Luminor Bank AS Latvian branch

Luminor Link specification
(B2B functional description)

Luminor_Link_FS_EN_1_EXTSYS_1_L_2013

Table of contents

1. Purpose of the system

Service providers on the Internet (hereinafter – the Merchants), and the customers of Internet bank (hereinafter - the Customers) with the help of LUMINOR Link system can carry out data exchange, provide services, initiate payment transactions and data transfers. LUMINOR Link is a system to provide the following business processes:

- Merchants may direct their Customers to the Internet-bank with already prepared payment orders and receive confirmation from the bank on successful / unsuccessful execution of the orders (payment). E.g. allow to make payment of the goods, from e-shops, insurance companies and other systems, using special Internet-bank interface;
- User authorization for External systems, using Internet-bank;
- Transfer of personal data of Internet-bank user to External systems.

2. Business processes

2.1. Payment for goods and services

Payments for goods and services can be made only to Merchants who have entered into the agreement with the bank on utilization of service.

The scheme of payment for goods and services is shown in Fig. 1.

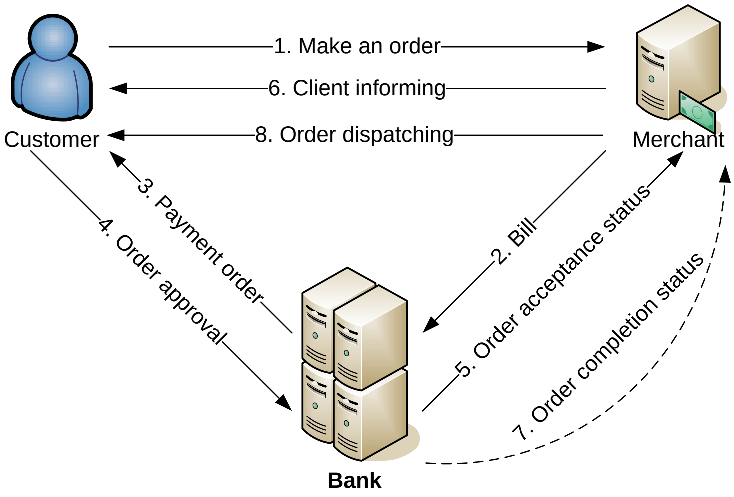

Fig. 1 Payment scheme

The process consists of the following stages:

1. The Customer initiates the process by using the Internet-shop or other External system. The Customer needs a Web-browser to select services and goods from the Merchant and to make a payment through Internet-bank. The Customer selects certain items he wants to buy.
2. The Merchant offers to the Customer the possibility of payment via Internet-bank, by creating an HTML page, which generates deposit slip data and redirects the Customer's Web-browser to the Internet-bank server. The integrity of the data is provided by a digital signature of the Merchant.
3. The Bank:
   a. Displays Internet-bank webpage, where the Customer is asked to enter the user name, password and code from the code calculator or code card.
   b. The Bank undertakes verification of the Merchant's digital signature and then the Customer is asked to confirm a prepared and already completed payment order.
4. The Customer can confirm the prepared payment order or return to the home page of the Merchant. If the Customer returns to the Merchant without confirming the payment, the payment is not saved in the database.
5. After confirmation of orders by the Customer the Bank will do the following:
   a. Send information about the payment order execution status to the Merchant, securing integrity of information by the digital signature of the Bank, invoking a page from the Merchant side, using POST method.
   b. Generate an HTML page that contains information about the status of the successful adoption of the payment order for processing and display it to the Customer.
6. The Customer on this page can do the following:
   a. Return to the Merchant’s page;
   b. Continue to work with the Internet-bank;
   c. Close the Web-browser.

In case of incorrect signature the system will generate an appropriate error message and preclude sending of the payment order.

7. After execution or cancellation of the payment order the Bank requests a specified page of the Merchant to confirm the operation and pass parameters by using the POST method. The operation is executed asynchronously.
8. The dealer after receiving the final status of the payment from the Bank verifies the Bank's digital signature and performs the appropriate action. For example: in case of confirmation, goods and services are sent to the Customer. Or the order is cancelled in case of payment cancelation.

