e-Link Technical Specification

Valid from 8th of December, 2020

1. General information

Client (Merchant) – SEB banka's Client who signed e-Link agreement with the Bank.

Bank – AS SEB banka.

User – SEB Internet bank user and Merchant Client (WEB page visitor).

e-Link channel – SEB API (application program interface) that ensures online connection between the Client's (Merchant) E-System and the Bank system. e-Link is designed for companies that are offering online services and wish to collect payments for purchases using e-Link **e-Payment service** or to authenticate the WEB page visitors via SEB internet bank using e-Link **e-Identification service.**

E-system – Client's system that ensures data exchange via e-Link channel between the Bank and the Client (Merchant) using HTTPS requests and responses. Client sends to the Bank HTTPS requests and Bank sends back to E-system responses in a HTTPS form.

Certificates – e-Link service uses two types of certificates:

1. *Transport certificate* that ensures channel encryption and secure connection. Client HTTPS server has to run certificate issued by one of the certificate authorities listed in CA/Browser Forum - https://cabforum.org/members/.
2. *Message signing certificate* (Public Key) that is used to verify message integrity. Client must generate and provide to the Bank self-signed certificate (Public Key). Different tools can be used to create certificate archive: *OpenSSL CSR Tool*, *KeyStore Explorer*, etc. Bank will sign response messages with valid Bank's Public Key that is provided in the Specification. e-Link message signing examples in JAVA and PHP are availavle in SEB banka web page www.seb.lv.

2. Message signing

2.1. Message Signing Certificate

Client has to provide to the Bank valid message-signing certificate (**Public key**) and send it to the Bank's e-mail address ecommerce@seb.lv from the Client's e-mail address that is indicated in the Agreement. It is recommended for Public Key to be at least 2048 bit long with maximum validity period - 3 years. Please keep certificate Private Key secure by preventing third party access. **DO NOT SEND** IT TO THE BANK OR OTHER THIRD PARTY!

Bank will store Client Public Key in the Bank's system and will use it for Client's requests messages verification (that message is signed with correct key). E-system signs every request message with Client Private Key that corresponds to the Client Public Key that is stored in the Bank's system and sends it to the Bank's URL address:

https://ibanka.seb.lv/ipc/epakindex.jsp

Based on the Client requests Bank prepares response messages, signs them with the Bank Private Key, that corresponds to the following Bank's Public Key:

-----BEGIN CERTIFICATE-----
MIIB9TCCAV4CCQC7RlKZ7y4JPTANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJM
VjENMAsGA1UEBwwEUmlnYTERMA8GA1UECgwIU0VCIGJhbmsxDjAMBgNVBAMMBVNF
QlVCMB4XDTE2MDcxODA4NTQxM1oXDTIxMDYyMjA4NTQxM1owPzELMAkGA1UEBhMC
TFYxDTALBgNVBAcMBFJpZ2ExETAPBgNVBAoMCFNFQiBiYW5rMQ4wDAYDVQQDDAVT
RUJVQjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA3gfAFe64YIu21x2UOTby
stFPMo7TFRWd7oW1L1YQWLHQuNVOh1kjrQWehECyK8cyX1hdHXPoAY3B2Virgj8U
g70ZfO6QQx9zifhlN0gbxRdPjq5jM7Ni5RMWsIayErAhk8IjbPSINLe5l/CpVAhp
yGJWRW8CYH9c/HLsUeg0sKUCAwEAATANBgkqhkiG9w0BAQUFAAOBgQDY9hRVOZkK
957h2Ij8iwV7fIR3Nw8l+248D09xuknBrDOSYMXEDvEPKAW+CS0sQ64MOFybAFRx
YICfpu2DQkcmMM5APo79YzwMCjElRn5BsNyX7oDe4SZHbdUVqF4/mrFI3FU1KdN2
MJizE92BjvgQlJocLJePUi6jbO5YrmICkw==
-----END CERTIFICATE-----

Signed messages are sent to the Client's Feedback URL address that is stated in the request message IB_FEEDBACK field

2.2. Message Signature

Signature of the values must be attached to the messages **IB_CRC** field (e-Link messages structure and format is provided in the next paragraphs). IB_CRC string is authentication code used for identification of the Client or the Bank and is computed from message data and Private Key of the respective party (Client or Bank). The party shall verify the IB_CRC string of the other party with the Public Key by using RSA algorithm of public keys and hash algorithm SHA-1.

