



mTransfer

Technická dokumentácia

Pre externých partnerov



Obsah

1 SLOVNÍK POJMOV	3
2 ÚVOD	4
3 OPIS RIEŠENIA.....	4
4 SPÔSOB INICIALIZÁCIE PLATBY EXTERNÝM PARTNEROM	4
4.1 Formát odosielanej požiadavky http pri inicializácii.....	4
4.2 Formát dát.....	4
4.3 Formát nakódovaného objektu	5
4.4 Vzorový komunikát.....	5
5 NÁVRAT ZÁKAZNÍKA PO UKONČENOM PROCESE PLATBY	5
5.1 Formát odoslanej žiadosti HTTP počas návratu.....	5
5.2 Formát dát návratu	5
5.3 Vzorový komunikát.....	6
6 KONFIGURÁCIA SLUŽBY.....	6
6.1 Požiadavky na verejný kľúč a podpis	6
7 KONFIGURÁCIA CERTIFIKÁTOV V IB	6



1 Slovník pojmov

mTransfer	Funkcionalita (služba), ktorú poskytuje mBank, ktorá umožňuje zákazníkom zúčtovať platby bankovým prevodom z vyhradeného formulára umiestneného na internetovej stránke externého podnikateľského subjektu. Formulár presmeruje používateľa na internetovú stránku banky
Klient	Osoba, ktorá má vedený účet v mBank a využíva službu mTransfer na zaplatenie externému podnikateľskému subjektu za služby / tovar.
Externý partner	Subjekt (predávajúci, poskytovateľ služieb, charitatívna inštitúcia atď.) S registrovanou službou mTransfer, v prospech ktorého zákazníci prevádzajú peniaze pomocou služby mTransfer.
Pozitívne vykonanie služby mTransfer klientom	Správne vykonanie prevodu peňažných prostriedkov.
Negatívne vykonanie služby mTransfer klientom	Nesprávne vykonanie prevodu peňažných prostriedkov (napr. Zadanie nesprávneho čísla TAN) alebo prerušenie prenosu výberom možnosti odhlásenia alebo zrušenia Poznámka: prerušenie prevodu zatvorením prehliadača nie je považované za negatívny prípad; takáto udalosť nebude zaregistrovaná v systéme NPM.
IB	Internet banking



2 Úvod

mTransfer je služba od mBank, ktorá umožňuje externým subjektom umiestniť na svoje webové stránky formulár presmerovania do systému banky. Ak má zákazník v mBank účet, toto presmerovanie umožňuje zákazníkovi uskutočniť platbu bankovým prevodom na účet externého subjektu - majiteľa služby.

Tento dokument popisuje súčasnú funkčnosť mTransferu, predstavuje spôsob prevádzky riešenia a prezentuje informácie potrebné na implementáciu tohto mechanizmu na strane externého subjektu.

3 Opis riešenia

mTransfer je funkcionalita, ktorá umožňuje externej spoločnosti s účtom v mBank umiestniť na svojej web stránke formulár, ktorý umožní zákazníkovi (ktorí majú účet taktiež v mBank) okamžitú úhradu za službu alebo tovar.

Všeobecná prevádzka mTransferu je nasledovná:

1. Pri rozhodovaní o kúpe tovaru/služby na webovej stránke externej strany si zákazník zvolí spôsob platby prostredníctvom platobného tlačidla mTransfer a partner (predajca služby) presmeruje zákazníka na internetovú stránku banky. Pri presmerovaní na webovú stránku banky sa prenášajú parametre umožňujúce prenos a súčasne podpis RSA.
2. Klient sa prihlási do banky pomocou svojho účtu a potom uskutoční platbu.
3. Po úspešnom dokončení transakcie je zákazník presmerovaný naspäť na webovú stránku partnera na adresu definovanú v nastaveniach kladného prípadu.
4. Ak po prihlásení si klient vyberie možnosť "zrušiť", bude presmerovaný na určenú adresu uloženú v nastaveniach pre negatívny prípad.

Podrobný opis požiadaviek a hlásených parametrov nájdete v nasledujúcich častiach.

4 Spôsob inicializácie platby externým partnerom

Aby externý partner umožnil klientom platiť prostredníctvom služby mTransfer, musí implementovať riešenie popísané nižšie.

