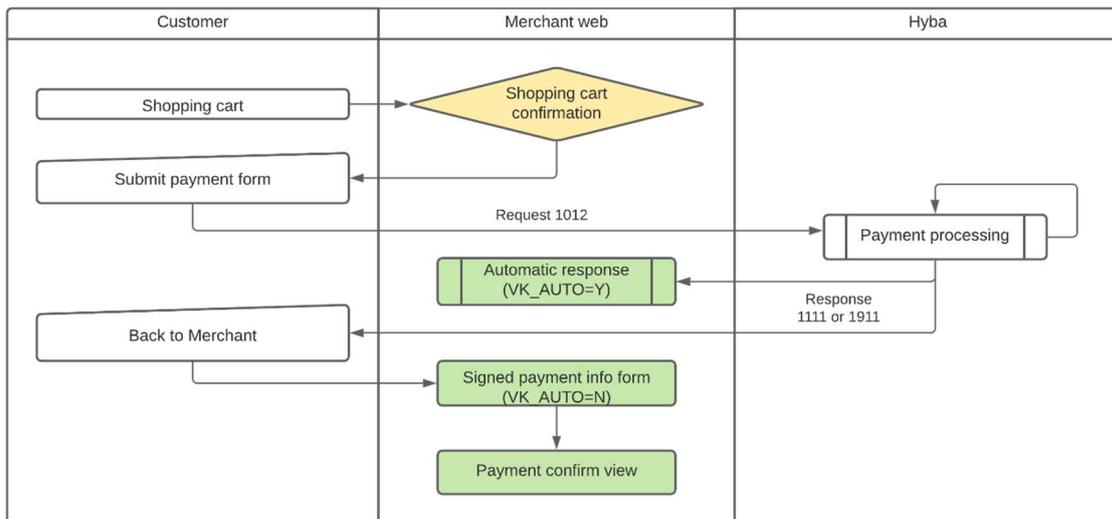


HyBa Payment Technical Specification

<i>Last updated</i>	03.08.2021
<i>Version</i>	1.12
<i>HyBa service URL</i>	POST https://hyba.ee/banklink/
<i>WooCommerce plugin</i>	https://hyba.ee/wp-content/uploads/2021/08/hyba-for-woocommerce.zip
<i>Assets archive</i>	https://hyba.ee/wp-content/uploads/2021/07/HyBa-payment-assets.zip

Table of Contents

HyBa payment Technical Specification	1
Requirements for the Merchant website	2
Exchange of public keys.....	2
HyBa Pay Queries	4
Finding the VK_MAC control code.....	4
IPizza Query Specification.....	4
Query 1012 (Payment initiation request).....	4
Query 1111 (Payment success response).....	5
Query 1911 (Payment failure response).....	6
HyBa payment CVI.....	7
HyBa payment assets download.....	7
Usage example & code libraries	8
Usage in WooCommerce.....	8
Example code & libraries.....	8



Requirements for the Merchant website

HyBa payment enables merchant customers to initiate payment using HyBa financial services.

Bank Link requests are HTTP POST requests with specified parameters. Each query contains a service number. Each service has its own list of parameters and query parameters. Requests from the Merchant to HyBa will be directed to the URL: <https://hyba.ee/banklink/> (if you use multiple HyBa payment banklinks then consult with representative which appendix to add in the end).

It's using the IPizza standard that is easily integrate with Baltic banklinks and commonly used. An existing Baltic banklink IPizza integration can be used/extended to add HyBa integration into existing solutions.

HyBa payment method	Service URL	Minimum checkout amount
PAY	https://hyba.ee/banklink/pay	1 EUR
SPLIT	https://hyba.ee/banklink/split	100 EUR
PLAN	https://hyba.ee/banklink/plan	300 EUR

For Merchant onboarding, please visit and apply for integration.

Contacts for contract & onboarding

E-mail (primary) partner@hyba.ee
 Phone +372 600 2021

Exchange of public keys

Once the contract is set and details agreed on how to exchange keys, please proceed with the following manual.

The client must generate its own key pair corresponding to the X.509 standard. We recommend that you create the key based on the following conditions:

- Signature algorithm - SHA1RSA
- Public key - RSA (2048 bits)
- Validity not exceeding 10 years

HyBa accepts a certificate request or a so-called self-signed certificate. Public keys are exchanged upon entry into the agreement. HyBa sends a public key certificate to the merchant, which the customer must enter into the system and validates the packages sent by HyBa.

The key pair can be generated from the command line using the openssl utility:

```
openssl genrsa 2048> privkey.pem  
openssl req -new -key privkey.pem -out cert-req.pem
```

The generated public key must be sent to HyBa and then the HyBa payment instrument will be activated.

HyBa Pay Queries

This document sets out the query specifications, in which each service has its own list of parameters. To create a working service, you must not add any parameters that are not specified in the specification and follow the instructions in the document.