Client generates IB_CRC field string (e-signature) as follows:

Base64Encode (Sign (len (p1) || p1 || len (p2) || p2 || … || len (pn) || pn)))

where:

Base64Encode() – base64 encoding function;
Sign() – SHA1 with RSA signing function;
|| – concatenation of symbol lines;
p1, p2, …, pn – message parameters signed with message sender Private Key, in sequence in which they are described in the Specification before IB_CRC. Parameters IB_CRC, IB_FEEDBACK and IB_LANG are not used in e-signature generation process (message parameters and format described in next paragraphs);
len (pi) – parameter character count function.

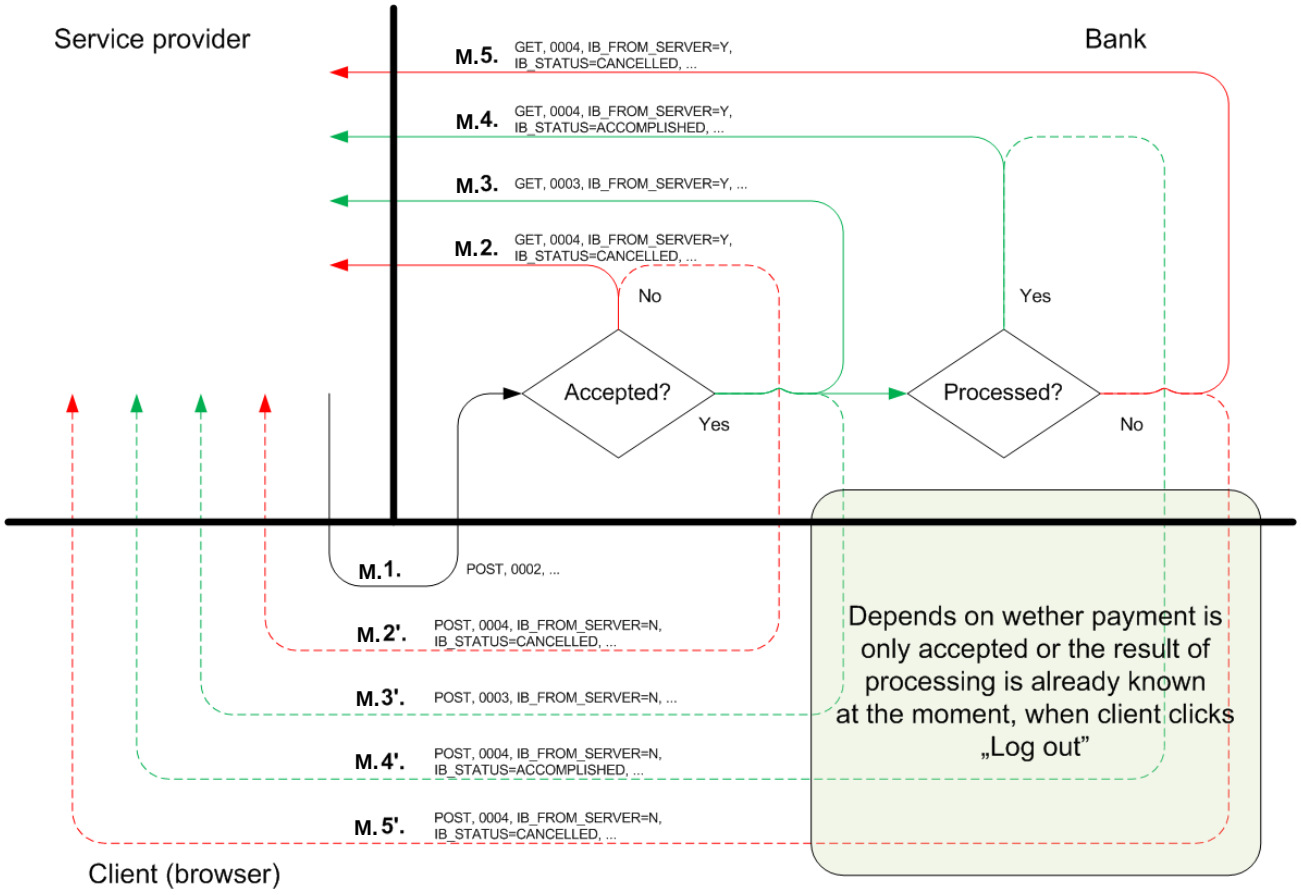
This function returns parameter length in symbols as a 3-digit line (for example, if length is 7 symbols, length must correspond to symbol line “007”, in case of zero length – “000”).

