ŠIAULIŲ BANKAS

ELEKTRONINIO ATSISKAITYMO PASLAUGOS TECHNINĖ SPECIFIKACIJA

Šis dokumentas aprašo reikalavimus tarp Elektroninio atsiskaitymo paslaugos, kuri teikiama per Paslaugos gavėjo internetinį tinklalapį ir Banko internetinės bankininkystės sistemos, naudojantis IB Pay sistema.

1. Elektroninio atsiskaitymo paslaugos veikimo scenarijus

- ✓ Klientas Paslaugos gavėjo interneto tinklalapyje http://www.____.lt suformuoja prekės ir/ar paslaugos užsakymą ir pasirenka Banko internetinės bankininkystės sistemą kaip apmokėjimo būdą.
- ✓ Paslaugos gavėjo sistema pagal prekės/paslaugos užsakymą suformuoja ir siunčia HTTP POST pranešimą 1001 Banko nurodytu URL https://online.sb.lt/ib/site/ibpay/login. Banko serveris suformuoja Banko internetinės bankininkystės prisijungimo langą.
- ✓ Klientui sėkmingai įvedus prisijungimo prie Banko internetinės bankininkystės duomenis, jam yra atidaromas langas su automatiškai suformuotu Mokėjimo nurodymu iš Kliento sąskaitos į Paslaugos gavėjo Sąskaitą, kurį Klientas turi patvirtinti. Mokėjimo nurodymas negali būti redaguojamas (išskyrus mokėtojo (Kliento) sąskaitą), ir gali būti Kliento patvirtintas arba atšauktas.
- ✓ Bankui įvykdžius arba atmetus Kliento patvirtintą Mokėjimo nurodymą, Banko serveris siunčia HTTP POST pranešimą Paslaugos gavėjo nurodytu URL.
- ✓ Jeigu Mokėjimo nurodymas buvo Kliento atšauktas arba Banko atmestas dėl klaidų (pvz. sąskaitoje trūksta lėšų), Banko serveris siunčia pranešimą 1901, apie neįvykdytą Mokėjimo nurodymą.
- ✓ Klientui patvirtinus Mokėjimo nurodymą, Banko serveris siunčia Paslaugos gavėjui pranešimą 1201 apie sėkmingai priimtą, bet dar neįvykdytą Mokėjimo nurodymą.
- ✓ Jei Kliento Mokėjimo nurodymas yra įvykdytas, Banko serveris siunčia pranešimą 1101 apie sėkmingą Mokėjimo nurodymo įvykdymą.

2. Elektroninės paslaugos pranešimų formatas

IB Pay pranešimai yra HTTP(S) užklausos su HTML formos parametrais, kurios perduodamos HTTP POST metodu.
HTML formos parametruose perduodami pranešimo laukai, kurių vienas yra kitų pranešimo laukų skaitmeninis parašas. Skaitmeniniu parašu pasirašoma viena eilutė, sudaryta iš apibrėžta tvarka sujungtų pranešimo laukų reikšmių, kur pranešimo lauko reikšmės ilgis susideda iš trijų skaitmenų (jeigu ilgis mažesnis už 100 priekyje pridedami nuliai) tada seka pati lauko reikšmė, dar toliau seka kito pagal eilės numerį esančio pranešimo lauko reikšmės ilgis ir reikšmė, ir taip kartojama kol sujungiamos visos pranešimo laukų reikšmės, trijų laukų pavyzdys: 007ABCDEFG001A00288. Laukų reikšmių pradžioje ir gale esantys tarpai naikinami, o tuščios reikšmės iš viso nepasirašomos. Parametrų reikšmių seką pasirašymo eilutėje apibrėžia parametro eilės numeris atitinkamo pranešimo lentelėje.
HTML puslapyje su perduodamų laukų forma bei parašo gamyboje negalima naudoti Unicode koduotės, o kad laukuose perduoti nacionaliniai simboliai būtų teisingai vaizduojami FORPOST*Internet Banking puslapiuose, lietuvių kalbai reikia naudoti Windows-1257, rusų – Windows-1251, anglų – bet kokią vieno baito koduotę.
Pasirašymui naudojama schema RSASSA-PKCS1-v1_5 su SHA1 santraukos algoritmu. Į pranešimo lauką rašomas parašas užkoduojamas Base64 algoritmu.

Pranešimo laukų rinkinių aprašymas (visi pasirašomi laukai turi eilės numerį):

2.1 Pranešimas Nr. 1001

Sėkmingai suformuotas Mokėjimo nurodymas pagal Paslaugos gavėjo pateiktus Mokėjimo nurodymo duomenimis.

