НАРОДНА БАНКА НА РЕПУБЛИКА МАКЕДОНИЈА

Верзија 3.0.2

НАЧИН НА ПРЕНЕСУВАЊЕ НА ПОРАКИ ВО МИПС

БРОЈ 2

Пренесување на пораки согласно Одлуката за поврзувањето со информатичкиот систем на Народната банка на Република Македонија

Август 2014 година

Пренесување на пораки согласно Одлуката за поврзувањето со информатичкиот систем на Народната банка на Република Македонија

Учесникот кој за пренесување пораки во МИПС го користи овој начин на пренесување треба да обезбеди:

- еден BIC код;
- еден или повеќе логички терминали;
- еден или повеќе регистрирани корисници за секој логички терминал;
- соодветни телекомуникациски приклучоци;
- користење на дефиниран протокол;
- хардвер и
- софтвер.

При тоа треба да ги употребува и форматира пораките согласно со Стандардот за намената и форматот на пораките во МИПС, даден како посебен документ.

Со одбирањето на овој начин на пренесување на пораки учесникот се согласува дека:

- сите пораки кои ќе пристигнат од неговиот логички терминал во МИПС и ќе го содржат неговиот електронски потпис се валидни;
- сите пораки кои ќе ги прими на својот логички терминал од BIC адресата на МИПС со валиден електронски потпис на МИПС ќе ги процесира како валидни, согласно со Стандардот за намената и форматот на пораките во МИПС.

Валиден електронски потпис претставува низа од знаци во пораката која проверена со средството за проверка на електронскиот потпис дава потврден одговор.

I. BIC код на Учесникот

BIC кодот на Учесникот се состои од 11 знаци. Првите 8 знаци се единствени за секое правно лице, а последните 3 знаци се однесуваат на организационата единица во рамки на правното лице која настапува како посебен учесник. BIC кодот на Учесникот мора да биде регистриран на име на правното лице.

II. Логички терминал на Учесникот

Логичкиот терминал на Учесникот се состои од 12 знаци. Првите 8 знаци се првите 8 знаци од BIC кодот на Учесникот, деветтиот знак е кодот на логичкиот терминал на Учесникот и последните 3 знаци се последните 3 знаци од BIC кодот на Учесникот. Во случаите кога се работи за основниот BIC код на учесникот последните три знаци се: "XXX". Кодот на логички терминал е секогаш "A", освен кога поради потребата на работата од страна на МИПС не се доделат и кодови на наредните логички терминали: "B", "C", "D" итн.

За секој логички терминал Учесникот добива лозинка од Службеникот за сигурност на МИПС.

Службеникот за сигурност на МИПС од страна на Учесникот е должен со употреба на апликацијата KeyManager опишана во глава VII.1 на овој документ да генерира еден пар од јавен и таен електронски клуч за секој логички терминал.

Службеникот за сигурност на МИПС од страна на Учесникот е должен да го чува тајниот клуч на сигурно место. Секој електронски потпис генериран со овој таен клуч ќе се смета за валиден.

Службеникот за сигурност на МИПС од страна на Учесникот е должен да го достави јавниот клуч до службеникот за сигурност на МИПС во Народна банка на Република Македонија. Службеникот за сигурност на МИПС го сертифицира доставениот јавен клуч и му го враќа на Учесникот. Сертифицираниот јавен клуч ќе се користи за проверка на електронскиот потпис на влезните пораки во МИПС и шифрирање на излезните пораки до Учесникот.

При сертифицирањето на јавниот клуч на Учесникот службеникот за сигурност во МИПС на Службеникот за сигурност на МИПС од страна на Учесникот ќе му ги достави јавниот сертифициран клуч на МИПС и јавниот клуч за проверка на сертификатите.

Учесникот е должен да ги шифрира сите влезни пораки со јавниот сертифициран клуч на МИПС пред нивното праќање во МИПС и да ја проверува валидноста на електронскиот потпис на МИПС на излезните пораки добиени од МИПС. Во случај ако потписот на пораката не одговара на јавниот сертифициран клуч на МИПС Учесникот е должен веднаш да го извести Службеникот за сигурност во МИПС.

Учесникот е должен да ги постави јавните и тајните клучеви за електронско потпишување и шифрирање, како и лозинката за пристап на МИПС во соодветното место во конфигурационите параметри на апликациите опишани во глава VI на овој документ, во согласност со Упатството за користење на соодветната апликација.

