1 Architektúra riešenia

Z dôvodu rozdielneho spôsobu pripojenia je IT riešenie pre elektronickú komunikáciu medzi Objednávateľom (ďalej len „Municipality“ alebo „Obec“ a bankami logicky aj fyzicky rozčlenené do dvoch celkov:

- Webový portál Objednávateľa (ďalej aj ako „Web portál Municipalít“), prostredníctvom ktorého je zabezpečené pripojenie a elektronická komunikácia zo strany Obce,
- Dátový uzol bánk, do ktorého sú pripojené všetky Banky, ktoré sa aktívne zúčastňujú projektu.

Každá Obec, ktorá bude využívať IT riešenie pre elektronickú komunikáciu medzi obcami a bankami, bude pripojená/á k Webovému portálu Municipalít prevádzkovanému CRIF SK.

Pre pripojenie bude využívať verejnú internetovú linku. Po pripojení a autentifikácii prihlasovacích údajov Obec zasiela prostredníctvom zabezpečeného pripojenia (HTTP so šifrovaným SOAP obsahom) na Webový portál Municipalít Žiadosť alebo Príkaz Banke, alebo viacerým určeným Bankám, v štruktúre podľa Prílohy č.1 a Prílohy č. 2.

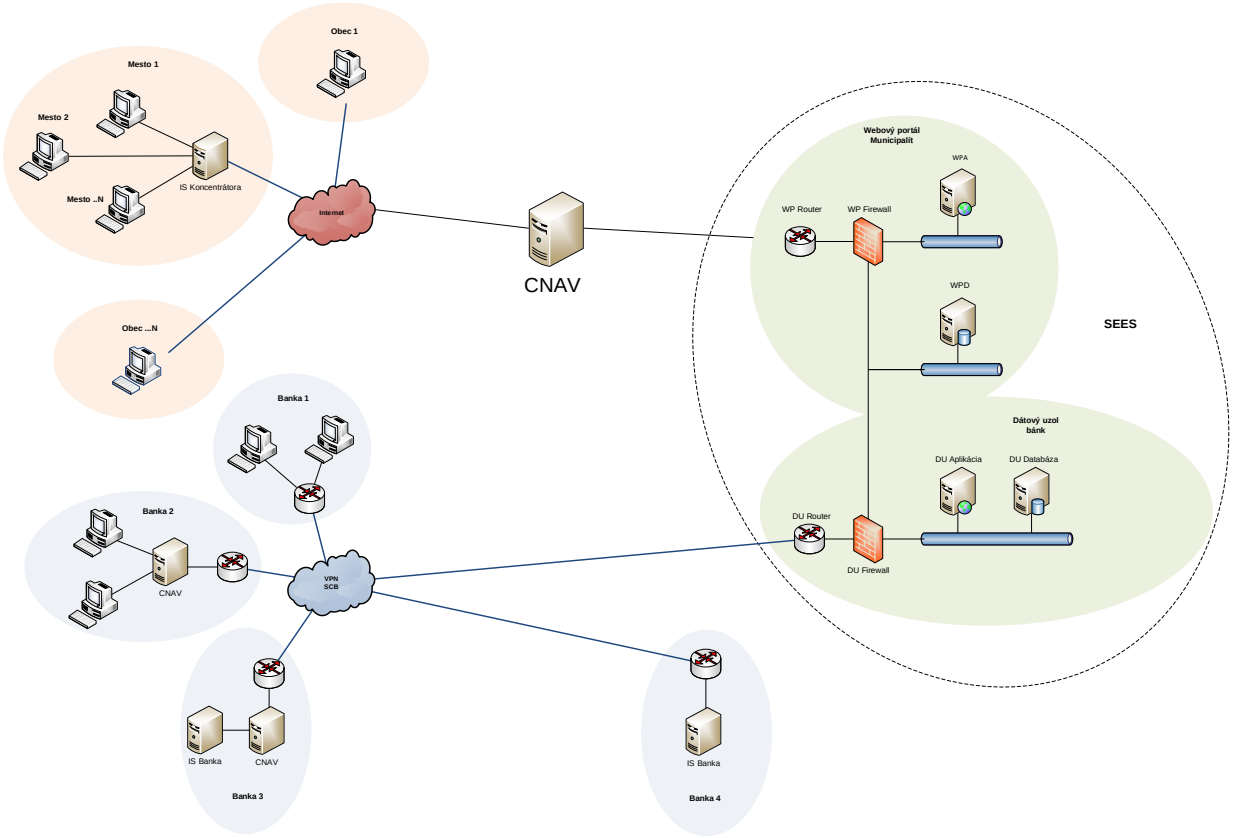
Webový portál Municipalít spracuje Žiadosť alebo Príkaz a automaticky odošle Obci potvrdenie prevzatia, prípadne chybovú správu. Žiadosť a Príkaz sú následne prenesené do Dátového uzla bánk.