Nr.	HTML formos parametro pavadinimas	Max ilgis	Būtinas	Aprašymas (Reikšmė)
1.	VK_SERVICE	4	Taip	Pranešimo numeris 1001
2.	VK_VERSION	3	Taip	Parašo algoritmo numeris 008
3.	VK_SND_ID	100	Taip	Paslaugos gavėjo identifikatorius. Atitinka IB Pay sandorio numerį, kurį suteikia bankas
4.	VK_STAMP	100	Ne	Užklausos identifikatorius. Dažniausiai atitinka Kliento krepšelio identifikatorių
5.	VK_AMOUNT	16	Taip	Mokėjimo suma centus atskiriant tašku
6.	VK_CURR	3	Taip	Valiutos trumpinys (ISO 4217)
7.	VK_TERM	19	Ne	Mokėjimo galiojimo terminas. Formatas:

				DD.MM.YYYY HH24:MI:SS Jeigu nenurodytas, nustatomas pagal IB Pay sutartį
8.	VK_ACC	35	Ne	Gavėjo sąskaitos numeris. Jeigu nenurodytas, nustatomas pagal IB Pay sutartį – parenkama aukščiausio prioriteto atitinkamos valiutos sąskaita
9.	VK_PCODE	50	Ne	Įmokos kodas. Gali būti naudojamas tik suderinus su banku
10.	VK_PANK	35	Ne	Gavėjo banko kodas (banko kuriame sudaryta IB Pay sutartis kodas)
11.	VK_NAME	200	Ne	Gavėjo pavadinimas. Jeigu nenurodytas – nustatomas pagal pardavėjo kaip banko kliento pavadinimą
12.	VK_REF	10	Ne	Mokėjimo dokumento numeris. Jeigu nenurodytas – jį pasirenka pats mokėtojas (pirkėjas). Rekomenduojama suderinti šio lauko naudojimą su banku
13.	VK_MSG	300	Taip	Mokėjimo paskirtis. Čia dažniausiai nurodomi visi mokėjimą ir pirkėją identifikuojantys duomenys
14.	VK_MAC	400	Taip	Skaitmeninis parašas RSASSA-PKCS1-v1_5 su SHA1 santraukos algoritmu
15.	VK_RETURN	256	Ne	Pranešimų apie atsiskaitymo eigą siuntimo internetu adresas (paslaugos gavėjo URL)
16.	VK_LANG	3	Ne	Pirkėjo kalba (ISO-639: trijų arba dviejų raidžių kodas)

2.2 Pranešimas Nr. 1101

Banko pranešimas apie sėkmingą Mokėjimo nurodymo įvykdymą.

Nr.	HTML formos parametro pavadinimas	Max ilgis	Aprašymas (Reikšmė)
1.	VK_SERVICE	4	*Pranešimo numeris (1101)*
2.	VK_VERSION	3	Parašo algoritmo numeris (008)
3.	VK_SND_ID	100	Banko identifikatorius. ABSB
4.	VK_REC_ID	100	Paslaugos gavėjo identifikatorius. Atitinka IB Pay sandorio numerį, kurį suteikia bankas
5.	VK_STAMP	100	Užklausos identifikatorius. Dažniausiai atitinka Kliento krepšelio identifikatorių
6.	VK_AMOUNT	16	Apmokėjimo suma. Centai turi būti atskirti tašku
7.	VK_CURR	3	Valiutos trumpinys (ISO 4217)
8.	VK_REC_ACC	35	Gavėjo sąskaitos numeris
9.	VK_REC_NAME	200	Gavėjo pavadinimas
10.	VK_SND_ACC	35	Kliento sąskaitos numeris
11.	VK_SND_NAME	200	Kliento pavadinimas
12.	VK_REF	10	Mokėjimo nurodymo numeris
13.	VK_MSG	300	Mokėjimo paskirtis
14.	VK_T_DATE	10	Mokėjimo data. Formatas: DD.MM.YYYY
15.	VK_PANK	35	Gavėjo banko kodas
16.	VK_MAC	400	Skaitmeninis parašas RSASSA-PKCS1-v1_5 su SHA1 santraukos algoritmu
17.	VK_LANG	3	Kliento kalba (ISO-639: dviejų raidžių kodas)
18.	VK_AUTO	1	Reikšmė lygi „Y“, jeigu IB Pay sistema pranešimą siunčia automatiškai. Reikšmė lygi „N“, jeigu pranešimas siunčiamas nukreipiant Klientą į Paslaugos gavėjo puslapį.
19.	VK_T_NO	12	Pranešimo identifikatorius

2.3 Pranešimas Nr. 1201

Banko pranešimas apie sėkmingai priimtą, bet dar neįvykdytą Mokėjimo nurodymą.