4.1 Formát odosielanej požiadavky http pri inicializácii

```
POST https://mtransfer.mbank.pl/api/mtransfer/initialize <\n>  
Content-Type: aplikace / x-www-form-urlencoded <\n>  
Dĺžka obsahu: <DATA_LENGTH> <\n>  
<\n>  
<DATA> <\n>  
<\n>
```

Kde:

<DATA_LENGTH> Dĺžka dát formulára podľa protokolu HTTP
<DATA> dáta formulára vo formáte opísanom v sekcii 4.2 Formát dát
<\n> znak konca riadku

4.2 Formát dat

Správa musí obsahovať dve polia, ktorých opis je uvedený v nasledujúcej tabuľke.

Názov poľa	Opis
Content	Pole je objekt v notácii JSON zakódovanej v BASE64. Opis polí, ktoré musia / možno nájsť, je v sekcii Kódovanie kódovaného objektu.
Signature	Podpis obsahu poľa Content partnera so súkromným kľúčom a verejnou časťou musí byť pridelený danej službe. Popis konfigurácie nájdete v kapitole 7.

Požiadavky na podpis:

- Formát ASCII Armor z RFC 4880 zo sekcie 5.2
- RSA podpisový algoritmus
- Sha256 hash algoritmus
- verejný kľúč musí byť k dispozícii banke a musí spĺňať požiadavky uvedené v kapitole 7



5.2 Formát dat návratu

Komunikát musí obsahovať polia, ktorých opis sa nachádza v tabuľke nižšie:

Názov poľa	Opis
ServiceId	ID služby, s ktorou je platba prepojená
Properties	Obsah poľa "Properties" z inicializačného komunikátu, nachádzajúceho sa v poli „Content“

5.3 Vzorový komunikát

POST <https://mbank.pl/return/positive>

accept: */*

accept-encoding: gzip, deflate

cache-control: no-cache

content-type: application/x-www-form-urlencoded

properties=%7B+%22sessionId%22%3A+%221234%22%2C+%22orderId%22%3A+%221234%22%7D&serviceId=42519950

6 Konfigurácia služby

Aby služba fungovala správne, je potrebné odoslať do mBank verejný kľúč, ktorý umožní overenie podpisu. Verejný kľúč je potrebné zaslať na nasledujúcu adresu: Andrzej.Ksiazek@mbank.pl s informáciou, ku ktorej službe ServiceId sa vzťahuje.

6.1 Požiadavky na verejný kľúč a podpis

Verejný kľúč, ktorý má banka použiť počas inicializácie prevodu, musí spĺňať nasledujúce požiadavky.

Kontrolujú sa nasledujúce parametre:

- 1) Aktívne kľúč (z pohľadu OpenPGP)
- 2) Dátum skončenia platnosti (či platnosť certifikátu uplynula)
- 3) Dátum vytvorenia (v budúcnosti sa nedá vytvoriť)
- 4) Dĺžka platnosti (nepovoľujeme certifikáty na dobu neurčitú)
- 5) Bitová sila šifrovania / dĺžka kľúča (certifikát musí byť minimálne 2048 bitov)
- 6) Typ algoritmu použitý na generovanie (povolený len RSA)

Podpis musí byť vykonaný pomocou kľúča, ktorý je spárovaný s daným ID služby. Povolený algoritmus hash-ovania je sha256.

7 Konfigurácia certifikátov v IB

Po prihlásení sa do internet bankingu je možné prehliadať si doručené certifikáty a ich dodatočnú konfiguráciu. Po kliknutí na "Nastavenia" a následne dlaždicu "mTransfer" sa zobrazí zoznam certifikátov s priradenými službami.

K dispozícii sú nasledujúce možnosti:

- 1) Pridanie certifikátu,
- 2) Modifikácia certifikátu:
 - a) Pripojenie registrovanej služby k danému certifikátu,
 - b) odpojenie služby od daného certifikátu.
- 3) Odstránenie certifikátu (vrátane vymazania expirovaných certifikátov).

UPOZORNENIE!

K jednej službe mTransfer (identifikovanej ServiceID) je možné pripojiť maximálne 3 certifikáty.