За секоја активност на Службеникот за сигурност на МИПС од страна на Учесникот одговара Учесникот и Народна банка на Република Македонија не презема одговорност за извршување на инструкциите на Службеникот за сигурност на МИПС од страна на Учесникот.

III. Регистрирани корисници кај Учесникот

Учесникот е должен да регистрира барем еден корисник за секој логички терминал. Учесникот може да регистрира неограничен број на корисници за секој логички терминал. Името на секој корисник се содржи од првите 4 знаци на BIC кодот на Учесникот и потоа уште максимум 8 знаци кои не смее да завршуваат со "XXX".

За потпишување секој корисник мора да генерира свој пар клучеви (јавен и таен клуч) и при тоа јавниот клуч треба да биде пријавен кај Службеникот за сигурност во МИПС и сертифициран од него.

Корисникот од страна на Учесникот е должен да го чува тајниот клуч на сигурно место. Секој електронски потпис генериран со овој таен клуч ќе се смета за валиден.

Корисникот е должен самостојно или преку Службеникот за сигурност на МИПС од страна на Учесникот да го достави јавниот клуч до службеникот за клучеви во МИПС во Народна банка на Република Македонија. Службеникот за сигурност во МИПС го сертифицира доставениот јавен клуч и му го враќа на доставувачот. Сертифицираниот јавен клуч ќе се користи за проверка на електронскиот потпис на влезните пораки во МИПС. Сопственикот на тајниот клуч е должен да провери дали соодветниот јавен клуч е сертифициран од страна на Службеникот за сигурност во МИПС од страна на Народна банка на Република Македонија со валиден сертификациски клуч. Информациите за сертификацискиот клуч може да се добијат на барање директно кај службеникот за клучеви во МИПС или да се превземат од официјалната Интернет страна на Народна банка на Република Македонија.

Еден од регистрираните корисници кај Учесникот мора да ја потпише секоја влезна порака пред таа да се потпише со тајниот клуч на логичкиот терминал на Учесникот од глава XI на овој документ.

МИПС проверува дали електронскиот потпис одговара на документот кој е пратен со примена на јавните клучеви на регистрираните корисници на Учесникот и ако не одговара документот не го процесира.

IV. Поврзување

Учесникот се поврзува согласно Одлуката за поврзувањето со информатичкиот систем на Народната банка на Република Македонија.

V. Протокол за мрежата

Како протокол на мрежата се користи IP (Internet Protocol). Комуникацијата се одвива на строго дефинирани порти со примена на транспортните протоколи: TCP и UDP.

VI. Хардвер

VI.1. Комуникациска опрема

- Учесникот е должен да обезбеди комуникациска опрема со која ќе ги оствари бараните поврзувања согласно глава IV од овој документ.

VI.2. Компјутер

Компјутер кој има инсталиран еден од следните оперативни системи:

- Windows 2003 Server (може да се користи до 14.7.2015 година, кога завршува поддршката за него од Microsoft);
- Windows 2008 Server;
- Windows 2008 R2 Server;
- Windows Vista;
- Windows 7;
- Windows 8 и
- Windows 8.1.

Компјутерот не смее да се користи за други намени, освен со писмена дозвола на Народна банка на Република Македонија. Дозволата се издава на барање на Учесникот во кое тој точно треба да наведе за каков компјутер се работи и кои други апликации ќе се користат. Доколку истите не претставуваат оптоварување и не го зголемуваат ризикот за работата, Народна банка на Република Македонија може да издаде дозвола за користење на други апликации. Со издавањето на таа дозвола Народна банка на Република Македонија не го превзема ризикот од користењето на другите апликации и ефектите кои тие може да ги имаат на перформансите и сигурноста на врската на Учесникот со МИПС туку за истиот одговара Учесникот.

Опремата опишана во глава VI.1 и VI.2 на овој документ е минимална опрема со која секој Учесник може да се приклучи на МИПС на овој начин. Учесникот може да обезбеди и уреди со подобри карактеристики. Исто така Учесникот е должен да обезбеди доволна опрема опишана во глава VI.1 и VI.2 на овој документ за да го обезбеди континуитетот на своето работење.

VII. Софтвер

За комуницирање со МИПС на овој Начин на пренесување Народна Банка на Република Македонија на Учесниците им доставува софтвер за комуникација кој праќа и прима пораки во определен формат. За составување на пратените пораки и процесирањето на примените пораки е одговорен Учесникот. За таа цел тој треба да обезбеди софтвер кој ќе се надогради на клиентската комуникациска компонента.