Number of symbols is determined by taking into account UTF-8 coding peculiarities: US-ASCII the first 128 symbols are coded with one byte but the remaining ones (‘ā’, ‘č’, ‘ī’, etc.) with two to four bytes.
Len function counts each of them as one symbol.
Obtained string of symbols is signed with the Private Key, by using RSA and SHA-1 functions (RFC 8017 with encoding method EMSA-PKCS1-v1_5).
The Private Key can’t be longer than 4096 bits.
Obtained binary data set is encoded with BASE64 algorithm.
Obtained value – hash in IB_CRC field is the e-signature of the message.

Recipient of the message (Client, Bank) checks if the message data corresponds to the e-signature:
- Symbol string corresponding to the received message is generated, by using mentioned algorithm;
- By using the Public Key, the obtained symbol string is compared to the received e-signature (IB_CRC string value);
- Message signing and e-signature verification functions are OpenSSL library or analogous library functions.

3. e-Payment interface

3.1. e-Payment processing scheme



Marking lines:

Green line - *the data of successful results;*
Red line - *the data of unsuccessful results;*
Continuous line - *server message where data transfer success does not depend on the User;*
Discontinued line - *data transfer success depends on User browser;*

3.2. e-Payment service process flow

e-Payment service process flow is described using Payment message format parameters that are provided below in e-Payment message format paragraph.

1. The User chooses a product/ service in e-shop and indicates SEB internet bank as means of payment. The Client must ensure that SEB logo picture in available for the Users on the Merchant portal that will redirect Users to the following Bank's Internet bank login page (URL address):

   https://ibanka.seb.lv/ipc/epakindex.jsp

2. Once User pressed on SEB logo, E-System automatically sends **M.1** Client message (IB_SERVICE=0002) to the Bank and redirects User to the SEB Internet bank login page mentioned above.
3. User authenticates to the Internet bank by entering his login data. During authentication process, the Bank checks User's log-in data and also in parallel that message sender (Client/ Merchant) has active e-Link agreement and, that Client request message is created and signed according to Specification.
4. Once the User is authenticated, the Bank opens Internet bank page with prefilled payment order that User must authorize or decline:
   4.1 In case User authorizes a payment order and then presses button "Back to the Merchant" or closes the browser, the Bank closes Internet bank session for the User and redirects him back to the Client e-shop. In parallel the

Bank accepts payment order for processing and sends to the E-system message **M.3** (with IB_SERVICE=0003, IB_FROM_SERVER=Y). The Bank' message is regarded as received by the E-system when the Bank receives from the E-system HTTP code 200. Otherwise, the Bank will continue resend **M.3** message (IB_SERVICE=0003**,** IB_FROM_SERVER=Y) every 60 seconds once again for 100 times. After that, if no successful response received the message sending from the Bank will be abandoned. Once Bank receives HTTPS code 200 from E-system, the Bank sends to E-system **M.4** message (IB_SERVICE=0004, IB_FROM_SERVER=Y, IB_STATUS=ACCOMPLISHED) informing that payment order was executed or **M.5** message (IB_SERVICE=0004, IB_FROM_SERVER=N, IB_STATUS=CANCELLED) informing that payment order is declined by the Bank.

4.2 In case payment order was cancelled by the user in the Internet bank before authorization or session was timed out, the Bank will redirect customer to the Client's E-system with **M.2'** or **M.5'** message (IB_SERVICE=0004, IB_FROM_SERVER=N) informing that payment order was not delivered to processing and was cancelled. **M.2** or **M.5** server-to-server message (IB_SERVICE=0004, IB_FROM_SERVER=Y) will be sent to E-system and E-system must return HTTP status code 200.

