



Popis prostředí

Příloha č. 2 zadávací dokumentace pro zadávací řízení „Nasazení MFA a pořízení nosičů certifikátů“

Obsah

[1 Úvod 3](#_Toc198626992)

[2 Popis prostředí SŽ – datové sítě a datová centra 3](#_Toc198626993)

[2.1 Datové komunikační sítě 3](#_Toc198626994)

[1.1 Páteřní uzly uživatelské sítě UAS 3](#_Toc198626995)

[1.2 Propojení uzlů uživatelské sítě UAS 4](#_Toc198626996)

[1.3 Připojení vybraných lokalit do sítě UAS 5](#_Toc198626997)

[1.4 Síťové prostředí TDS 5](#_Toc198626998)

[2.2 Datová centra 6](#_Toc198626999)

[3 Popis prostředí Windows domény 6](#_Toc198627000)

[3.1 Seznam vlastních provozovaných domén v prostředí SŽ 7](#_Toc198627001)

[3.2 Plánované změny 7](#_Toc198627002)

[3.3 Integrace, vztahy a federace 8](#_Toc198627003)

[1.5 Replikace s prostředím MS Entra ID 8](#_Toc198627004)

[3.4 Vztahy důvěry mezi doménami 8](#_Toc198627005)

[3.5 Nákres architektury komponent Windows domén 9](#_Toc198627006)

[4 Popis prostředí PKI 9](#_Toc198627007)

[4.1 PKI ve forestech AD Business zóny 11](#_Toc198627008)

[4.2 Hierarchie CA 12](#_Toc198627009)

[5 Počty uživatelů a koncových stanic 13](#_Toc198627010)

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace veřejné zakázky s názvem „Nasazení MFA a pořízení nosičů certifikátů“, pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje nezbytné součásti prostředí organizace SŽ, které jsou relevantní k poskytnutí dodavatelům.

# Popis prostředí SŽ – datové sítě a datová centra

## Datové komunikační sítě

Síťové prostředí SŽ je rozsahem své celorepublikové sítě porovnatelná se sítěmi poskytovatelů datové konektivity.

SŽ je organizace působící v lokalitách rozprostřených po celé ČR. Jednotlivé budovy, drážní objekty a ostatní součásti drážní infrastruktury jsou vzájemně propojeny s cílem zajištění přenosů např. telematických dat, řídících signálů, kamerových záznamů/streamů, zabezpečovacích komunikací a v neposlední řadě IT komunikací.

Síťovou infrastrukturu SŽ je tedy třeba vnímat jako kombinaci více druhů sítí, které spolu sdílí části přenosové infrastruktury. Z hlediska projektu PAM je důležitá skutečnost, že uvedená síťová infrastruktura poskytuje služby jak systémům kritické infrastruktury (primární aktiva), tak podpůrným aktivům a prvkům kybernetické bezpečnosti.

## Páteřní uzly uživatelské sítě UAS

Uživatelské síťové prostředí (UAS – uživatelsko-administrativní síť) nebo také intranet jsou tvořeny strukturou směrovačů, které zajišťují vzájemné propojení lokalit – zejména administrativních budov, datových center, objektů s kancelářskými prostory a přítomným personálem. Dostupnost takové konektivity v rámci celé ČR zajišťují páteřní komunikační uzly staré MPLS sítě, které jsou dislokovány do označených lokalit:



## Propojení uzlů uživatelské sítě UAS

Páteřní uzly komunikační infrastruktury UAS jsou navzájem propojeny a zajišťují směrování síťových komunikací a na vybraných trasách i redundanci v případě ztráty průchodnosti tras.



## Připojení vybraných lokalit do sítě UAS

Pro připojení jednotlivých lokalit k síti UAS platí, že veškeré lokality, které mají technickou možnost napojení na MPLS síť, tak jsou do této sítě připojeny. U lokalit, kde nejsou dostatečné technické možnosti připojení, jsou využity veřejné sítě (ADSL, GSM) a bezpečný přístup do sítí SŽ je realizován prostřednictvím VPN.

Pro jednotlivé lokality není zcela jednotná architektura zapojení a síťové topologie, což je dáno postupným vývojem prostředí v čase a používáním různých technologií.