2.2. Authorization in External systems

Authorization is possible only in External systems the Bank has concluded a contract with.

Authorization scheme is shown in Fig. 2.

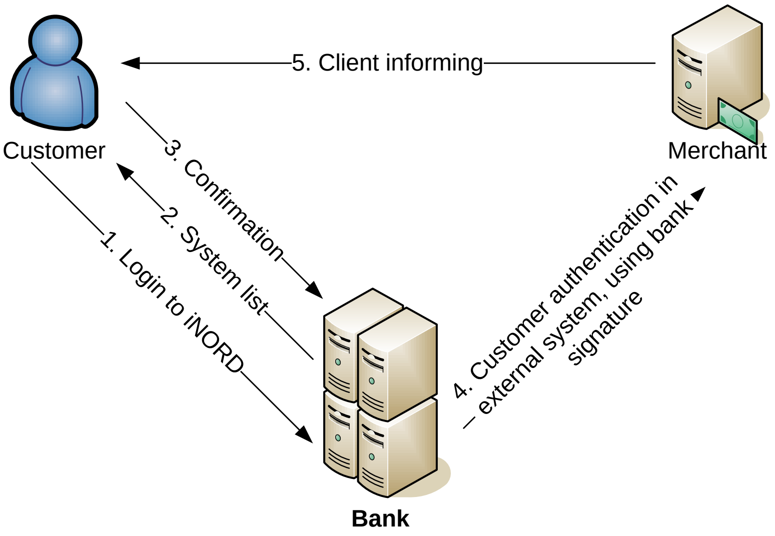

Fig. 2 Scheme of authorization in External systems

The process consists of the following stages:

1. The Customer starts the process after authentication in Internet-bank.
2. The Bank provides to the Customer a page with a list of External systems, the Customer can choose from by clicking a hyperlink.
3. The Customer can either confirm or cancel data transfer. The Customer’s redirection to an External system is possible only in case the Customer confirms his personal data transfer.
4. After confirmation the Bank performs redirection of the Customer to the requested system by opening a new browser window and confirming the request with a Bank’s digital signature.
5. The External system after verification of the Bank's digital signature authenticates the Customer and offers to the latter the relevant services.

2.3. Transfer of personal Customer data to Merchants

Transfer of personal Customer data to Merchants is possible only subject to the Customer’s agreement and only to Merchants the bank has concluded a contract for enabling such service with.

The scheme of transfer of personal Customer data to Merchants is shown in Fig. 3.

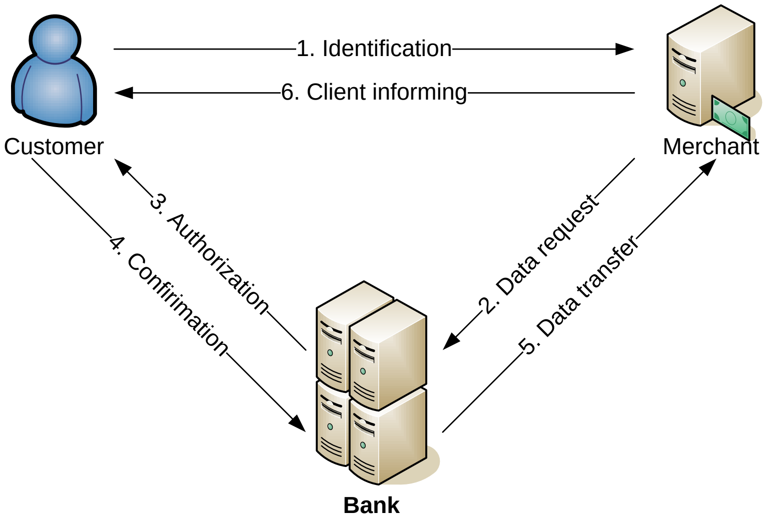

Fig. 3 Scheme of transfer of personal Customer data to Merchants

The process consists of the following stages:

1. The Customer begins the process by using the Merchant's Internet-shop or another External system.
2. The Merchant, if identification of the Customer is necessary, offers to them the opportunity to confirm personal data through Internet-bank. The Merchant creates HTML page that redirects the Customer's web browser to the Internet-bank server. Data integrity is provided by a Merchant's digital signature.
3. The Bank:
   a. Displays an Internet-bank webpage, where the Customer will be asked to enter a user name, password and code from the code calculator or from the code card, i.e. to make an authorization.
   b. Verifies the Merchant's digital signature and asks the Customer to confirm personal data transfer to the Merchant.
4. The Customer can either confirm or reject the transfer.
5. In case of transfer confirmation Bank will:
   a. Transfer personal data of the Customer to the Merchant, by securing integrity of this data with the Bank’s digital signature.
   b. Redirect the Customer to the Merchant’s web-page.
6. The Merchant, after receiving the data from the Bank, verifies the Bank's digital signature and executes appropriate actions in its own system.

3. Security

3.1. General principles

To ensure the security of data the transmission system must meet the following requirements:

- Connection between the Merchant and the Customer is organized according to safety requirements put forward by the Merchant;
- The Merchant communicates with the Bank using a standard HTTPS/SSL protocol;
- The Bank connects to the Merchant in accordance with safety requirements put forward by the Merchant, namely: HTTP/HTTPS protocols;
- The Customer communicates with the Bank using a standard HTTPS/SSL protocol.
- Any data that is transferred by the Bank to the Merchant or vice versa, must contain a digital signature, which thus allows the second party to ensure the integrity of the data. Algorithm for generating a digital signature is described in section 3.3. The data is not further encoded.

3.2. Digital signature

Digital signature means insertion of a fragment of foreign encrypted information in the data. Transmitted information is not protected, i.e., remains open and available for review to the persons through whom it is transmitted. Foreign encrypted information is formed by using two methods: hash function to calculate the checksum and signing of results by the private key.

3.2.1. Checksum

This is a tool for monitoring the integrity of the transmitted data, whose modus operandi is based on the fact that on the information output by a particular algorithm calculates a value. This value (checksum) is sent along with the data. At input the checksum is calculated by the same algorithm and compared with that calculated at output.

SHA-1 hash algorithm is used to create a checksum. Hash function works in such a way that it is practically impossible to create two different texts with the same checksum.

3.2.2. Signing

Actual signing and sign-checking is done by two keys - private (closed) and public (opened). Public key is operable by all of your correspondents, but private key - for only you. The algorithm works in such a way that for signing is used the Merchant's private key and for checking - the Merchant's public key.

Checksum, created by hash-function is encrypted by using the sender's private key with RSA algorithm and sent as the request part. The algorithm for generating the checksum is described in Section 3.3.

3.3. Algorithm for generating a digital signature

All requests - from the Merchant to the Bank, and vice versa - contain digital signature. A digital signature is computed at the following algorithm and depends on the values of the query parameters and the algorithm parameters. The algorithm used is specified in the contract between the Bank and the Merchant. Request parameters to be included in the calculation depend on the request type. Calculated digital signature will be translated into a number of characters, using the BASE64 code, and sent to the counterpart in the VK_MAC request parameter.

Calculation of the digital signature is done by a RSASSA-PSS algorithm of a public key with a SHA-1 hash algorithm. Calculation takes into account the requested parameter length, so-called request's empty fields.

SIGN(x1,x2,…,xn) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || … ||p(xn)||xn),e,n)

where:

- **||** – symbol row concatenation;
- **x1, x2, …, xn** – request parameters;
- **p(xi)** – function of the parameter length. Returns parameter length as 3-digit number padded by '0' (zero) from left. In case of zero it returns '000';
- **e, n** – private key, RSA parameters;
- All request parameters must be encoded in UTF-8 encoding.