3.3. e-Payment message format

Client's request message - 0002

Payment order request (M.1):

Sequence	Parameter title	Max length	Example of value	Description
1	IB_SND_ID	10	COMPANY	Client Agreement ID – issued by the Bank. Constant.
2	IB_SERVICE	4	0002	Request message type. Constant 0002
3	IB_VERSION	3	001	ID of digital signature algorithm. Constant 001
4	IB_AMOUNT	17	1234.56	Payment amount
5	IB_CURR	3	EUR	Payment currency (EUR)
6	IB_NAME	30	SIA Company	Merchant name (in this case: SIA Company)
7	IB_PAYMENT_ID	20	UB0000000000015	Payment order reference number
8	IB_PAYMENT_DESC	100	Invoice No. 1234 is paid	Payment order description
9	IB_CRC	500	C/DBTOY70OJK5NX1AN9	E-signature hash
10	IB_FEEDBACK	150		Client URL stated in Agreement, to which the Bank will send server messages with payment parameters and status
11	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)

Bank's response message - 0003

Payment order acceptance for processing (M.3):

Sequence	Parameter title	Max length	Example of value	Description
1.	IB_SND_ID	10	SEBUB	Bank ID. Constant SEBUB
2.	IB_SERVICE	4	0003	Response message type: Constant 0003
3.	IB_VERSION	3	001	ID of digital signature algorithm. Constant 001
4.	IB_PAYMENT_ID	20	UB0000000000015	Payment order reference number
5.	IB_AMOUNT	17	1234.56	Payment amount
6.	IB_CURR	3	EUR	Payment currency (EUR)
7.	IB_REC_ID	10	COMPANY	Client Agreement ID – issued by the Bank. Constant.
8.	IB_REC_ACC	21		Client (Merchant) payment collection account (IBAN).
9.	IB_REC_NAME	30	SIA Company	Client name (in this case: SIA Company)
10.	IB_PAYER_ACC	21		Payer's account (IBAN)
11.	IB_PAYER_NAME	110	Jānis Ozols	Payer's name
12.	IB_PAYMENT_DESC	100	Invoice No.1234 is paid	Payment order description
13.	IB_PAYMENT_DATE	10	12.12.2005	Payment confirmation date (DD.MM.YYYY)
14.	IB_PAYMENT_TIME	8	21:12:34	Payment confirmation time (HH:MM:SS).
15.	IB_CRC	500		E-signature hash
16.	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)
17.	IB_FROM_SERVER	1	Y / N	In case of M.4 –**Y** (ACCOMPLISHED); M.5 – Y (CANCELLED);

Bank's response message - 0004

Payment order status (M.2, M.4 or M.5):

Sequence	Parameter title	Max length	Example of value	Description
1.	IB_SND_ID	10	SEBUB	Bank ID. Constant SEBUB
2.	IB_SERVICE	4	0004	Response message type: Constant 0004
3.	IB_VERSION	3	001	ID of digital signature algorithm. Constant 001.
4.	IB_REC_ID	10	COMPANY	Client Agreement ID – issued by the Bank. Constant.
5.	IB_PAYMENT_ID	20	UB0000000000015	Payment order reference number
6.	IB_PAYMENT_DESC	100	Invoice No. 1234 is paid	Payment order description
7.	IB_FROM_SERVER	1	Y/ N	In case of M.4 – **Y (**ACCOMPLISHED); M.2 - M.5 – **N** (CANCELLED)
8.	IB_STATUS	12	ACCOMPLISHED	Payment order status: (ACCOMPLISHED / CANCELLED)
9.	IB_CRC	300	C/DBTOY70OJK5NX1AN9	E-signature hash
10.	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)

Client's E-System have to read all Bank's response message values that are stated in this Specification and must verify certain fields values according to following rules:

- IB_REC_ID – verify that response message is addressed exactly to that Client (merchant);
- IB_CRC – verify that message e-signature comply to valid Bank's public key stated in this Specification;
- IB_SND_ID – verify that Bank's response message contains Bank's constant ID value – SEBUB in that field;
- IB_DATE and IB_TIME – verify that Bank's response message is not too old to avoid the situation that message could be reused again to access E-system.

