),
- specifikované servisní činnosti:
  - řešení případných poruch nebo problémů na vyžádání DPP,
  - instalace a konfigurace (při přechodu na nové verze produktů),
  - údržba dokumentace,
  - kontrola funkčnosti a nastavení systému (profylaxe),
  - konzultace dle požadavku DPP.

5.2.2. Ad-hoc podpora

Mimo výše uvedenou podporu požaduje DPP specifikaci fixní ceny za člověkoden pro případ, že bude DPP vyžadovat čerpání prací nad rámec výše uvedené paušální servisní podpory. V tomto případě by se jednalo o čerpání na základě standardní ad-hoc objednávky.