Example:

Received request with such parameters:

- VK_SERVICE="1002"
- VK_VERSION="101"
- VK_SND_ID="MERCHANT"
- VK_STAMP="1234567890"
- VK_AMOUNT="6.79"
- VK_CURR="EUR"
- VK_REF="01012001-001"
- VK_MSG="Payment for goods XXXXXX"

Calculation of the digital signature upheld by a number of characters, which consists of the following elements (the length and value of the relevant parameters):

- "0041002"
- "003101"
- "008MERCHANT"
- "0101234567890"
- "0046.79"
- "003EUR"
- "01201012001-001"
- "024Payment for goods XXXXXX"

or as a single string:

"0041002003101008MERCHANT01012345678900046.79003EUR01201012001-001024Payment for goods XXXXXX"

For example, if VK_MSG parameter is empty, then parameter string will be following: "0041002003101008MERCHANT01012345678900046.79003EUR01201012001-001000"

3.4. Order of exchange of X509 certificates

Order of exchange of X509 certificates is as follows:

1. The Merchant:
   a. Generates both keys – private and public in length of 2048 bit, as well as X509 certificate;
   b. Saves private key in its system for signing requests to the bank;
   c. At the time of signing a contract with the Bank provides him with X509 certificate;
   d. Saves X509 certificate received from the Bank in its own system to check the Bank's digital signature.
2. The Bank:

a. Generates unique 2048 bit private and public keys as well as X509 certificate used by the Merchant, before signing the contract;
b. Saves its private key in its own system by attaching to the particular Merchant;
c. At the time of signing an agreement with the Merchant provides him with a generated X509 certificate;
d. Saves X509 certificate received from the Merchant in its own system to check the Merchant's digital signature.

X509 certificates are transmitted between the Bank and the Merchant in PEM (Privacy Enhanced Mail) format. PEM format is a DER certificate encoded in BASE64, placed between the lines: "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

Restrictions with regard to the effective period of the certificate are stipulated by the Bank. The effective period of such certificate must extend to 3 years. Prior to expiry of the effective period the Bank and the Merchant shall agree on execution and exchange of new certificates.

4. Data exchange protocol

Exchange protocol describes type and sequence of calls for each business process. Calls are HTTP POST requests with certain parameters (fields).

Each request contains the request type. Each type of query corresponds to the list of mandatory parameters and processing algorithm.

- All parameters that are included into requests are required. Required parameters always must be included in requests, even if their values are not defined (blank field);
- Amounts in requests must be specified using point (".") as a decimal delimiter. Thousand delimiters are not used at all;
- Date must be specified in "DD.MM.YYYY" format. For example: "17.01.2010";
- Time must be specified in "hh24:mm:ss" format. For example: "17:02:59";
- Parameter value length should not exceed maximum, defined in the specification.
- Parameter value length may be less than maximum, also no need to fill empty spaces. Parameter values should not contain beginning and trailing whitespaces (" ");
- Incorrectly constructed or broken requests will not be processed;
- Operations, which are performed by request, must meet the general requirements of service (requirements related to payment orders etc.);
- All data must be encoded in UTF-8 encoding.

4.1. "Payment for goods and services" requests

4.1.1. 1002 "Data for payment order" request

The Merchant sends to the Bank the request that contains information about payment order, which Customer cannot change in Internet-bank. This request is sent by the POST method by using Bank's address specified in the agreement.

Table 1. 1002 «Data for payment order» request

№	Parameter	Particip. in dig. sign.	Max. length	Description	Explanation
1.	VK_SERVICE	Yes	4	Request type (1002)	1002
2.	VK_VERSION	Yes	3	Digital signature algorithm (101)	101
3.	VK_SND_ID	Yes	20	Merchant ID	Merchant's identifier in the bank
4.	VK_STAMP	Yes	32	Request ID – unique number – (not used by bank).	Formed by the Merchant
5.	VK_AMOUNT	Yes	13	Payment amount	Formed by the Merchant. Point delimiter (21.36)
6.	VK_CURR	Yes	3	Payment currency (EUR)	EUR
7.	VK_ACC	Yes	21	Recipient's account	Merchant's account number
8.	VK_NAME	Yes	105	Recipient's name	Merchant's name
9.	VK_REG_ID	Yes	20	Recipient's registration number	Merchant's registration number

10.	VK_SWIFT	Yes	20	Recipient’s bank code	Merchant’s bank code
11.	VK_REF	Yes	20	Payment number at Merchant’s side	Formed by the Merchant
12.	VK_MSG	Yes	140	Payment detail	Formed by the Merchant
13.	VK_RETURN	Yes	400	URL where request asynchronously Customer after payment is processed	Formed by the Merchant
14.	VK_RETURN2	Yes	400	URL where to send status after process ends	Formed by the Merchant
15.	VK_MAC	No	300	Digital signature	Formed by the Merchant
16.	VK_TIME_LIMIT	No	19	Date and time of request expiration	After this date the request will be considered as invalid Format: dd.MM.yyyy HH:mm:SS
17.	VK_LANG	No	3	Preferred language (LAT/ENG/RUS)	LAT