4. e-Identification interface

4.1. e-Identification service process flow

1. The User visits Merchant portal and chooses option to login to Merchant portal using SEB Internet bank authentication. The Client must ensure that SEB logo picture in available for the Users on the Merchant portal and will redirect Users to the following Bank's Internet bank login page (URL address):

   https://ibanka.seb.lv/ipc/epakindex.jsp

2. Once User pressed on SEB logo, E-System automatically sends request message IB_SERVICE=0005 to the Bank and redirects User to the SEB Internet bank login page stated above.
3. User authenticates to the Internet bank by entering his login data. During authentication process, the Bank checks User's login data and in parallel also that message sender (Client/ Merchant) has active e-Link agreement, and that Client request message is created and signed according to Specification.
4. Once the User is authenticated, the Bank opens Internet bank page where User must give or decline consent to the Bank for forwarding his personal data to the Merchant.
   4.1 If User agrees to provide such a consent, the Bank sends IB_SERVICE=0001 response message to the E-System's URL address that is indicated in the Agreement and redirects User to the Merchant portal. Internet bank session for the User is closed.
   4.2 If User does not agree to provide a consent, the Bank sends IB_SERVICE=0008 response message to the E-System's URL address that is indicated in the Agreement and redirects User to the to the Internet bank login page. Internet bank session for the User is closed.

4.2. e-Identification message format

Client's request message 0005:

Client (merchant) requests user personal data from the Bank

Sequence	Name of parameter	Max length	Example of value	Description
1.	IB_SND_ID	10	COMPANY	Client Agreement ID – issued by the Bank. Constant
2.	IB_SERVICE	4	0005	Request message type. Constant 0005
3.	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)

Bank's response message 0001:

User provides consent to the Bank

Sequence	Name of parameter	Max length	Example of value	Description
1.	IB_SND_ID	10	SEBUB	Bank ID. Constant SEBUB
2.	IB_SERVICE	4	0001	Response message. Constant 0001
3.	IB_REC_ID	10	COMPANY	Client Agreement ID – issued by the Bank. Constant.
4.	IB_USER	16	050505-12123	User's personal identification code
5.	IB_DATE	10	05.12.2017	Date of creating request (format DD.MM.YYYY)
6.	IB_TIME	8	10:00:00	Time of creating request (format HH:MM:SS)
7.	IB_USER_INFO	300	ID=050505-12123; NAME=JOHN DOE ID=40000000000; NAME=SIA COMPANY; USER=JOHN DOE	User's data format (private user): ID=<person ID>; NAME=<Name Surname>; User's data format (business user); ID=<Registration No.>; NAME=<Company name>; USER=<Name Surname>
8.	IB_VERSION	3	001	ID of e-signature algorithm. Constant 001
9.	IB_CRC	500	C/DBTOY70OJK5NX1AN	E-signature hash
10.	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)

Bank's response message 0008:

User do not provide consent to the Bank

Sequence	Name of parameter	Max length	Example of value	Description
1.	IB_SND_ID	10	SEBUB	Bank ID. Constant SEBUB
2.	IB_SERVICE	4	0008	Response message. Constant 0008
3.	IB_LANG	3	LAT	Language (possible values: LAT/ ENG/ RUS)

Client's E-System have to read all Bank's response message values that are stated in this Specification and must verify certain fields values according to following rules:

- IB_REC_ID – verify that response message is addressed exactly to that Client (merchant);
- IB_CRC – verify that message e-signature comply to valid Bank's public key stated in this Specification;
- IB_SND_ID – verify that Bank's response message contains Bank's constant ID value – SEBUB in that field;
- IB_DATE and IB_TIME – verify that Bank's response message is not too old to avoid the situation that message could be reused again to access E-system.

Customer service

Working days at 9.00 – 17.00
Telephone: 67779993;
E-mail: ecommerce@seb.lv, info@seb.lv