Elektronická výmena údajov medzi partnerskými organizáciami a Slovenskou poštou.

Tento dokument popisuje spôsoby výmeny súborov cez predradený server a prostredníctvom elektronického komunikačného portálu medzi Slovenskou poštou a jej zmluvnými partnermi.

1. Komunikácia cez predradený server

Slovenská pošta, a.s. (ďalej SP, a.s.) má tzv. predradený server, ktorý plní úlohu centra pre výmenu dátových súborov na základe zmluvných vzťahov. Komunikácia s predradeným serverom prebieha na protokole TCP/IP a server je prístupný z verejnej siete internet. Samotná výmena údajov sa uskutočňuje protokolom FTP ľubovoľným FTP klientom, ktorý umožňuje obojsmerný prenos súborov v pasívnom móde, napr. Total Commander, Internet Explorer ....

Bezpečnosť a ochrana údajov pozostáva z niekoľkých častí:

- Komunikácia cez verejný internet je vždy realizovaná kryptovaným kanálom.
- Prístup k serveru je obmedzený len pre definovaných užívateľov – autentifikácia menom a heslom.
- Jednotlivé súbory alebo ich celky sú zabezpečené komerčnými softvérmi proti nedovolenému prístupu alebo modifikácii ich obsahu.

Kryptovací SW slúži na zakryptovanie a elektronické podpísanie súborov. V prípade neoprávneného získania súborov tak nie sú čitateľné. Zároveň je zabezpečená ich celistvosť a nezameniteľnosť.
Slovenská pošta v súčasnosti akceptuje nasledovné spôsoby kryptovania a podpisovania súborov:

- PGP – komerčný produkt spoločnosti PGP Corporation. Pre kryptovanie súborov postačí PGP Desktop Email,
- GPG – voľne šíriteľný program spĺňajúci štandard OpenPGP opísaný v RFC 2440.

1.1 Pripojenie na predradený server je možné realizovať niekoľkými spôsobmi:

a) Pripojením prostredníctvom VPN klienta prostredníctvom verejného internetu.
   VPN klient
   Tento produkt od firmy Cisco slúži na vytvorenie kryptovaného kanála cez verejný internet. Je poskytovaný bezplatne Slovenskou poštou.

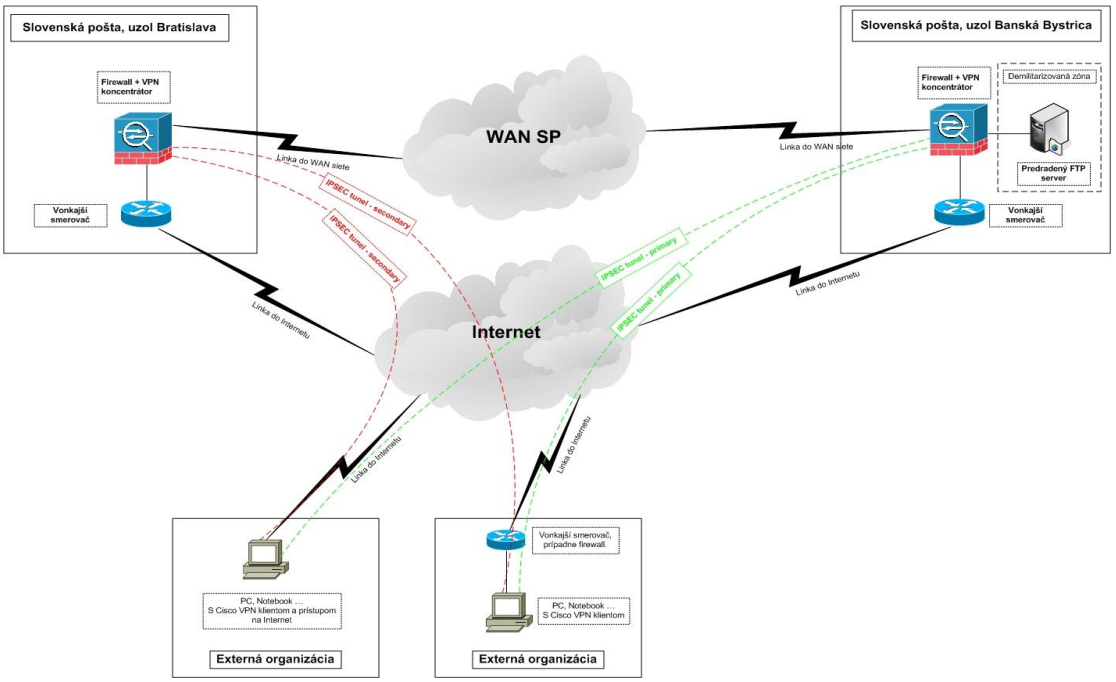
b) Priamym prepojením aktívnych prvkov siete prostredníctvom IPSec tunela prostredníctvom verejného internetu, ak aktívne prvky siete partnerskej organizácie toto podporujú.
   Aktívny prvok s podporou štandardu IPSec
   Sieťové zariadenie (smerovač - router) slúžiace na spojenie lokálnej siete partnerskej organizácie s internetom a na vytvorenie kryptovaného IPSec kanálu z hraničných bodov siete Slovenskej Pošty a.s. a partnerskej organizácie, cez prostredie verejného internetu. V prípade použitia smerovača s implementovaným IPSec nie je potrebná inštalácia VPN klienta na PC. Vyžaduje sa zariadenie kompatibilné so zariadeniami a implementáciou IPSec spoločnosti Cisco Systems