## Síťové prostředí TDS

Fyzicky jsou TDS provozovány ve třech různých fyzických sítích, které jsou spolu různě propojené.

* Původní MPLS síť – V této síti je mimo technologických procesů provozován i intranet SŽ (VRF szdc\_global) pro kancelářské systémy SŽ. Intranet SŽ je routován podle oblastí a pro číslování je použita interní metodika. Je zde např. provozován i systém elektronických pokladen cizího právního subjektu ČD, podpůrný systém ISOŘ atd. Využití původní MPLS sítě pro systémy TDS pochází historicky z doby, kdy nebylo v požadovaných lokalitách dostupné jiné datové připojení do TECHLAN. Technicky jsou různé technologie a oblasti rozděleny do VLAN, ale ve společné routovací doméně.
* SDH – síť dedikovaná pro OT a budována jako TDS propojení jednotlivých VLAN a segmentů probíhá přes routovací tabulky. Síť je využívána i pro přenos hlasových služeb
* Nová MPLS síť – V současné době probíhá v prostředí OT sítí projekt segmentace, jejímž cílem je migrace TDS z původní IP MPLS a SDH sítě do nově segmentované IP MPLS sítě. Nahrazuje se tím páteřní funkce SDH sítě, kterou nově nahrazuje MPLS síť, avšak v některých koncových segmentech (listech) síťové infrastruktury se plánuje její napojení na MPLS, zachování a využívaní, zejména metalických síťových segmentů. V plánu MPLS sítě je zřízení šesti až osmi lokálních anebo globálních segmentů (VRF) propojených přechodovými firewally. Segmenty mají respektovat dosavadní členění podle oblastních ředitelství, kde B-pozice v adrese určuje oblast a C-pozice technologii používanou v segmentu. Dosavadní řešení přechodů mezi jednotlivými VLAN je přes přechodové firewally v některých případech přes routovací tabulky (původní SDH síť).

Jako problematické je vnímáno právě spojení TDS s UAS (Intranetem), což má částečně řešit projekt segmentace a přechodu do nové MPLS sítě.

## Datová centra

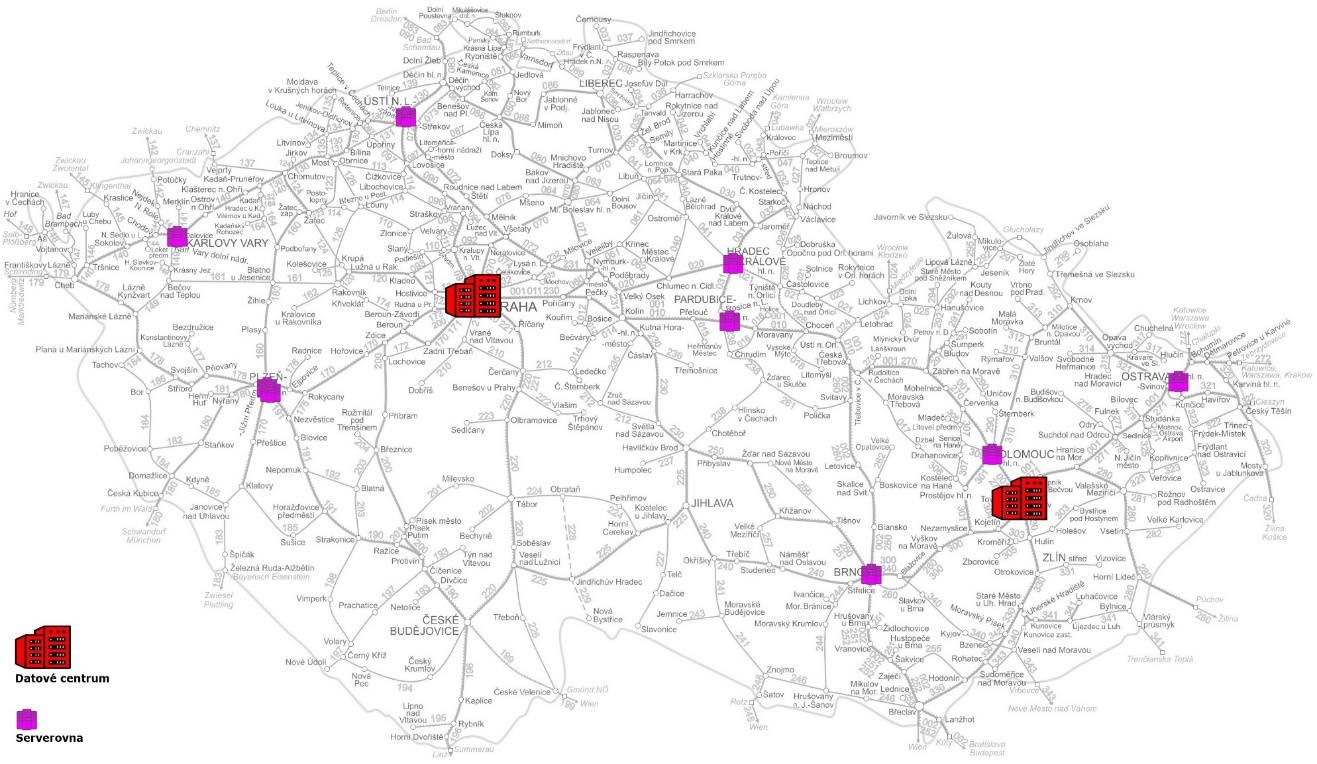
SŽ v současnosti provozuje čtyři datová centra dislokované po území ČR (u pátého se připravuje dostavba a rozšíření).

