

Technický popis k službe e Platby VÚB

Pridelené ID obchodu:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Poznámka:

ID obchodu prideluje a vyplňa pracovník odboru 4700 Ústredia VÚB, a.s.

1. Aplikácia internetového obchodu musí po výbere spôsobu platby zavolať Internet banking VÚB, a.s., nasledovným volaním:

Metóda so SIGN parametrom

- <https://ib.vub.sk/e-platby.aspx>

Parametre sú uložené ako napr. HIDDEN INPUT polia na stránke obchodníka.

Príklad:

```
<FORM name="FORM1" action=" https://ib.vub.sk/e-Platby.aspx " METHOD="POST">
  <INPUT type="hidden" NAME="MID" value="Obchod1">
  <INPUT type="hidden" NAME="AMT" value="100.50">
  <INPUT TYPE="hidden" name="VS" value="1234567890">
  <INPUT TYPE="hidden" name="CS" value="0308">
  <INPUT TYPE="hidden" name="RURL" value="http://mojobchod/shop">
  <INPUT TYPE="hidden" name="SIGN" value="7FB47B8887977421">
</FORM>
```

kde:

- **<MID>** - ID obchodu, ktoré prideluje banka (maximálne 20 alfanumerických znakov bez medzier)
- **<AMT>** - suma, maximálne 13 znakov (ako oddeľovač desatinných miest sa použije „.“)
- **<VS>** - variabilný symbol, jednoznačný identifikátor platby (maximálne 10 numerických znakov)
- **<CS>** - konštantný symbol (max. 4 numerické znaky)
- **<RURL>** - URL adresa na ktorú banka presmeruje klienta po realizácii platby alebo po chybe
- **<SIGN>** - bezpečnostný kľúč pre zabezpečenie integrity údajov. Pre vygenerovanie kľúča je potrebné heslo, ktoré obchodník obdrží od banky
- **<SS>** - špecifický symbol (max. 10 numerických znakov)
- **<DESC>** - popis transakcie. Parameter je nepovinný a klient ho bude môcť na stránke Internet Bankingu zmeniť
- **<REM>** - emailová adresa obchodníka, kam bude zaslaná informácia o realizácii platby
- **<RSMS>** - slovenské mobilné číslo obchodníka, kam bude zaslaná informácia o realizácii platby. (09XXXXXXXXX)

Parametre **<MID>**, **<AMT>**, **<VS>**, **<CS>**, **<RURL>**, **<SIGN>** sú povinné.

Vytvorenie SIGN parametra:

Obchodník obdrží od banky heslo, ktoré sa použije na vytváranie parametra SIGN. Veľkosť hesla je 8 bytov.

Parameter SIGN sa vygeneruje nasledovným spôsobom:

1. Vytvorí sa reťazec pre zašifrovanie.
 - a) Komunikácia obchodník -> banka – spojením parametrov MID, AMT, VS, CS, RURL vznikne reťazec na zašifrovanie.
 - b) Pri komunikácii banka -> obchodník – spojením parametrov VS, (SS), RES vznikne reťazec na zašifrovanie. V prípade, že SS nie je zadaný použijú sa len parametre VS a RES.
2. Z takto vytvoreného reťazca sa vytvorí HASH s dĺžkou 20 bytov pomocou algoritmu SHA1.
3. Prvých 8 bytov HASH-u sa zakrytuje algoritmom DES s použitím hesla, v móde ECB bez inicializačného vektora.
4. Vznikne 8 bytový kľúč, ktorý sa skonvertuje do 16 bytového reťazca, reprezentujúceho jeho hexadecimálny zápis.

Poznámka: Ukážky implementácie v rôznych programovacích jazykoch sú uvedené v bode 4.

Linka pre kontrolu správnosti šifrovania SIGN parametra:

<https://ib.vub.sk/Development/EPayments.aspx>

Banka prijme požiadavku od obchodníka len v prípade, že bankou vygenerovaný SIGN parameter bude zhodný so SIGN parametrom od obchodníka.

Redirect z banky na stránky obchodníka

Pri redirecte klienta zo stránok banky na stránku obchodníka sa použije hodnota parametra RURL. K tomuto URL sa pridajú parametre VS, (SS), RES, SIGN.

- VS – variabilný symbol zadaný obchodníkom
- (SS) – špecifický symbol zadaný obchodníkom. V prípade, že tento parameter nie je zadaný, nepoužije sa
- RES – výsledok spracovania transakcie na strane banky. tento parameter môže mať 2 hodnoty:
 - OK – platba bola zrealizovaná
 - FAIL – pri realizácii sa vyskytla chyba
- SIGN – parameter, ktorého vytvorenie je popísané v časti „Vytvorenie SIGN parametra“

2. Potvrdenie o realizácii platby

Realizáciu platby VÚB, a.s., potvrdí obchodníkovi zaslaním správy na e-mailovú adresu obchodníka, ktorú uviedol v Zmluve o prepojení Internet bankingu VÚB, a.s., a internetového obchodu. Potvrdenie o realizácii platby je zaslané jednotlivými potvrdzovacími e-mailami, okamžite po uskutočnení platby v prospech účtu obchodníka.

