



mTransfer

Technická dokumentace

Pro externí partnery



Obsah

1 SLOVNÍK POJMŮ	3
2 ÚVOD	4
3 POPIS ŘEŠENÍ	4
4 ZPŮSOB INICIALIZACE PLATBY EXTERNÍM PARTNEREM	4
4.1 Formát odesílané požadavky http při inicializaci	4
4.2 Formát dat	4
4.3 Formát kódovaného objektu	5
4.4 Vzorová zpráva	5
5 NÁVRAT ZÁKAZNÍKA PO UKONČENÉM PROCESU PLATBY	5
5.1 Formát odeslané žádosti HTTP během návratu	5
5.2 Formát dat návratu	5
5.3 Vzorová zpráva	6
6 KONFIGURACE SLUŽBY	6
6.1 Požadavky na veřejný klíč a podpis	6
7 KONFIGURACE CERTIFIKÁTŮ V IB	6



1 Slovník pojmů

mTransfer	Funkcionalita (služba), kterou poskytuje mBank, která umožňuje zákazníkům zúčtovat platby bankovním převodem z vyhrazeného formuláře umístěného na internetové stránce externího podnikatelského subjektu. Formulář přesměruje uživatele na internetovou stránku banky
Klient	Osoba, která má vedený účet v mBank a využívá službu mTransfer na zaplacení externímu podniku za služby / zboží.
Externí partner	Subjekt (prodejce, poskytovatel služeb, charitativní instituce atd.) S registrovanou službou mTransfer, v jehož prospěch zákazníci převádějí peníze pomocí služby mTransfer.
Pozitivní provedení služby mTransfer klientem	Správné provedení převodu peněžních prostředků
Negativní provedení služby mTransfer klientem	Nesprávné provedení převodu peněžních prostředků (např.: Zadání nesprávného čísla TAN) nebo přerušení převodu výběrem možností odhlášení nebo zrušení. Poznámka: přerušení převodu zavřením prohlížeče není považováno za negativní případ; taková událost nebude zaregistrována v systému NPM.
IB	Internetové bankovníctví



2 Úvod

mTransfer je služba od mBank, která umožňuje externím subjektům umístit na své webové stránky formát přesměrování do systému banky. Pokud má zákazník v mBank účet, toto přesměrování umožňuje zákazníkovi provést platbu bankovním převodem na účet externího subjektu - majitele služby.

Tento dokument popisuje současnou funkčnost mTransfer, představuje způsob provozu řešení a prezentuje informace potřebné pro provádění tohoto mechanismu na straně externího subjektu.

3 Popis řešení

mTransfer je funkcionalita, která umožňuje externí společnosti s účtem v mBank umístit na své webové stránce formulář, který umožní zákazníkům (kteří mají účet také v mBank) okamžitou úhradu za službu nebo zboží.

Obecný provoz služby mTransfer je následující:

1. Při rozhodování o koupi zboží /služby na webové stránce externí strany si zákazník zvolí způsob platby prostřednictvím platebního tlačítka mTransfer a partner (prodejce služby) přesměruje zákazníka na internetovou stránku banky. Při přesměrování na webovou stránku banky se přenášejí parametry umožňující přenos a současně podpis RSA.
2. Klient se přihlásí do banky pomocí svého účtu a pak uskuteční platbu.
3. Po úspěšném dokončení transakce je zákazník přesměrován zpět na webovou stránku partnera na adresu definovanou v nastavení kladného případu.
4. Pokud klienta po přihlášení zvolí "zrušit", bude přesměrován na určenou adresu uloženou v nastavení pro negativní případ.

Podrobný popis požadavků a hlášených parametrů naleznete v následujících částech.

4 Způsob inicializace platby externím partnerem

Aby externí partner umožnil klientům platit prostřednictvím služby mTransfer, musí implementovat řešení popsané níže.

4.1 Formát odesílané požadavky http při inicializaci

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

Kde:

<DATA_LENGTH> Délka dat formuláře podle protokolu HTTP

<DATA> data formuláře ve formátu popsaném v sekci 4.2 Formát dat

<\ n> znak konce řádku

4.2 Formát dat

Zpráva musí obsahovat dvě pole, jejichž popis je uveden v následující tabulce.

Název pole	Popis
Content	Pole je objekt v notaci JSON zakódované v base64. Popis polí, které musí / lze nalézt, je v sekci Kódování kódovaného objektu
Signature	Podpis obsahu pole Content partnera se soukromým klíčem a veřejnou částí musí být přidělen dané službě. Popis konfigurace naleznete v kapitole 7.

Požadavky na podpis:

- Formát ASCII Armor z RFC 4880 opsán v části 6.2
- RSA podpisový algoritmus
- Sha256 hash algoritmus
- veřejný klíč musí být k dispozici bance a musí splňovat požadavky uvedené v kapitole 6



5.2 Formát dat návratu

Zpráva musí obsahovat pole, jejich popis se nachází v tabulce níže:

Název pole	Popis
ServiceId	ID služby, se kterou je platba propojená
Properties	Obsah pole "Properties" z inicializační zprávy, nacházejícího se v poli "Content"

5.3 Vzorová zpráva

Zpráva je identická bez ohledu na výsledek procesu.

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 Konfigurace služby

Aby služba fungovala správně, je třeba odeslat veřejný klíč do mBank, který umožní ověření podpisu. Veřejný klíč je třeba zaslat na adresu: Andrzej.Ksiazek@mbank.pl s informací, ke které službě ServiceId se vztahuje.

6.1 Požadavky na veřejný klíč a podpis

Veřejný klíč, který má banka použít během inicializace převodu, musí splňovat následující požadavky.

Kontrolují se následující parametry:

- 1) Aktivní klíč (z pohledu OpenPGP)
- 2) Datum ukončení platnosti (zda platnost certifikátu vypršela)
- 3) Datum vytvoření (v budoucnu nelze vytvořit)
- 4) Délka platnosti (nepovolujeme certifikáty na dobu neurčitou)
- 5) Bitová síla šifrování / délka klíče (certifikát musí být minimálně 2048 bitů)
- 6) Typ algoritmu použitý ke generování (povolen pouze RSA)

Podpis musí být proveden pomocí klíče, který je spárován s daným ID služby. Povolený algoritmus hash-ování je sha256.

7 Konfigurace certifikátů v IB

Po přihlášení do internetového bankovníctví je možné prohlížet si doručené certifikáty a jejich dodatečnou konfiguraci. Po kliknutí na "Nastavení" a následně dlaždici "mTransfer" se zobrazí seznam certifikátů s přiřazenými službami.

K dispozici jsou následující možnosti:

- 1) Přidání certifikátu,
- 2) Modifikace certifikátu:
 - a) Připojení registrované služby k danému certifikátu,
 - b) odpojení služby od daného certifikátu.
- 3) Odstranění certifikátu (včetně vymazání expirovaných certifikátů).

UPOZORNĚNÍ!

K jedné službě mTransfer (identifikované ServiceID) lze připojit maximálně 3 certifikáty.