4.1.2. 1102 “Payment status” request

The Merchant receives this request three times – one is directly from the Bank’s server after payment order confirmation by the Customer (parameters are transmitted by using POST method, calling page on the Merchant’s side, using address specified in the 1002 request’s VK_RETURN2 parameter, status “1” is being transmitted), second time – when the Customer after payment confirmation returns to the Merchant’s web page (parameters are transmitted by the POST method, using address specified in the 1002 request’s VK_RETURN parameter, status “1” is being transmitted). And the third time – when the banking system has finished payment processing (the third call is done by calling page on the Merchant’s side, using POST method for parameters transmitting to the address specified in VK_RETURN2 parameter. Status “2” or “3” is sent, depending on success in processing of the payment).

The Merchant can receive this request also if an error has occurred while sending 1002 request. In this case the Merchant receives the request synchronously.

In case the Customer closes web browser after the Customer’s redirection to the payment confirmation web page without authorization or confirmation of the payment, the Merchant will not receive an answer.

After the payment processing the Bank asynchronously sends 1102 request with different values of VK_T_STATUS field:

- When the Customer has confirmed sending of the payment order it is being saved in DB, but still is not processed by the banking system. The Bank sends the answer “1102” with status “1”.
- After successful payment processing in the banking system, the Bank sends the answer “1102” with status “2” to the Merchant;
- If the Customer doesn’t confirm the payment order or for any reason the payment order cannot be accepted for execution (insufficient funds on the Customer’s account, etc.), the Bank sends the answer “1102” with status “3”.

Table 2. 1102 «Payment status» request

№	Parameter	Particip. in dig. sign.	Max. length	Description	Explanation
1.	VK_SERVICE	Yes	4	Request type (1102)	1102
2.	VK_VERSION	Yes	3	Digital signature algorithm (101)	101
3.	VK_SND_ID	Yes	20	Sender ID (bank’s)	Formed by the bank
4.	VK_REC_ID	Yes	20	Recipient ID (Merchant’s)	VK_SND_ID field from 1002 request
5.	VK_STAMP	Yes	32	Request ID – unique number – (not used by bank).	VK_STAMP field from 1002 request
6.	VK_T_NO	Yes	12	Number of payment order	Formed by the bank
7.	VK_AMOUNT	Yes	13	Payment amount	VK_AMOUNT field from 1002 request
8.	VK_CURR	Yes	3	Payment currency (EUR)	EUR
9.	VK_REC_ACC	Yes	21	Recipient’s account	VK_ACC field from 1002 request
10.	VK_REC_NAME	Yes	105	Recipient’s name	VK_NAME field from 1002 request

11.	VK_REC_REG_ID	Yes	20	Recipient's registration number	VK_REG_ID field from 1002 request
12.	VK_REC_SWIFT	Yes	20	Recipient's bank code	VK_SWIFT field from 1002 request
13.	VK_SND_ACC	Yes	21	Payer's account	Payer's account
14.	VK_SND_NAME	Yes	105	Payer's name	Payer's name
15.	VK_REF	Yes	20	Payment number on the Merchant side	VK_REF field from 1002 request
16.	VK_MSG	Yes	140	Payment details	VK_MSG field from 1002 request
17.	VK_T_DATE	Yes	10	Payment processing date	Formed by bank
18.	VK_T_STATUS	Yes	4	Payment processing status	1 – Accepted for execution 2 – Executed 3 – Cancelled
19.	VK_MAC	No	300	Digital signature	Formed by the bank
20.	VK_LANG	No	3	Language (LAT/ENG/RUS)	LAT

4.2. Authorization in External systems

4.2.1. 2001 "Customer authorization in External system" request

The Bank directs the Customer to the address of the selected Merchant/External system with parameters described in "2001" request. This request is sent by the POST method to the selected Merchant/External system address, specified in the agreement.