Nr.	HTML formos parametro pavadinimas	Max ilgis	Aprašymas (Reikšmė)
1.	VK_SERVICE	4	Pranešimo numeris 1201

2.	VK_VERSION	3	Parašo algoritmo numeris 008
3.	VK_SND_ID	100	Banko identifikatorius. ABSB
4.	VK_REC_ID	100	Paslaugos gavėjo identifikatorius. Atitinka IB Pay sandorio numerį, kurį suteikia bankas
5.	VK_STAMP	100	Užklausos identifikatorius. Dažniausiai atitinka Kliento krepšelio identifikatorių
6.	VK_AMOUNT	16	Mokėjimo suma centus atskiriant tašku
7.	VK_CURR	3	Valiutos trumpinys (ISO 4217)
8.	VK_REC_ACC	35	Gavėjo sąskaitos numeris
9.	VK_REC_NAME	200	Gavėjo pavadinimas
10.	VK_SND_ACC	35	Mokėtojo sąskaitos numeris
11.	VK_SND_NAME	200	Mokėtojo pavadinimas
12.	VK_REF	10	Mokėjimo dokumento numeris
13.	VK_MSG	300	Mokėjimo paskirtis
14.	VK_PANK	35	Gavėjo banko kodas
15.	VK_MAC	400	Skaitmeninis parašas RSASSA-PKCS1-v1_5 su SHA1 santraukos algoritmu
16.	VK_LANG	3	Pirkėjo kalba (ISO-639: dviejų raidžių kodas)
17.	VK_AUTO	1	Reikšmė lygi „N“
18.	VK_T_NO	12	Pranešimo identifikatorius

2.4 Pranešimas Nr. 1901

Banko pranešimas apie nutrauktą Mokėjimo nurodymą kai:

- Klientas atmetė Mokėjimo nurodymą jo nepatvirtinęs;
- Klientas patvirtino Mokėjimo nurodymą, tačiau Bankas jo neįvykdė dėl lėšų trūkumo Kliento sąskaitoje ar dėl kitų priežasčių, nurodytų Sutarties 3.7 punkte.

Nr.	HTML formos parametro pavadinimas	Max ilgis	Aprašymas (Reikšmė)
1.	VK_SERVICE	4	Pranešimo numeris (1901)
2.	VK_VERSION	3	Parašo algoritmo numeris (008)
3.	VK_SND_ID	100	Banko identifikatorius. ABSB
4.	VK_REC_ID	100	Paslaugos gavėjo identifikatorius. Atitinka IB Pay sandorio numerį, kurį suteikia bankas
5.	VK_STAMP	100	Užklausos identifikatorius. Dažniausiai atitinka Kliento krepšelio identifikatorių
6.	VK_REF	10	Mokėjimo nurodymo numeris
7.	VK_MSG	300	Mokėjimo paskirtis
8.	VK_MAC	400	Skaitmeninis parašas RSASSA-PKCS1-v1_5 su SHA1 santraukos algoritmu
9.	VK_LANG	3	Kliento kalba (ISO-639: dviejų raidžių kodas)
10.	VK_AUTO	1	Reikšmė lygi „Y“, jeigu IB Pay sistema pranešimą siunčia automatiškai. Reikšmė lygi „N“, jeigu pranešimas siunčiamas nukreipiant Klientą į Paslaugos gavėjo puslapį.

3. Elektroninio parašo formavimo algoritmas

3.1 Versijos 008 algoritmas:
MAC008(x_1, x_2, ..., x_n) := RSA(SHA-1(p(x_1)||x_1||p(x_2)||x_2||...||p(x_n)||x_n),d,n)
3.1.1 || - simbolių eilučių sujungimas, o ne skiriamieji simboliai;
3.1.2 x_1, x_2, ..., x_n - užklausos parametrai;
p - parametro ilgio funkcija. Rezultatas pateikimas trijų skaičių eilute (pvz. 007);
d - slapta RSA eksponentė;
n - RSA modulis

4. Susitarimai

4.1 Bankas ir Paslaugos gavėjas apsikeičia Viešaisiais raktais.