Luminor

E. PREKYBOS PASLAUGOS TECHNINĖS SĄLYGOS

1. B2B Veikimo scenarijus

1.1. Klientas Banko partnerio – Prekybininko puslapyje **http://www._____ (IP** -) suformuoja prekės/paslaugos užsakymą ir pasirenka BANKAS INTERNETE kaip apmokėjimo būdą.
1.2. Prekybininko sistema pagal prekės užsakymą suformuoja ir siunčia HTTPS POST pranešimą 2001 Banko nurodytu URL **https://ib.dnb.lt/loginb2b.aspx**. Banko serveris suformuoja BANKAS INTERNETE prisijungimo langą.
1.3. Klientui sėkmingai įvedus identifikacijos kodus ir slaptažodžius, jam yra atidaromas langas su suformuotu mokėjimo pavedimu iš Kliento sąskaitos į Prekybininko sąskaitą. Pavedimas negali būti redaguojamas(išskyrus mokėtojo sąskaitą), ir gali būtu Kliento patvirtintas arba atšauktas.
1.4. Bankui įvykdžius arba atmetus Kliento patvirtintą pavedimą, Banko serveris siunčia HTTPS POST pranešimą Interneto prekybininko nurodytu URL:
1.4.1. Jeigu pavedimas buvo Kliento atšauktas arba Banko atmestas dėl klaidų (pvz. Sąskaitoje trūksta lėšų), Banko serveris siunčia HTTPS POST pranešimą 1901.
1.4.2. Jei Kliento pavedimas yra įvykdytas, Banko serveris siunčia HTTPS POST pranešimą 1101.
Pastaba. Visa komunikacija tarp Prekybininko ir Banko atliekama naudojant 443 protokolą.

2. B2B pranešimų formatas

2.1. Pranešimas 2001

Nr.	Parametro pavadinimas	Max ilgis	Aprašymas (Reikšmė)
1.*	VK_SERVICE	4	Pranešimo numeris (2001)
2.*	VK_VERSION	3	Šifravimo algoritmo versijos numeris (008)
3.*	VK_SND_ID	9	Pranešimo siuntėjo identifikatorius (įmonės kodas)
4.*	VK_STAMP	20	Pranešimo identifikatorius
5.*	VK_AMOUNT	16	Apmokėjimo suma. Centai turi būti atskirti tašku (pvz. 50.25)
6.*	VK_CURR	3	Valiuta (EUR)
7.*	VK_ACC	20	Gavėjo sąskaita
8.*	VK_PANK	9	Banko kodas (40100)
9.*	VK_NAME	200	Gavejo pavadinimas
10.*	VK_REF	20	Užsakymo numeris
11.*	VK_MSG	200	Apmokėjimo aprašymas (laisva forma)
-*	VK_MAC	600	Elektroninis parašas
-*	VK_RETURN	100	URL, į kurį Bankas siunčia HTTP POST pranešimą
-	VK_MANUAL_RETURN	100	URL, į kurį Bankas siunčia neautomatinį HTTP POST pranešimą (nukreipia klientą paspaudus mygtuką „Grįžti į el-parduotuvę“). Jei parametras neperduodamas, pranešimas siunčiamas VK_RETURN parametre nurodytu adresu
-	VK_LANG	3	Naudojama kalba (LIT)
-	VK_TIME_LIMIT	19	Data ir laikas, iki kada galioja pavedimas. (yyyy-mm-dd hh:mm:ss). Jei laukas tuščias ar visiškai neatsiunčiamas, pavedimas laiko limito neturi.

* - privalomi parametrai

2.2. Pranešimas 1101

Nr.	Parametro pavadinimas	Max ilgis	Aprašymas
1.	VK_SERVICE	4	Pranešimo numeris (1101)
2.	VK_VERSION	3	Šifravimo algoritmo versijos numeris (008)
3.	VK_SND_ID	9	Siuntėjo (banko) identifikatorius (112029270)
4.	VK_REC_ID	9	Gavėjo (parduotuvės) identifikatorius. (VK_SND_ID iš 2001 pranešimo)
5.	VK_STAMP	20	Pranešimo identifikatorius (VK_STAMP iš 2001 pranešimo)
6.	VK_T_NO	35	Apmokėjimo numeris
7.	VK_AMOUNT	16	Apmokėjimo suma (VK_AMOUNT iš 2001 pranešimo)
8.	VK_CURR	3	Valiuta (EUR)
9.	VK_REC_ACC	20	Gavėjo sąskaita(VK_ACC iš 2001 pranešimo)
10.	VK_REC_NAME	200	Gavėjo pavadinimas (VK_NAME iš 2001 pranešimo)
11.	VK_SND_ACC	20	Mokėtojo sąskaita
12.	VK_SND_NAME	200	Mokėtojo pavadinimas

13.	VK_REF	20	Užsakymo numeris (VK_REF iš 2001 pranešimo)
14.	VK_MSG	200	Apmokėjimo aprašymas (VK_MSG iš 2001 pranešimo)
15.	VK_T_DATE	10	Apmokėjimo data (yyyy.mm.dd)
-	VK_PANK	9	Banko kodas (40100)
-	VK_MAC	600	Elektroninis parašas
-	VK_LANG	3	Naudojama kalba (LIT)
-	VK_AUTO	1	'Y' – Bankas pranešimą išsiuntė automatiškai, 'N' - neautomatiškai

2.3. Pranešimas 1901

Nr.	Parametro pavadinimas	Max ilgis	Aprašymas
1.	VK_SERVICE	4	Pranešimo numeris (1901)
2.	VK_VERSION	3	Šifravimo algoritmo versijos numeris (008)
3.	VK_SND_ID	9	Siuntėjo (banko) identifikatorius (112029270)
4.	VK_REC_ID	9	Gavėjo (parduotuvės) identifikatorius (VK_SND_ID iš 2001 pranešimo)
5.	VK_STAMP	20	Pranešimo identifikatorius (VK_STAMP iš 2001 pranešimo)
6.	VK_REF	20	Užsakymo numeris (VK_REF iš 1001 pranešimo)
7.	VK_MSG	200	Apmokėjimo aprašymas (VK_MSG iš 2001 pranešimo)
-	VK_MAC	600	Elektroninis parašas
-	VK_LANG	3	Naudojama kalba (LIT)
-	VK_AUTO	1	'Y' – Bankas pranešimą išsiuntė automatiškai, 'N' - neautomatiškai

3. Elektroninio parašo formavimo algoritmas

Elektroninio parašo reikšmė, kuri saugoma lauke VK_MAC ir naudojama užklausose apskaičiuojama pagal sutartą algoritmą, kurio numeris saugomas lauke VK_VERSION. Naudojama algoritmo versija 008 (001, 002, 007 nenaudojamos). Algoritmas ateityje gali būti keičiamas, atsiradus naujiems šifravimo būdams. VK_MAC reikšmė yra užkoduota BASE64 kodavimo algoritmu.

<u>008 versijos algoritmas:</u>
$MAC008(x_1, x_2, \ldots, x_n) := RSA(SHA\text{-}1(p(x_1)||x_1||p(x_2)||x_2||\ldots||p(x_n)||x_n),d,n)$

Čia
|| - simbolių eilučių sujungimas
$x_1, x_2, \ldots, x_n$ - užklausos parametrai, naudojami tik sunumeruoti parametrai;
p - parametro ilgio funkcija. Rezultatas pateikimas trijų skaičių eilute (pvz. 007);
d - slapta RSA eksponentė;
n - RSA modulis