- The length of the field value must not exceed that specified in the specification. If the length is exceeded, the request will not be processed.
- Field value lengths are in symbols.
- The field value may be shorter than maximum length allows, missing spaces will not be filled.
- Failure to describe a parameter required in the service specification counts it as an empty field.
- The data should be sent in UTF-8 encoding (VK_ENCODING).
- The dot is used as decimal separator in the amounts.
- Date and time are presented in the DATETIME ex 2021-01-01T10:06:01+0200 (ISO 8601 standard) with the precision of second and with the time zone.

Finding the VK_MAC control code

The calculation of the **VK_MAC** with the electronic signature used in the queries is based on an agreed algorithm. The version of the algorithm is determined by the query parameter **VK_VERSION**. Currently, only version 008 is used.

The signature **VK_MAC** is transmitted to the request in **BASE64** encoding, with **VK_MAC** (MAC008) computers including the human capture algorithm **RSA** and the hash algorithm **SHA-1**. Blank fields are "000" long.

MAC008 (x1, x2,..., xn): = RSA (SHA-1 (p (x1) || x1 || p (x2) || x2 ||... || p (xn) || xn), d, n).

x1, x2,..., xn	Query parameters
P	Function of the parameter length in symbols for queries corresponding to the new specification (1012, 1111, 1911). The length is formatted as a three-digit string. In other words, length 1 on "001".
D	RSA secret exponent
n	RSA modulus
	String addition operation

IPizza Query Specification

Services for the HyBa usage.

Query 1012 (Payment initiation request)

The Merchant sends a Customer's request to HyBa for a Transaction. The payee's name and account number are taken from the agreement between HyBa and the Merchant. After a successful payment, a query "1111" is prepared for the Merchant, in case of a failed payment "1911".

No	Field name	Length	Description
----	------------	--------	-------------

1	VK_SERVICE	4	Service number (1012)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	Merchant ID
4	VK_STAMP	20	Merchant Order ID
5	VK_AMOUNT	17	Amount paid. Decimals and cents separated by a period ".". Thousands separators are not used.
6	VK_CURR	3	Currency (EUR)
7	VK_REF	35	Reference Number of the Invoice (https://www.pangaliit.ee/settlements-and-standards/reference-number-of-the-invoice)
8	VK_MSG	95	Description of the payment
9	VK_RETURN	255	URL where reply of successful transaction is sent
10	VK_CANCEL	255	URL where reply of failed transaction is sent
11	VK_DATETIME	24	Date and time of the payment order in ISO 8601 format to the nearest second with time zone information (2021-01-21T12:11:16+0200)
	VK_MAC	700	Control signature
	VK_ENCODING	12	Content encoding (UTF-8)
	VK_LANG	3	Language code (EST, ENG, RUS)
	VK_PHONE	15	(optional data) Customer valid mobile number with country code
	VK_IDCODE	11	(optional data) Customer personal identity code
	VK_EMAIL	320	(optional data) Customer e-mail address

Query 1111 (Payment success response)

Used to respond to the execution of a payment order.

No	Field name	Length	Description
1	VK_SERVICE	4	Service number (1111)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	Bank ID
4	VK_REC_ID	15	Merchant ID
5	VK_STAMP	20	Merchant Order ID
6	VK_T_NO	20	Payment transaction identifier
7	VK_AMOUNT	12	Amount paid. Decimals and cents separated by a period ".". Thousands separators are not used.
8	VK_CURR	3	Currency (EUR)
9	VK_REC_ACC	34	Recipient's account number
10	VK_REC_NAME	70	Recipient's name
11	VK_SND_ACC	34	Remitter's account number
12	VK_SND_NAME	70	Remitter's name
13	VK_REF	35	Reference Number of the Invoice (https://www.pangaliit.ee/settlements-and-standards/reference-number-of-the-invoice)
14	VK_MSG	95	Description of the payment
15	VK_T_DATETIME	24	Date and time of the payment order in ISO 8601 format to the nearest second with time zone information (2021-01-21T12:11:16+0200)
	VK_MAC	700	Control signature

	VK_ENCODING	12	Content encoding (UTF-8)
	VK_LANG	3	Language code (EST, ENG, RUS)
	VK_AUTO	1	Y = automatic response sent by the bank N = response with the customer's movement back to the merchant's page

Query 1911 (Payment failure response)

Used to report a failed transaction.

No	Field name	Length	Description
1	VK_SERVICE	4	Service number (1911)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	Bank ID
4	VK_REC_ID	15	Merchant ID
5	VK_STAMP	20	Merchant Order ID
6	VK_REF	35	Reference Number of the Invoice (https://www.pangaliit.ee/settlements-and-standards/reference-number-of-the-invoice)
7	VK_MSG	95	Description of the payment
	VK_MAC	700	Control signature
	VK_ENCODING	12	Content encoding (UTF-8)
	VK_LANG	3	Language code (EST, ENG, RUS)
	VK_AUTO	1	Y = automatic response sent by the bank N = response with the customer's movement back to the merchant's page

HyBa payment CVI

Front page icon, placed on the home page of the store



Icon "alt" attribute text: "HyBa payment", "HyBa (product name) button" (if payment PAY, then "HyBa PAY button").