SŽ provozuje hlavní datová centra v lokalitách:

* Praha (dvě fyzické lokality)
  + Praha U2 – Pod Táborem
  + CDP Praha – V Trianglu
* Brno – Kounicova
* Plzeň – Škroupova
* Přerov – Tovární (*připravuje se*)

Dále provozuje lokální větší serverovny v lokalitách Ústí nad Labem, Karlových Varů, Pardubic, Hradce Králové, Plzně, Olomouce a Ostravy, a více než 200 technologických a sdělovacích místností na území celé ČR.

Datové centrum Praha U2 je ze síťového pohledu považováno za centrum sítě SŽ, kde se nachází prostup k síti Internet.



# Popis prostředí Windows domény

Doménová struktura adresářové služby ActiveDirectory je v současné implementaci SŽ relativně složitá a probíhá její konsolidace pro podpůrná aktiva. **Výstavba adresářová služby AD pro systémy kritické infrastruktury v TDS je v plánu a nebude ve vztahu k AD pro UAS**.

Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky. Kromě informací o objektech v počítačové síti (uživatelské účty, počítače, tiskárny) umožňuje používat stromovou strukturu objektů, nastavovat globálně systémové politiky, instalovat programy na počítače nebo aplikovat kritické aktualizace v celé organizační struktuře.

## Seznam vlastních provozovaných domén v prostředí SŽ

Následující tabulka je souhrnným seznamem domén, které pro své účely provozuje organizace SŽ ve svých datových centrech.

|  |  |  |  |
| --- | --- | --- | --- |
| Doména | Účel domény | Řadiče (hostname) | Lokalita |
| UADF | Forest uživatelských domén UADF | sis0000phant020  sis0000plznt020  sis0000bnont020 | Praha – U2  Plzeň  Brno |
| UADFD01 | Uživatelé a uživatelské stanice | sis0000phant022  sz00000phant022  sis0000plznt022  sis0000bnont022  sz00000bnont022 | Praha – U2  Praha – U2  Plzeň  Brno  Brno |
| UADFD02 | Uživatelé (strojvedoucí) a uživatelské stanice | sis0000phant024  sis0000plznt024  sis0000bnont024 | Praha – U2  Plzeň  Brno |
| OADF | OADF.CZ - odbory | sis0000phant088  sis0000plznt088  sis0000bnont088 | Praha – U2  Plzeň  Brno |
| EADF | EADF.CZ – externí pracovníci | sis0000phant090  sis0000plznt090  sis0000bnont090 | Praha – U2  Plzeň  Brno |
| MADF01 | MADF.CZ – elektronická pošta | sis0000phant050  sis0000plznt050 | Praha – U2  Plzeň |

Verze všech výše uvedených domén (funkční level) jsou Windows 2012 R2.