Banka bude pripojená do Dátového uzla bánk už existujúcou privátnou linkou používanou pre komunikáciu so Spoločným registrom bankových informácií (SRBI) a so Sociálnou poisťovňou (SIC).

Po pripojení na Dátový uzol bánk a autentifikácii prihlasovacích údajov banky si Banka prostredníctvom zabezpečeného pripojenia vyzdvihne Žiadosť alebo Príkaz zaslaný Obcou.

Následne po spracovaní Žiadosti odosiela obdobným spôsobom Informáciu ako odpoveď na Žiadosť na Dátový uzol bánk. Táto Informácia je presunutá na Webový portál Municipallít, kde je sprístupnená cieľovému adresátovi, ktorý si ju po pripojení vyzdvihne. Týmto spôsobom sú Obci sprístupnené všetky Informácie od Banky, alebo Bánk, ktorým adresoval Žiadosť.

Príloha č.3 Zmluvy o spolupráci a technickej podpore
Architektúra IT riešenia



WP Webový portál Municipalít
WPA aplikačný server WP, umožňuje komunikáciu Obcí cez webovú službu
WPD databáza WP, slúži na výmenu dát medzi zónami WP a DU

DU Dátový uzol bánk
DUA aplikačný server DU, umožňuje komunikáciu Bánk cez webovú službu
DUD databáza DU v ktorej sú uložené prenášané správy (t.j. Žiadosti, Informácie a Príkazy), certifikáty s verejnými kľúčmi klientov (t.j. Obcí a Bánk) a prístupové oprávnenia klientov
CNAV Credit navigator - aplikácia/rozhranie umožňujúce komunikáciu klienta (Obce)

Uvedené skratky sú použité v ďalšom texte.

1.1 Možnosti pripojenia klientov

Klientom je spoločnosť (Obec alebo Banka) jednoznačne identifikovaná menom, heslom a certifikátom.. Každá banka ma pridelený jeden prístup. Obce maju pridelený v Systéme jeden prístup, ďalej sa rozlišujú podľa identifikátora v CNAV. Identifikátor je zároveň kódom (viď 1.2.2) pobočky/skupiny, ktorú má Obec pridelenú. Počet používateľov pobočky/skupiny nie je obmedzený.

Obce => CNAV

a. Obce sa budú pripájať cez web rozhranie CNAV na www.sees-obce.sk. Prihlasujú sa prideleným menom/heslom.
b. Koncentrátori veľkých miest a obcí môžu komunikovať cez A2A www.sees-obce.sk/a2a

CNAV => Webový portál Municipalít

- V CNAV sa Žiadosť/Príkaz zašifrujú a podpíšu CRIF SK komerčným certifikátom,
- CNAV následne odošle Žiadosť/Prikaz do Webového portálu Municipalít

Banka

IS Banky komunikuje cez privátnu linku s webovou službou Dátového uzla HTTP protokolom so šifrovaným SOAP obsahom

1.2 Bezpečnostné aspekty

Výmena dát medzi zónami „Webový portál Municipalít“ (WP) a „Dátový uzol bánk“ (DU) prebieha jednosmerne zo strany DU. Komunikačná služba DUA sa dopytuje na nové požiadavky WP a ukladá zasielané správy. Neexistuje žiadny aktívny prístup smerom WP – DU.

Klient je pri komunikácii vždy overený prihlasovacím menom, heslom a certifikátom.

Komunikácia je zabezpečená - zasielané dáta sú šifrované od chvíle vytvorenia spojenia klient – server a nie je možné ich zneužiť.

1.2.1 Certifikáty

Každý účastník (Banka) elektronickej komunikácie (vrátane serverov WPA, DUA, DUD) používa vlastný certifikát, ktorý je vydaný a ktorého podmienky používania sú definované na základe samostatnej zmluvy medzi účastníkmi elektronickej komunikácie a certifikačnou autoritou. Za bezpečnú manipuláciu a ochranu privátneho kľúča je zodpovedný jeho držiteľ, rovnako ako zodpovedá za prípadné škody spôsobené porušením tejto povinnosti.