Table 3. 2001 «Customer authorization in the External system» request

№	**Parameter**	**Particip. in dig. sign.**	**Max. length**	**Description**	**Explanation**
1.	VK_SERVICE	Yes	4	Request type (2001)	2001
2.	VK_VERSION	Yes	3	Digital signature algorithm (101)	101
3.	VK_SND_ID	Yes	20	Sender's ID (bank's)	Formed by the bank
4.	VK_REC_ID	Yes	20	Recipient's ID (Merchant/External system)	Field from the agreement with Merchant (Merchant identifier)
5.	VK_STAMP	Yes	32	Request ID – unique number	VK_STAMP field from the 3001 request, in case of authorization on the initiative of the bank – field is empty.
6.	VK_T_NO	Yes	12	Answer ID – unique number	Formed by the bank (unique for each request).
7.	VK_PER_CODE	Yes	12	Personal code	Personal code
8.	VK_PER_FNAME	Yes	100	Customer name	-
9.	VK_PER_LNAME	Yes	100	Customer surname	-
10.	VK_COM_CODE	Yes	20	Company's registration number	-
11.	VK_COM_NAME	Yes	200	Company name	-
12.	VK_TIME	Yes	32	Request timestamp	Format yyyyMMddHHmmSS
13.	VK_MAC	No	300	Digital signature	Formed by bank
14.	VK_LANG	No	3	Preferred language (LAT/ENG/RUS)	LAT

4.3. Transfer of personal Customer data to Merchants

4.3.1. 3001 “Request for Customer data” request

This request is sent by POST method to the Bank’s address specified in the agreement.

Table 4. 3001 «Request for Customer data» request

№	Parameter	Particip. in dig. sign.	Max. length	Description	Explanation
1.	VK_SERVICE	Yes	4	Request type (3001)	3001
2.	VK_VERSION	Yes	3	Digital signature algorithm (101)	101
3.	VK_SND_ID	Yes	20	Merchant/External system ID	Merchant identifier
4.	VK_STAMP	Yes	32	Request ID – unique number	Formed by the Merchant (unique for each request).
5.	VK_RETURN	Yes	400	URL where to redirect the Customer when the process ends	Formed by the Merchant
6.	VK_MAC	No	300	Digital signature	Formed by the Merchant
7.	VK_LANG	No	3	Preferred language (LAT/ENG/RUS)	LAT

4.3.2. 2001 “Customer authorization in External system” request

In case of data transfer to the Merchant is confirmed by the Customer, the Bank redirects the Customer to the selected Merchant/External system address with parameters described in “2001” request. This request is sent by POST method to the address specified in VK_RETURN parameter of the “3001” request.

5. Processing of payments through banking systems

5.1. LUMINOR Link modules

LUMINOR Link “payment module” is accessible to users of Internet-bank customers (private individuals and legal entities), on condition that both the authority and the signature assigned to the specific user support application of functionality.

LUMINOR Link “Authorization module” is accessible to private individuals only, on condition that Internet-bank “user = the customer”.

5.2. Processing of LUMINOR Link payments under Internet-bank multi-user conditions

In situations when LUMINOR Link is used by the Customer - legal entity or the Customer - private individual to whom are assigned special Internet-bank application rights LUMINOR Link payments are processed similarly to processing of other Internet-bank payments (e.g., domestic, cross-border), as their generation is initiated concurrently with LUMINOR Link application and further activities are exercised after logging-in in the Internet-bank following the regular procedure.

If any of the authorities assigned to the Internet-bank user (Internet-bank application mode, signature, scope of application thereof, daily or payment limits) preclude preparation of Internet-bank payment and its dispatch for execution concurrently with LUMINOR Link application further processing of such payment shall follow in Internet-bank from the menu “BANK - Payments - List of payments”. The Customer in the menu “List of payments” may perform standard activities with the payment, i.e. delete, edit (applicable to changes in the remitter’s account number only), sign and send for execution.

Multi-user situations are particularly sensitive to limitations of VK_TIME_LIMIT setting.

5.3. Internet-bank business hours and limitations to execution of payments

5.3.1. Modes of operation

Internet banking working mode is 24x7.