The link from the icon on the page <https://hyba.ee> opens in a new window or after clicked additionally confirm purchase. The link recommended name "HyBa" or brand name with payment method extension ("HyBa PAY").

Icon to initiate the payment



The HTML code is placed in the form element together with the electronic payment order data.

HyBa payment assets download

Archive: <https://hyba.ee/wp-content/uploads/2021/07/HyBa-payment-assets.zip>

Download suitable **assets archive** from and name title HyBa payment in e-shop settings based on used payment method:  <https://hyba.ee/wp-content/uploads/2021/07/HyBa-payment-assets.zip>.

Supported files are in format **.png, .svg** and in measurements: **88x31, 120x60**.

Examples:

- if used HyBa **PAY** payment, then choose suitable format PAY asset, name title "Osta kohe, maksa hiljem. 0 € lisakulu!"; description "HyBa PAY - osta kohe, maksa 60 päeva jooksul. Ilma ühegi lisatasuta!"; Sample file names usage for PAY based on which fits the best for you: "HybaPay_logo_asetus3_valgel_taustal_r6huga_toode_rgb", "HybaPay_logo_asetus3_lillal_taustal_r6huga_toode_rgb", "HybaPay_logo_asetus1_valgel_taustal_r6huga_toode_rgb", "HybaPay_logo_asetus1_lillal_taustal_r6huga_toode_rgb";
- if used HyBa **PAY** payment and asset does not fit well to your e-shop, then choose **HyBa asset** and name title and description regarding used payment method;
- if used HyBa **SPLIT** payment, then choose suitable format SPLIT asset, name title: "Osta kohe, maksa osadena. 0 € lisakulu!", description: "HyBa SPLIT - osta kohe, maksad 3 või 6 osas. Ilma ühegi lisatasuta!";
- if used HyBa **PLAN** payment, then choose suitable format SPLIT asset, name title: "Osta kohe, maksa osadena", description: "HyBa PLAN - osta kohe, maksa mitmes osas";
- if used HyBa other payment, then choose from assets folder that specific payment asset icon, add payment method name, description regarding instruction in email from HyBa representative;

- if used **multiple HyBa payment methods**, then choose HyBa named asset and name title “HyBa nutikas makseviis” or “HyBa – osta kohe, maksa hiljem makseviis” or “HyBa makseviis”.

Usage example & code libraries

PS: due to each ecommerce platform and plugin differences setup and usage might be different.

Usage in WooCommerce

Available separate WooCommerce plugin.

Important fields common in IPizza payment modules in WooCommerce

- Service URL (Pangalingi URL), defined [here](#);
- Bank ID (Panga ID) that is [VK_SND_ID](#) value;
- Your private key (Teie isiklik privaativõti) generated as described [here](#);
- Bank public key (Panga avalik võti – given from [HyBa](#));
- [Additional fields](#) defined in the document must be integrated individually as they are not part of the standard.

The screenshot shows the WooCommerce 'Payment methods' settings page for the 'HyBa' payment method. The left sidebar contains navigation options like Home, Tellimused (29), Kliendid, Raportid, Seaded, Olek, and Laiendused. The main content area is titled 'HyBa payment' and includes the following fields:

- Description:** A text area for the checkout title. Below it is a description text: "This controls the title which the user sees during checkout."
- Pangalingi URL:** A text input field containing "https://live.hyba.ee/wp-service/". Below it is the text: "Siia läheb Pangalingi URL".
- Panga ID (VK_SND_ID):** A text input field containing "hyper". Below it is the text: "Selle saate pangast."
- Teie isiklik privaativõti:** A text area containing a long RSA private key string. Below it is the text: "Avage oma privaativõtme fail tekstiredaktoris ning kopeerige KOGU faili sisu siia lahtrisse".
- Privaativõtme parool:** A password input field. Below it is the text: "Kui Teie privaativõti on parooliga kaitstud, siis sisestage siia parool. Kui mitte, siis jätke see lahter tühjaks".
- Panga avalik võti:** A text area containing a long RSA public key string. Below it is the text: "Avage panga avaliku võtme fail tekstiredaktoris ning kopeerige KOGU faili sisu siia lahtrisse".
- Selgitus pangale:** A text input field containing "Arve nr. %s tasu". Below it is the text: "Vaikimisi: Arve nr. %s tasu, kus %s asendatakse tellimuse numbriga".

Example code & libraries

Payment libraries supporting IPizza protocol

<https://github.com/renekorss/Banklink>

<https://www.npmjs.com/package/ipizza>

<https://github.com/Voog/ipizza>

<https://github.com/BitWeb/banklink-java-sdk>