Obce ako účastníci elektronickej komunikácie používajú komerčný certifikát vydaný pre CRIF SK, a ktorého podmienky používania sú definované na základe samostatnej zmluvy medzi účastníkmi elektronickej komunikácie a certifikačnou autoritou. Za bezpečnú manipuláciu a ochranu privátneho kľúča je zodpovedný jeho držiteľ, rovnako ako zodpovedá za prípadné škody spôsobené porušením tejto povinnosti.

Certifikáty zabezpečujú:

- dôvernosť informácií - neautorizované subjekty nemajú možnosť prístupu k dôverným informáciám
  - autentifikácia klienta
  - šifrovanie obsahu správ
- integritu - informácie sú zabezpečené voči neautorizovanej modifikácii digitálnym podpisom založeným na PKI (ďalej len „digitálny podpis“).

Klient - Banka môže použiť samostatné certifikáty pre autentifikáciu počas nadväzovania spojenia a podpisovanie/šifrovanie obsahu správ.

Systém umožňuje:

- evidenciu certifikátov s verejnými kľúčmi,
- zaevidovanie nového certifikátu vo fáze obnovy,
- označenie certifikátu ako neplatného na žiadosť klienta (technické problémy, diskreditácia certifikátu).

Certifikáty s verejnými kľúčmi sú evidované na DUD a replikované na WPD pre zabezpečenie funkcií:

- zaslanie jednoznačného identifikátora certifikátu požadovaného klienta

- zaslanie certifikátu podľa požadovaného jednoznačného identifikátora

Potrebné certifikáty si Banky a CRIF SK zabezpečia v spoločnosti D. Trust Certifikačná Autorita, a.s., (DTCA) - výhradný poskytovateľ certifikačných služieb akreditovanej certifikačnej autority První certifikační autorita, a.s., Praha (I.CA) v Slovenskej republike.
Typ certifikátu – osobný komerčný certifikát vydaný pre právnickú osobu, HASH algoritmus SHA-2, dĺžka kryptografických kľúčov pre RSA 2048 Bits

Operačné systémy Microsoft a podpora SHA-2 certifikátov

Operačný systém	**Podpora SHA-2**
Windows 7 alebo novší	Áno
Windows Server 2012R2 alebo novší	Áno

Proces vytvorenia žiadosti, vydania a obnovenie platnosti osobného komerčného certifikátu je popísaný na webových stránkach spoločnosti DTCA (www.dtca.sk).
Súkromné kľúče k osobným komerčným certifikátom je možné uchovávať na pevnom disku počítača, prípadne na bezpečnom zariadení pre generovanie a uchovávanie kľúčov.
Certifikáty s verejnými časťami kľúčov sú uložené a udržiavané v DND poverenými pracovníkmi CRIF SK.

Podmienky používania certifikátov sú definované v zmluve medzi účastníkom/držiteľom certifikátu a certifikačnou autoritou

Držiteľ certifikátu je povinný najmä:

a) zaobchádzať so svojim súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k zneužitiu jeho súkromného kľúča,
b) uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,
c) v prípade prezradenia súkromného kľúča druhej osobe je povinný túto skutočnosť bezodkladne oznámiť predpísaným spôsobom certifikačnej autorite a CRIF SK a súčasne vykonať všetky prípustné opatrenia na zamedzenie alebo aspoň obmedzenie vzniku prípadných škôd z dôvodu neoprávneného použitia prostriedku na vytvorenie digitálneho podpisu.

Komunikácia medzi držiteľom certifikátu/účastníkom elektronickej komunikácie a CRIF SK prebieha mailom na základe zoznamu poverených osôb. Pre potvrdenie prijatia správy bude použitý telefonický kontakt a mailom zaslaná informácia kontaktným osobám.

Zrušenie certifikátu

1. držiteľ certifikátu ukončí platnosť certifikátu zaslaním žiadosti do DTCA a zároveň o tejto skutočnosti upovedomí CRIF SK,
2. CRIF SK preverí požiadavku telefonátom osobe ktorá zaslala požiadavku na t.č. uvedené v zozname kontaktných osôb,
3. v prípade potvrdenia požiadavky CRIF SK certifikát bezodkladne zablokuje pre ďalšie použitie v systéme elektronickej komunikácie,
4. CRIF SK bude bezodkladne informovať mailom kontaktné osoby danej spoločnosti o vybavení požiadavky,
5. v prípade zneplatnenia certifikátu bude o tejto skutočnosti CRIF SK bezodkladne informovať všetkých účastníkov elektronickej komunikácie.