Internet banking activities may be limited or terminated by technical breakdowns or system maintenance works.

5.3.2. Limitations to execution of payments

LUMINOR Link payments incorporate VK_TIME_LIMIT parameter.

VK_TIME_LIMIT means „payment maturity” – pre-set time limit the payment may be signed within Internet-bank (by affixing all required signatures) and executed within the system. VK_TIME_LIMIT as specified in the payment must be „greater / equal” to the current time to enable successful processing and execution of payment.

Unless otherwise instructed by the Bank VK_TIME_LIMIT parameter should be specified as a blank field. Will be applied the bank's parameter by default, i.e. +10 days by 9 p.m.

6. Libraries description

6.1. Folder description

Archive contains following folders:

- Data – contains scripts to emulate 3001 and 2001 requests and parse those responses;
- Shop – contains scripts to emulate 1002 and 1102 requests and parse those responses;
- Src – contains libraries source codes.

Here is links to libraries:

https://www.luminor.lv/sites/default/files/corporate_remote_banking/documents/Java.zip
https://www.luminor.lv/sites/default/files/corporate_remote_banking/documents/net.zip
https://www.luminor.lv/sites/default/files/corporate_remote_banking/documents/php.zip

6.2. PHP and Java

6.2.1. Class InordLink

Base class for client libraries API. Its methods are not used directly.

6.2.2. Class AuthorizationRequest

Class process response from the Bank for 2001 "Customer authorization in external system" request and 3001 «Request for customer data».

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 3. Additional parameter is pPub – path to Bank public PKCS#8 certificate in PEM format.
decode	Method is used to check response integrity using v_mac parameter and corresponding cipher algorithm.

6.2.3. Class CustomerDataRequest

Class generates request to the Bank for 3001 «Request for customer data».

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 4. Additional parameter is pPriv – path to merchant private PKCS#8 certificate in PEM format.

6.2.4. Class OrderRequest

Class generates request to the Bank for 1002 «Data for payment order» request.

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 1. Additional parameter is pPriv – path to merchant private PKCS#8 certificate in PEM format.

6.2.5. Class OrderResponse

Class process response from the Bank 1102 «Payment status» request.

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 2. Additional parameter is pPub – path to Bank public PKCS#8 certificate in PEM format
decode	Method is used to check response integrity using v_mac parameter and corresponding cipher algorithm.

6.3. .NET

6.3.1. *Class InordLink*

Base class for client libraries API. Its methods are not used directly.

6.3.2. *Class AuthorizationRequest*

Class process response from the Bank for 2001 “Customer authorization in external system” request and 3001 «Request for customer data».

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 3. Additional parameter is pPub – path to Bank public PKCS#8 certificate in PEM format.
decode	Method is used to check response integrity using v_mac parameter and corresponding cipher algorithm.

6.3.3. *Class CustomerDataRequest*

Class generates request to the Bank for 3001 «Request for customer data».

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 4. Additional parameters are: • pPriv – path to merchant private PKCS#12 certificate; • pPass – password to merchant PKCS#12 certificate.

6.3.4. *Class OrderRequest*

Class generates request to the Bank for 1002 «Data for payment order» request.

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 1. Additional parameters are: • pPriv – path to merchant private PKCS#12 certificate; • pPass – password to merchant PKCS#12 certificate.

6.3.5. *Class OrderResponse*

Class process response from the Bank 1102 «Payment status» request.

Method name	Description
Constructor	For initialization main constructor is used, parameters are mentioned in Table 2. Additional parameter is pPub – path to Bank public PKCS#8 certificate in PEM format.
decode	Method is used to check response integrity using v_mac parameter and corresponding cipher algorithm.

7. Requirements with regard to the Bank’s logo and profile, link design and deployment in web site

The Merchant shall place on its site the Bank’s profile and logo in compliance with the Bank requirements:

- Shall be indicated the Bank’s name – LUMINOR banka (please, note the use of upper case and lower case letters!);
- Shall be employed the Bank’s profile as placed on the Bank’s website under “Corporate - Remote services - LUMINOR Link” (doti .gif and .eps formats).