Од Народна Банка на Република Македонија секој Учесник ги добива следниве апликации:

- Key Manager;
- SWIFT Validator;
- Simple Checker и
- Клиентска комуникациска компонента (RSC компонента).

Учесникот е должен да ја користи последната верзија на апликациите доставена од Народна Банка на Република Македонија.

Подетални информации за инсталирањето, конфигурирањето и употребата на секоја од овие апликации може да се најдат во упатството за користење на соодветната апликација кое се доставува со самата апликација.

Учесникот се обврзува да не ги менува апликациите, да не ги користи за други цели освен за поврзување со МИПС и да не ги дистрибуира на трети лица.

VII.1. Key Manager

Оваа апликација служи за генерирање на пар на електронски клучеви за логичкиот терминал на Учесникот и за корисниците кај Учесникот и за проверка на сертификатот на клучевите.

Во МИПС може да се користат само клучеви сертифицирани од Службеникот за сигурност во МИПС од страна на Народна банка на Република Македонија.

VII.2. SWIFT Validator

Оваа апликација служи за проверка на форматот на пораките согласно со страндардите на МИПС.

VII.3. Simple Checker

Оваа апликација има две намени:

- потпишување на влезните пораки со тајниот клуч на корисникот кај Учесникот и
- проверка на електронски потписи на пораки.

Оваа апликација претставува средство за електронско потпишување и средство за проверка на електронски потпис.

Кога се користи како средство за електронско потпишување оваа апликација за влезни параметри има:

- таен клуч на корисникот кај Учесникот (чиј јавен клуч од истиот пар е сертифициран кај Службеникот за клучеви во МИПС) и
- исправна порака согласно со Стандардот за намената и форматот на пораките во МИПС.

При добивањето на овие податоци се генерира порака која е автентична со влезната порака, но со дополнување на електронскиот потпис на корисникот кај Учесникот.

Кога се користи како средство за проверка на електронски потпис оваа апликација како влезен параметар има јавни клучеви на можните потписници и потпишана порака, а како излез се прикажува податок за тоа КОЈ го потпишал документот од можните потписници или дека потписот не е исправен.

VII.4. Клиентска комуникациска компонента (RSC компонента)

Оваа апликација служи за комуникација помеѓу Учесникот и МИПС. Таа треба да биде правилно конфигурирана со лозинката на логичкиот терминал на Учесникот, тајниот клуч на логичкиот терминал на Учесникот, јавниот сертифициран клуч на МИПС, јавниот клуч за сертифицирање и параметрите за протокол на мрежата. Има две намени:

1. Да ја прати влезната порака при што ќе ја потпише со тајниот клуч на логичкиот терминал на Учесникот и ќе ја шифрира со јавниот сертифициран клуч на МИПС и
2. Да ги прими излезните пораки, да ги дешифрира со тајниот клуч на логичкиот терминал на Учесникот и да го провери електронскиот потпис со јавниот сертифициран клуч на МИПС.

Оваа апликација претставува средство за електронско потпишување и средство за проверка на електронски потпис.

Може да се користи на два начини:

1. Со пренесувањето на датотеки (FILE ADAPTER) - каде податоците се креираат во датотека, која потоа се сместува во одреден фолдер и со помош на оваа апликација автоматски се пренесува во МИПС.

Датотеката треба да е во согласност со пропишаниот Стандард за намената и форматот на пораките во МИПС за да биде пренесена;
или

2. Користење на API функции кои се достапни како COM компонента. За нивно користење Учесникот во МИПС треба да обезбеди софтвер кој ги користи овие функции. Во Упатството за користење на Клиентската комуникациска компонента се доставени документи кои треба да се користат за изготвување на софтвер за комуникација.

Клиентската комуникациска компонента обезбедува постојана врска со МИПС. Учесникот е должен да биде постојано приклучен на МИПС системот. Евентуалните прекини не смее да бидат подолги од 30 минути.