c) Priamym prepojením aktívnych prvkov prostredníctvom prenajatých okruhov

1.2 Podmienky pre jednotlivé spôsoby komunikácie:

a) Pripojenie prostredníctvom VPN klienta
Partnerská organizácia musí mať prístup do verejného internetu, SP, a.s. poskytne zdarma softvér na vytvorenie bezpečného pripojenia partnerskej organizácie na sieť SP, a.s. - VPN klienta pre platformu Windows, SP, a.s. SP, a.s. vytvorí priestor na výmenu dát na predradenom serveri, partnerská organizácia vymieňané dáta kryptuje vlastným kryptovacím SW na základe dohody s SP, a.s.

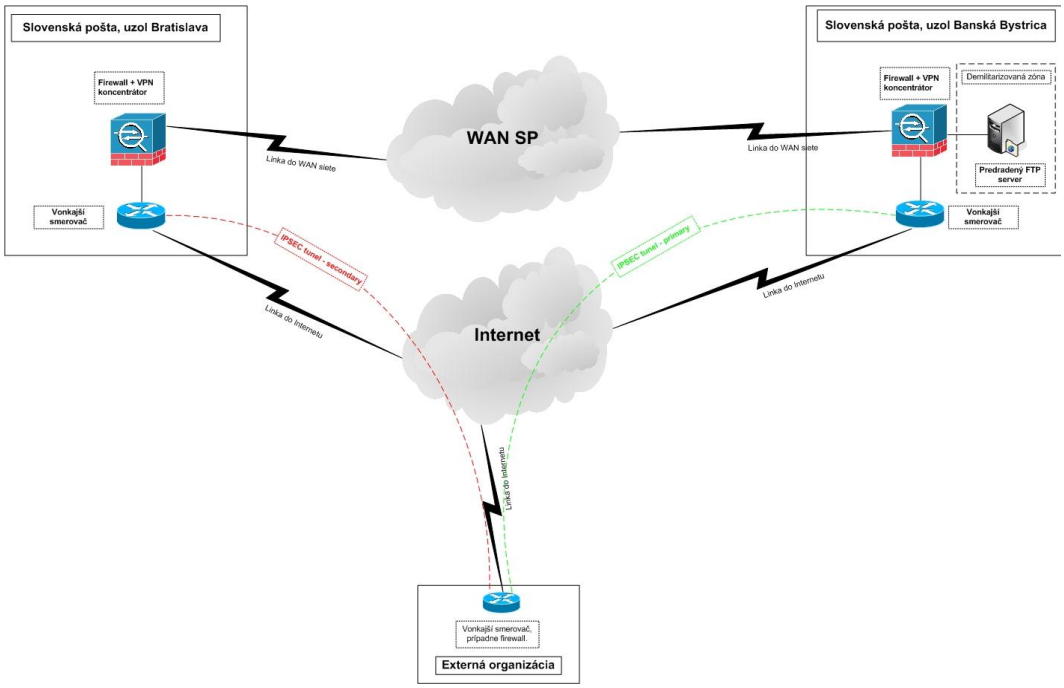
Prístup Externých organizácií prostredníctvom Cisco VPN klienta.



b) Pripojenie prostredniictvom IPSec tunela

Partnerská organizácia musí mať prístup do verejného internetu, aktívny prvok s podporou štandardu IPSec, SP, a.s. vytvorí priestor na výmenu dát na PS, partnerská organizácia vymieňané dáta kryptuje vlastným kryptovacím SW na základe dohody s SP, a.s.

