Luminor

E-COMMERCE SERVICE SPECIFICATIONS

This document describes the interfaces between the e-commerce services and INTERNET BANKING.

1. B2B Operation scenario

1.1. The user selects a service (commodity) in the webpage **http://www.example.lt** (IP **-**) of the bank's e-commerce partner and selects INTERNET BANKING as the payment method.

1.2. The system of the bank's e-commerce partner sends HTTP POST inquiry 2001 to the URL https://ib.dnb.lt/loginb2b.aspx indicated by the bank. The bank server forms the Internet bank connection window.

1.3. After the user successfully enters the identification codes and passwords, the formed window opens thereto for making the payment order from the user's account to the bank's e-commerce partner account. The order may not be corrected and it may be confirmed or cancelled.

1.4. In case the order was executed or rejected by the bank, the bank server sends HTTP POST inquiry to URL indicated by the bank's e-commerce partner:

1.4.1. In case the order is cancelled by user or rejected (for example insufficient funds) by bank, the bank server sends HTTP POST inquiry 1901

1.4.2.. In case the order is executed by Bank, the bank server sends HTTP POST inquiry 1101.

Note. All communication between the merchant and the bank performed using 443 protocol.

2. B2B inquiries format description

2.1. Inquiry 2001 (Payment initiation)

No.	Parameter	Max ilgis	Description
1.*	VK_SERVICE	4	Inquiry number (2001)
2.*	VK_VERSION	3	Numbering algorithm version (008)
3.*	VK_SND_ID	9	Identifier of the inquiry sender.
4.*	VK_STAMP	20	Unique number – inquiry identifier (not used by the bank).
5.*	VK_AMOUNT	16	Payment amount
6.*	VK_CURR	3	Currency (EUR)
7.*	VK_ACC	20	Beneficiary's account
8.*	VK_PANK	9	Bank code
9.*	VK_NAME	200	Beneficiary's name
10.*	VK_REF	20	Order number
11.*	VK_MSG	200	Payment description (free form)
-*	VK_MAC	600	Electronic signature
-*	VK_RETURN	100	URL where bank sends HTTP POST inquiry (1101 or 1901)
-	VK_MANUAL_RETURN	100	URL where bank sends manual HTTP POST inquiry (directs client by pressing button „Grįžti į el. parduotuvę (Go back to e-shop)). If parameter is not sent, then POST inquiry is sent to address given in VK_RETURN parameter
-	VK_LANG	3	Language used (LIT)
-	VK_TIME_LIMIT	19	Payment expiry date and time. (yyyy-mm-dd hh:mm:ss). If parameter is empty, payment doesn't have time limit.

* - madatory parameters

2.2. Inquiry 1101 (Order is executed)

No.	Parameter	Max length	Description
1.	VK_SERVICE	4	Inquiry number (1101)
2.	VK_VERSION	3	Numbering algorithm version (008)
3.	VK_SND_ID	9	Sender (bank) identifier
4.	VK_REC_ID	9	Beneficiary (shop) identifier
5.	VK_STAMP	20	Unique number – inquiry identifier (not used by the bank).
6.	VK_T_NO	12	Payment number
7.	VK_AMOUNT	16	Payment amount
8.	VK_CURR	3	Currency (EUR)

9.	VK_REC_ACC	20	Beneficiary’s account
10.	VK_REC_NAME	200	Beneficiary’s name
11.	VK_SND_ACC	20	Payer’s account
12.	VK_SND_NAME	200	Payer’s name
13.	VK_REF	20	Order number
14.	VK_MSG	200	Payment description (free form)
15.	VK_T_DATE	10	Payment date
-	VK_PANK	9	Bank code
-	VK_MAC	300	Electronic signature
-	VK_LANG	3	Language used (LIT)
-	VK_AUTO	1	‘Y’ – in case of an automatic reply sent, otherwise – ‘N’

2.3. Inquiry 1901 (Order is rejected)

No.	Parameter	Max length	Description
1.	VK_SERVICE	4	Inquiry number (1901)
2.	VK_VERSION	3	Numbering algorithm version (008)
3.	VK_SND_ID	9	Sender (bank) identifier
4.	VK_REC_ID	9	Beneficiary (shop) identifier
5.	VK_STAMP	20	Unique number – inquiry identifier (not used by the bank).
6.	VK_REF	20	Order number
7.	VK_MSG	200	Payment description (free form)
-	VK_MAC	300	Electronic signature
-	VK_LANG	3	Language used (LIT)
-	VK_AUTO	1	‘Y’ – in case of an automatic reply sent, otherwise – ‘N’

3. Electronic signature formation algorithm

Electronics signature meaning, which is stored in field VK_MAC and used in the inquiries, is calculated according to the agreed algorithm the number of which is stored in field VK_VERSION. Currently used algorithm version is 008. Versions 001, 002 and 007 are not used. The algorithm may be changed in the future in case new numbering methods appear.
VK_MAC meaning is coded by BASE64 numbering algorithm.

008 version algorithm:
$\mathrm{MAC008}(x_1, x_2, \ldots, x_n) := \mathrm{RSA}(\text{SHA-1}(p(x_1)||x_1||p(x_2)||x_2||\ldots||p(x_n)||x_n),d,n)$

where:

|| - symbol lines connecting

x_1, x_2, …, x_n inquiry parameters;
p function that returns the parameter length. The result is provided as a three-segment number (e.g. 007)

d – RSA secret exponent

n- RSA module