## Plánované změny

1. Je počítáno s návrhem optimalizace, tedy integrace doménových stromů EADF a OADF do struktury hlavní domény UADF.
2. Plán povýšení verzí na Windows 2019.

## Integrace, vztahy a federace

Specifikace integrací, vztahů a federací popisuje využití prostředků pro napojení na vnější služby vyžadující autentizaci a autorizaci. Pro tyto potřeby jsou využívány dodatečné služby prostředí MS Windows AD, které mají specifická pravidla zajišťující bezpečné a zcela řízené způsoby propojení, sdílení identit, objektů a účtů.

|  |  |  |  |
| --- | --- | --- | --- |
| Druh integrace | Doména | Účel integrace | Hostname serveru |
| ADFS (OpenID) | UADFD01 | Aplikace STROJDAP – tablety strojvedoucích | sis0000phant110 |
| ADFS (OpenID) | UADFD01 | Aplikace SAP Success Factor – HR proces | sis0000phant110 |
| AD Connect | UADFD01 | Synchronizace s prostředím MS Azure AD | sis0000phant115  sis0000phant116 |

## Replikace s prostředím MS Entra ID

* identity jsou replikovány z interní domény do MS Entra ID,
* dochází však také k replikaci z MS Entra ID do interní domény pro účely změny hesel, momentálně pouze pro vybranou skupinu uživatelů,
* identity založené v MS Entra ID nejsou replikovány do interní domény,
* replikace interních identit a objektů do MS Entra ID je řízena pomocí přítomnosti specifického atributu u objektu (pokud atribut není, není objekt replikován) a příslušnosti ke skupině/OU.

## Vztahy důvěry mezi doménami

Jednotlivé doménové „foresty“ a „stromy“ jsou navzájem ve vztahu vzájemné důvěry. Některé „foresty“ a „stromy“, zejména testovací, jsou udržovány mimo tyto důvěrné vztahy.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Doména | Směr důvěry | Doména | Typ vztahu důvěry | Tranzitivní |
| UADF00 |  | UADFD01 | child | ano |
| UADF00 |  | UADFD02 | child | ano |
| UADF00 |  | EADF | forest | ano |
| UADF00 |  | MADF01 | forest | ano |
| UADF00 |  | OADF | forest | ano |
| UADF00 |  | EXTERNAL.CZ | forest | ano |
| UADF00 |  | CD.CZ | forest | ano |
| UADF00 |  | ENSD.CZ | forest | ano |
| UADFD01 |  | CDT.LOCAL | external | ne |
| UADFD01 |  | UXKDC.CDT.LOCAL | realm | ne |

## Nákres architektury komponent Windows domén



# Popis prostředí PKI

Z organizačního pohledu je SŽ rozdělena na UAS (Business zóna) a TDS (Technologická zóna). Uživatelé, systémy, počítače a zařízení SŽ jsou rozděleny mezi tyto dvě zóny.

A diagram of a business structure

AI-generated content may be incorrect.

V obou zónách potřebuje SŽ vydávat a používat certifikáty. Pro zajištění svých potřeb SŽ provozuje (popř. plánuje provozovat) dvě samostatné hierarchie PKI:

* **„Perspektivní“ PKI**, vybudované na **moderních kryptografických algoritmech**, v souladu s doporučením NÚKIB a dalších institucí zabývajících se bezpečností IT.  
  Z této hierarchie jsou vydávány certifikáty, které mají být akceptovány v aplikacích, počítačích a zařízeních, které podporují moderní kryptografii.
* **Legacy PKI**, vybudované na **starších kryptografických algoritmech**.  
  SŽ provozuje celou řadu zařízení, systémů a aplikací, které nepodporují moderní kryptografii. I na těchto komponentách SŽ potřebuje využívat elektronické certifikáty. Pro zajištění kompatibility s těmito zařízeními SŽ provozuje legacy PKI hierarchii. Z legacy PKI jsou vydávány certifikáty, využívané na legacy zařízeních.