Prístup Externých organizácií prostredníctvom site-to-site IPsec tunelu.



c) Pripojenie prostredníctvom prenajatého okruhu

Partnerská organizácia zriadi prenajatý okruh na základe dohody s SP, a.s., SP, a.s. pripojí okruh na svoje aktívne prvky siete a vytvorí priestor na výmenu dát na PS, partnerská organizácia vymieňané dáta kryptuje vlastným kryptovacím SW na základe dohody s SP, a. s.

1.3 Technické údaje a podmienky pre jednotlivé varianty pripojenia

Pripojenie prostredníctvom	IP adresy SP, a.s.
VPN klient	Primárne VPN pripojenie 62.152.231.206, FTP 10.5.4.10 Sekundárne VPN pripojenie 62.152.231.142, FTP 10.5.4.10
IPSec tunel	Primárne pripojenie 62.152.231.62, potrebný kontakt osôb, nastavujúcich HW Sekundárne pripojenie 62.152.231.58, potrebný kontakt osôb, nastavujúcich HW
Prenajatý okruh	Potrebný kontakt osôb, zriaďujúcich okruh a nastavujúcich HW

2. Komunikácia prostredníctvom elektronického komunikačného portálu

Elektronický komunikačný portál (EKP) je rozhranie, cez ktoré majú klientske aplikácie prístup na elektronickú podateľňu SP, a. s., kde budú dokumenty podpísané elektronickým podpisom prijaté a následne spracované v príslušnej aplikácii.

EKP umožňuje:

- vkladanie dokumentov podpísaných elektronickým podpisom do interných systémov SP, a. s.
- preberanie výstupných dokumentov zo spracovania z interných systémov SP, a. s.

Klientska aplikácia – Externý klient SP, a.s. - vytvorí zo zadaných údajov dokument vo formáte, ktorý dokáže elektronická podateľňa spracovať a ponúkne ho na podpis elektronickým podpisom, zároveň umožní preberanie dokumentov z elektronickej podateľne SP, a. s. aj bez použitia elektronického podpisu.

Elektronická podateľňa je technické zariadenie slúžiace na prijímanie elektronických dokumentov podpísaných elektronickým podpisom a potvrdzovanie ich prijatia. Zabezpečuje

- prijatie elektronického podania a jeho kontrolu predovšetkým z hľadiska schopnosti bezproblémového čítania technickými prostriedkami a dodržanie ustanoveného formátu a obsahu
- vytvorenie a odoslanie potvrdenky o prijatí elektronického podania partnerovi, ktorý podanie odoslal
- spracovanie elektronického podania a úplne overenie zaručeného elektronického podpisu, ktorým je podanie podpísané
- vytvorenie a odoslanie potvrdenia o prijatí alebo odmietnutí elektronického podania
- odoslanie elektronického dokumentu na ďalšie vybavenie

2.1 Podmienky komunikácie prostredníctvom EKP

Partnerská organizácia musí mať prístup do verejného internetu, minimálne požadované pripojenie je cez dial-up s rýchlosťou aspoň 64 kb/s. V prípade, že je sieťové pripojenie filtrované, na firewalle musia byť povolené nasledujúce porty: 80-http, 443-htpps.

Partner musí byť zaregistrovaný ako používateľ EKP na www.ekp.posta.sk

SP, a.s. poskytne zdarma klientsku aplikáciu na vytváranie dokumentov dostupnú na webe SP. Pre zabezpečenie inštalácie klientskej aplikácie je potrebná inštalácia nasledovných komponentov: .NET Framework2.0, .NET Framework 3.5, Koreňový certifikát I.CA, D.Singer/XAdES , D.Singer/XAdESXML Plugin.

V prípade používania zaručeného elektronického podpisu je potrebný kvalifikovaný certifikát od niektorej z akreditovaných certifikačných autorít

3. Prehľad podmienok pre jednotlivé varianty komunikácie

Komunikácia prostredníctvom	Verejný internet	Prenajatý okruh	VPN klient	Aktívny prvok s podporou IPSec	Kryptovanie dát	Externý klient	Zaručený elektronický podpis
VPN klient	**A**		**A**		**A**		
IPSec tunel	**A**			**A**	**A**		
Prenajatý okruh		**A**			**A**		
Elektronický komunikačný portál	**A**					**A**	**A (len pre podaj)**