VII.5. Пренесување на пораки помеѓу учесникот и МИПС системот

VII.5.1. Пренесување на датотеки со апликацијата FILE ADAPTER

VII.5.1.1. Праќање на датотеки кон МИПС системот

Учесникот испраќа датотеки кон МИПС системот кои се форматирани во XML формат. Блокот 4 на пораките е електронски потпишан со тајниот клуч на корисникот кај Учесникот и целата порака е потпишана со тајниот клуч на логичкиот терминал на Учесникот. Апликацијата FILE Adapter пред испраќањето на датотеката кон МИПС системот прави резервна копија на датотеката во работен фолдер во кој се чуваат сите испратени датотеки кон МИПС системот (пример: OutArc).

Во овој работен фолдер апликацијата FILE Adapter ја запишува и датотеката форматирана во XML формат која претставува позитивна потврда за пренос - АСК или негативна потврда за пренос - NAK на испратената датотека. Содржината на потврдите за пренос на испратената датотека се потпишува со тајниот клуч на МИПС системот. Форматот и содржината на потврдите за потврдата за пренос на испратените датотеки кон МИПС системот се пропишани во Стандардот за намената и форматот на пораките во МИПС.

За успешно испратена датотека кон МИПС системот се смета датотеката за која од МИПС системот е добиена позитивна потврда за пренос - АСК која ја содржи МИР референцата на пораката. Учесникот не може да се повикува на оние пораки за кои нема потврда (АСК) од МИПС системот.

VII.5.1.2. Прием на датотеки од МИПС системот

Учесникот прима датотеки од МИПС системот кои се форматирани во XML формат и електронски потпишани со тајниот клуч на МИПС системот. Апликацијата FILE Adapter при приемот на датотеката од МИПС системот прави резевна копија на датотеката во работен фолдер во кој се чуваат сите примени датотеки од МИПС системот (пример: InArc).

Во овој работен фолдер апликацијата FILE Adapter ја запишува и датотеката форматирана во XML формат која претставува позитивна потврда за пренос - АСК или негативна потврда за пренос - NAK која е испратена до МИПС системот. Содржината на потврдата за пренос на примената датотека се потпишува со тајниот клуч на Учесникот. Форматот и содржината на потврдата за пренос на примените пораки од МИПС системот се пропишани во Стандардот за намената и форматот на пораките во МИПС.

За успешно примена порака од МИПС системот се смета пораката за која од страна на учесникот е добиена позитивна потврда за пренос - АСК која ја содржи МИР референцата на пораката. Во случај кога за примената порака од МИПС системот учесникот генерира негативна потврда за пренос - NAK или воопшто не генерира потврда за пренос МИПС системот ќе ја испраќа пораката повторно се до добивањето на позитивна потврда за прием - АСК од страна на учесникот и ќе се смета дека пораката не е пратена од МИПС системот до Учесникот.

VII.5.2. Пренесување на пораки со користење API функции кои се достапни како COM компонента

Софтверското решение на страна на учесникот со помош на API функциите треба да ги обезбеди следниве можности:

- поврзување на МИПС системот;
- форматирање на пораките во XML формат;
- потпишување на блокот 4 од пораките со тајниот клуч на корисникот кај Учесникот;
- потпишување на пораките со тајниот клуч на логичкиот терминал на Учесникот;
- правење резевна копија на испратената порака во формат на датотека која треба да биде форматирана во XML формат и треба да ги содржи сите елементи на испратената порака;
- успешно завршување на функциите за праќање на порака кон МИПС системот т.е. размена на позитивна потврда за прием - АСК за испратените пораки помеѓу учесникот и МИПС системот;

- шифрирање/дешифрирање на пратените/приемните пораки со јавниот клуч на МИПС системот;
- успешно завршување на функциите за прием на пораките од МИПС системот т.е. размена на позитивни потврда за прием - АСК за пораките помеѓу МИПС системот и учесникот;
- правење резервна копија на примените пораки во формат на датотека.

За успешно испратена порака кон МИПС системот се смета порака за која од МИПС системот е добиена потврда за прием - АСК која ја содржи МИР референцата на пратената порака. Учесникот не може да се повикува на оние пораки за кои нема потврда (АСК) од МИПС системот.

За успешно примена порака од МИПС системот се смета пораката за која од страна на учесникот е добиена позитивна потврда за пренос - АСК која ја содржи МИР референцата на пораката. Во случај кога за примената порака од МИПС системот учесникот генерира негативна потврда за пренос - NAK или воопшто не генерира потврда за пренос, МИПС системот ќе ја испраќа пораката повторно, се до добивањето на позитивна потврда за прием - АСК од страна на учесникот и ќе се смета дека пораката не е пратена од МИПС системот.