Každá hierarchie PKI („perspektivní“ i legacy) je reprezentována jednou kořenovou CA a několika vydávajícími CA. Vydávající CA mají certifikát vydán z kořenové CA dané hierarchie.

Mezi oběma hierarchiemi PKI SŽ není implicitní vztah důvěry. Je na jednotlivých systémech, aby si nastavily, které PKI hierarchii důvěřují. (Vztah důvěry se obvykle navazuje zavedením kořenového certifikátu do seznamu důvěryhodných kořenový CA.)  
Jak již název napovídá, SŽ do budoucna plánuje rozvíjet a provozovat „perspektivní“ hierarchii CA. Naopak, legacy PKI je považováno za dočasné řešení, zavedené z důvodu kompatibility se staršími zařízeními. Legacy PKI bude do budoucna utlumeno a odstaveno.

Obě hierarchie PKI jsou využívány jak v UAS (Business zóna), tak v TDS[[1]](#footnote-2) (Technologická zóna). Každá zóna může provozovat několik vydávajících CA – buď v rámci „perspektivní“ hierarchie anebo v rámci legacy hierarchie. Kořenové CA jsou společné pro Business i Legacy zónu. Obě zóny tedy sdílejí vztah důvěry ke stejným kořenovým CA. Z tohoto pohledu jsou Business i Technologická zóna sdruženy do jednoho bezpečnostního perimetru: sdílejí kořenovou CA a tím i perimetr důvěry. Certifikát, vydaný v rámci Business zóny je akceptován jako důvěryhodný v technologické zóně, a naopak.

## PKI ve forestech AD Business zóny

Bázovou technologickou platformou Business zóny SŽ jsou Active Directory. SŽ v Business zóně provozuje několik forestů, většina z nich má mezi sebou vytvořeny vztahy důvěry (*trust*).

A screenshot of a computer screen

AI-generated content may be incorrect.

Velká část aktiv Business zóny je součástí forestů s Active Directory: uživatelské účty, počítače (resp. operační systémy.) Součástí Business zóny jsou i počítače a zařízení, které nejsou součástí forestů AD. Vydávající CA v Business zóně i v Technologické zóně jsou vybudovány na technologické platformě MS Windows Server.

Díky vytvořeným vztahům důvěry mezi foresty lze z CA, provozované v jednom forestu, vydávat certifikáty doménovým identitám v jiném forestu. Foresty, které si navzájem důvěřují, pak z pohledu správy certifikátů fungují jako jediná doména AD. Enterprise CA v takovém aranžmá může fungovat jako vydávající CA všech „spřátelených“ forestů.

A diagram of a computer network

AI-generated content may be incorrect.

## Hierarchie CA

PKI SŽ je vybudováno tak, aby bylo možno v hierarchii PKI rozšiřovat a podle potřeby doplňovat.

Stručný popis hierarchie:

* Jedna kořenová CA (sdílená mezi Business zónou a Technologickou zónou)  
  Kořenová CA je provozována v offline režimu. Z kořenové CA budou vydány certifikáty pro podřízené vydávající CA.
* Vydávající CA v Business zóně. Obě CA budou integrovány do Active Directory a vydávají certifikáty doménovým i nedoménovým subjektům Business zóny.

A diagram of a computer network

AI-generated content may be incorrect.

Všechny certifikační autority jsou implementovány na platformě MS Windows Server 2019:

Vydávající CA jsou instalovány a provozovány v režimu *enterprise*. Jsou tedy těsně integrovány do domény a využívají benefitů doménového PKI: šablony, oprávnění, autorizace, archivace klíčů atp.

Kryptografické klíče vydávajících CA jsou chráněny v síťových HSM.

Struktura CA pro TDS (Technologickou zónu) je budována analogicky ke struktuře CA v UAS.

# Počty uživatelů a koncových stanic

Správa železnic v současnosti eviduje cca 14.400 aktivních uživatelů ICT prostředí, tj. uživatelů, kteří mají účet v Active Directory a aktivně se přihlašují do domény UADF01.

Správa železnic provozuje cca 9.600 koncových stanic typu PC nebo notebook s operačním systémem Windows 11.

1. V současnosti probíhá výstavba PKI pro TDS. [↑](#footnote-ref-2)