Štruktúra e-mailovej správy:

OD: Elektronické bankovníctvo VUB

Predmet: Informácia o realizácii

(nerealizácia) platby za tovar č. obj.

Telo správy (text):

Dátum realizácie (valuta)

Na účet : (číslo účtu príjemcu + kód banky)

V symbol: (číslo objednávky)

Suma:

Z účtu (číslo účtu kupujúceho + kód banky)

SS

KS

Stav (zrealizovaná/nezrealizovaná)

3. Súbor posielaný e-mailom

a) komprimovaný súbor s heslom (rozbalenie súboru s príponou .rar)

Súbor, posielaný e-mailom, je skomprimovaný programom WinRAR s heslom.

Rozbalenie súboru môže vykonať obchodník dvoma spôsobmi:

- a) v prípade, že obchodník má nainštalovaný program WinRAR, otvorí súbor v okne WinRAR dvojklikom myšou, alebo stlačením ENTER na mene súboru. Po zadaní hesla sa rozbalí súbor s potvrdenkou;
- b) v prípade, že obchodník nemá nainštalovaný program WinRAR, použije pri rozbalení súboru s potvrdenkou program **unrar.exe**, ktorý dostane na diskete po obojstrannom podpise Zmluvy o poskytovaní služby e Platby VÚB.

Program **unrar.exe** nakopíruje z diskety do užívateľského adresára. Do tohto adresára prekopíruje z e-mailovej schránky súbor s potvrdenkou.

Rozbalenie súboru vykoná zadaním nasledujúceho príkazu do príkazového riadka:

unrar e -p<heslo> meno_suboru

kde:

<heslo> je heslo na komprimovanie súborov
meno_suboru je názov súboru s potvrdenkou

b) rozbalenie súboru použitím PGP

Pri použití PGP musí obchodník zaslať banke elektronickou cestou svoju verejnú časť páru PGP kľúčov. Banka zašle obchodníkovi svoju verejnú časť kľúčov.

Pri vytváraní mailových potvrdeniek šifrovaných PGP sa správa pre obchodníka podpíše a zašifruje verejným kľúčom obchodníka a priloží sa do mailu ako príloha. Zašifrovaná príloha bude mať názov <MID>_<VS>.gpg, kde:

- MID – ID obchodníka
- VS – číslo objednávky resp. variabilný symbol

Pri e Platbách je použité open-source riešenie GnuPg vo verzii 1.4.6.

Ak na strane obchodníka dôjde k zmene PGP kľúčov, pre úspešné odosielanie šifrovaných mailových potvrdeniek je potrebné aby obchodník novú verejnú časť PGP kľúčov doručil banke čo najskôr.

4. Ukážky kódu pre metódu so SIGN parametrom:

```
// C#
private string CalculateSIGN(string MID, string AMT, string VS, string CS, string RURL, string PWD)
{
    string SIGN = "";

    try
    {
        string StringToEncypher = MID + AMT + VS + CS + RURL;

        byte[] bytesStringToEncypher = Encoding.ASCII.GetBytes(StringToEncypher);
        HashAlgorithm hash = new SHA1Managed();
        byte[] bytesHash = hash.ComputeHash(bytesStringToEncypher);

        DESCryptoServiceProvider des = new DESCryptoServiceProvider();
        des.Key = Encoding.ASCII.GetBytes(PWD);
        des.Mode = CipherMode.ECB;

        ICryptoTransform transform = des.CreateEncryptor();
        byte[] bytesSIGN = new byte[8];
        transform.TransformBlock(bytesHash, 0, 8, bytesSIGN, 0);

        SIGN = BitConverter.ToString(bytesSIGN).Replace("-", "");
    }
    catch (Exception e)
    {
        e = e;
    }
    return SIGN;
}
```

```
// Java
private String CalculateSIGN(String MID, String AMT, String VS, String CS, String RURL, String PWD)
{
    String SIGN = "";
    try
    {
        String StringToEncypher = MID + AMT + VS + CS + RURL;

        MessageDigest hash = MessageDigest.getInstance("SHA-1");
        byte bytesHash[] = hash.digest(StringToEncypher.getBytes());
        Cipher des = Cipher.getInstance("DES/ECB", "Cryptix");

        des.initEncrypt(new RawSecretKey("DES", PWD.getBytes()));
        byte bytesSIGN[] = des.crypt(bytesHash, 0, 8);

        SIGN = Hex.dumpString(bytesSIGN);
    }
    catch (Exception e)
    {
        ;
    }
    return SIGN;
}
```