Nahlásenie používaného certifikátu:

1. účastník elektronickej komunikácie zašle CRIF SK sériové číslo certifikátu, účel použitia a termín predpokladaného nasadenia,
2. CRIF SK preverí požiadavku,
3. v prípade úspešného preverenia bude certifikát zaevidovaný pre použitie podľa požiadavky,
4. CRIF SKzašle informáciu o vybavení požiadavky.

CRIF SK je povinný kontrolovať dobu platnosti certifikátov.

1.2.2 Prístupy

Obce - zoznam klientov – obcí - s priradenými identifikátormi je vytvorený a aktualizovaný v CNAV. Identifikátor pre danú Obec predstavuje číslo, ktoré identifikuje obec, a ktoré bolo Obci pridelené Štatistickým úradom SR.

CNAV bude mať vytvorené prístupové údaje vo WPD. Priradený identifikátor pre CNAV je vytvorený a aktualizovaný na DUD, replikovaný spoločne s certifikátmi s verejnými kľúčmi na WPD.

Banky – meno, heslo (hash) a certifikát, voči ktorým sa Banka autentifikuje, sú uložené na DUD

1.3 Výmena správ

Komunikáciu môžeme rozdeliť podľa smeru toku dát:

A. Správa zasielaná Bankou
   1. asymetrická kryptografia je použitá na tvorbu digitálneho podpisu a bezpečnú výmenu kľúčov pre symetrickú kryptografiu, ktorá je použitá na vlastné šifrovanie prenášaných údajov,
   2. webová služba potvrdí úspešné uloženie správy,
   3. výmena údajov medzi zónami DU a WP (jednosmerná zo strany DU),
   4. pri úspešnom prevzatí správy Obcou je nastavený príznak „*stav*“ zasielanej správy.

B. Správa zasielaná Obcou cez CNAV Web Interface

   1. Obec sa pripojí cez web rozhranie CNAV na www.sees-obce.sk,
   2. prihlási sa prideleným menom/heslom,
   3. v CNAV vyplná Žiadosť alebo Príkaz a stlači tlačítko pre odoslanie,
   4. CNAV Žiadosť alebo Príkaz na pozadí zašifruje a podpíše CRIF SK komerčným certifikátom a pošle do Webového portálu Municipalít,
   5. asymetrická kryptografia je použitá na tvorbu digitálneho podpisu a bezpečnú výmenu kľúčov pre symetrickú kryptografiu, ktorá je použitá na vlastné šifrovanie prenášaných údajov,
   6. kľúč pre symetrickú kryptografiu je zašifrovaný verejným kľúčom
      a. príjemcu (banka) v prípade, že ide o Príkaz alebo
      b. servera DUD v prípade, že ide o Žiadosť
   7. webová služba potvrdí úspešné uloženie správy,
   8. výmena údajov medzi zónami DU a WP (jednosmerná zo strany DU),

C. Správa zasielaná koncentrátorom veľkých Obcí cez CNAV A2A

1. koncentrátori veľkých Obcí komunikujú cez A2A www.sees-obce.sk/a2a/ prideleným menom/heslom,
2. pošlú Žiadosť alebo Príkaz cez informačný systém ich dodávateľa/koncentrátora,
3. CNAV Žiadosť alebo Príkaz na pozadí zašifruje a podpíše CRIF SK komerčnýmm certifikatom a pošle do Webového portálu Municipalít ,
4. asymetrická kryptografia je použitá na tvorbu digitálneho podpisu a bezpečnú výmenu kľúčov pre symetrickú kryptografiu, ktorá je použitá na vlastné šifrovanie prenášaných údajov,
5. kľúč pre symetrickú kryptografiu je zašifrovaný verejným kľúčom
    a. príjemcu (banka) v prípade, že ide o Príkaz alebo
    b. servera DUD v prípade, že ide o Žiadosť
6. webová služba potvrdí úspešné uloženie správy,
7. výmena údajov medzi zónami DU a WP (jednosmerná zo strany DU).

Webové služby na serveroch WPA a DUA budú dostupné nepretržite mimo plánované technické odstávky a poruchy, príjem správ bude obmedzený podľa vopred dohodnutých časov prevádzky. Počas neskorých nočných hodín prebieha denne údržba a systém môže byť čiastočne neresponzívny.

Na Architektúru riešenia nadväzuje Technická dokumentácia, ktorá bude súčasťou zmluvnej dokumentácie.