



EVP International, JSC

Service of
Payment Information Exchange and
Executing System
(PIEES)
API Version 1.1

Vilnius

August 24, 2015

Contents

Introduction.....	3
Definitions.....	3
References.....	3
Description of the PIEES service and its security.....	3
Installation of the payment transfer service.....	4
Encoding the content of a request content and sending the data.....	6
Formation of requests.....	7
Examples of error messages.....	8
Example and parameters of a payment transfer's XML request.....	8
Collection of the payment status (after processing) and sending of confirmation.....	11
Contact information.....	12

Introduction

The system of payment information exchange and executing is a service enabling Paysera clients to perform inter-bank transfers in Lithuania from their information systems.

Clients integrate the service to their information system in accordance with the parameters established by the payment institution EVP International, UAB.

Definitions

PIEES – Payment information exchange and executing system (PIEES).

Client – Owner of the account indicated in the PIEES service agreement.

EVP – The company EVP International, UAB, which provides the PIEES service.

References

No.	Name	Document number	Links
[1]	Currency name standard	ISO 4217	http://en.wikipedia.org/wiki/ISO_4217
[2]	Bank identification code (BIC)	ISO 9362	http://en.wikipedia.org/wiki/ISO_9362
[3]	IBAN account number	ISO 13616	http://en.wikipedia.org/wiki/ISO_13616
[4]	PKI (public key infrastructure)		http://en.wikipedia.org/wiki/Public_key_infrastructure
[5]	REST		http://en.wikipedia.org/wiki/REST
[6]	Country codes standard	ISO 3166	http://en.wikipedia.org/wiki/ISO_3166

Description of the PIEES service and its security

This service allows performing the following operations:

- Payment transfers.

Security measures

A possibility that the security of the PIEES service would be violated in an unauthorised way (for example, decoding the private key) is much lesser than a possibility of an attempt to perform illegal actions by a person having access to the program. The latter may be the third persons to whom the user has revealed the passwords.

1. Control of the access to the computer providing the service.

There is a number of software measures which may be used to control the use of passwords and user's rights. If possible, a register should be kept for registering related information.

2. The number of program users must be minimal.

Carefully consider the users before granting the right to use the PIEES system.

3. Unnecessary users must be removed.

If an employee does not use the system at all or does not use it for a long time, remove the user or restrict the login to the system.

4. Make backup copies of data.

This measure allows escaping technical problems but does not protect from malicious or illegal activities.

Safety requirements for the usage of certificates

In order to safely use the connection and security certificates, the Client must comply with the following security requirements:

- Certificates must be used only in accordance with their purpose;
- Certificates must be used only during their security period;
- The Client must ensure that the signature formation data would not be used by other persons;
- The Client must immediately request to terminate the validity of certificates in the following cases:
 - The control of the signature formation data has been lost;
 - Certificate activation data has been revealed;
 - The data contained in the certificates is incorrect.

Installation of the payment transfer service

Service referral address: <https://gateway.paysera.com>

This service is a data transfer channel, where request and response data is exchanged between EVP and the Client. PIEES operates using the HTTPS protocol, REST[5] style, and PKI[4] authentication.

Loading of payment transfer. PUT request.

Method	URL address	Explanation
PUT	https://gateway.paysera.com/api/v1/transfer	Sending of XML data

Content of the request:

- Header
- Body
- Response codes:
 - 200 – OK
 - 403 – Invalid authentication
 - 406 – Invalid request
 - 500 – Internal error

Header parameters of the request

Parameter	Type	Description
X-Client-ID	integer	Client's ID in Paysera.com API system. Paysera.com issues this ID by a separate message.
X-Timestamp	timestamp	Time of the request in unix timestamp format
X-Nonce	string	Unique value of each request
X-Sign	string	Signature of the request

Using the PUT method, XML or *.mokesis document (described below) is included in the body of the request.

Receipt of payment status. GET and DELETE requests

The data of the received EVP responses are comprised from two parts:

1. Together with GET request, the data of the response is received.
2. Together with DELETE request, the confirmation about the receipt of the response message must be sent.

GET request

Method	Address	Explanation
GET	https://gateway.paysera.com/api/v1/transfer/status	The request which returns the payment transfer status in a row.

Content of the request:

- Header
- Body
- Response codes:
 - 200 – OK
 - 403 – Invalid authentication
 - 404 – There are no messages
 - 406 – Invalid request
 - 500 – Internal error

In this case there are no parameters of the request, only responses will be received.

Request DELETE

Method	Address	Explanation
DELETE	https://gateway.paysera.com/api/v1/transfer/status/{statusId}	The request used to confirm the received message.

Content of the request:

- Header
- Body
- Response codes:
 - 200 – OK
 - 403 – Invalid authentication
 - 404 – There are no messages
 - 406 – Invalid request
 - 500 – Internal error

Header parameters of the request

Header	Type	Description
X-Client-ID	integer	Client's ID in Paysera.com API system. Paysera.com issues this ID by a separate message.
X-Timestamp	timestamp	Time of the request in unix timestamp format
X-nonce	string	Unique value of each request
X-Sign	string	Signature of the request

Encoding the content of a request content and sending the data

Types of data

Types of data used in the PIEES service:

Complex view – complex type of data, i.e. the type of data is comprised on the basis of other elements.

A – Only text is allowed to enter.

N – Only number is allowed to enter.

AN(0-100) – The type of data may be comprised from characters and figures, the minimum allowed value of which is indicated in brackets.

D – Type of the date

- The numbers of the accounts correspond to IBAN format [3]
- Data format is YYYY-MM-DD, where YYYY is the year, MM is the month, DD is the day.
- Two positions are designed for the code of the country [6]
- Three positions are designed for the currency code [1], for example: EUR, USD
- Encoding of symbols – UTF-8

Required and optional fields are marked as follows:

1..1 – Required field;

0..1 – Optional field. It is allowed to indicate only one element;

1..* - Required field. It is allowed to indicate one or more elements;

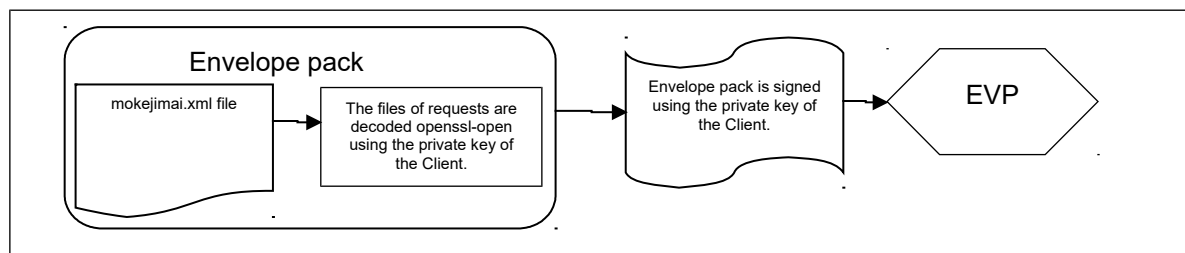
0..* - Optional field. It is allowed to indicate no elements or one or more elements.

All these rules are applied both to the provided data and the responses.

Sending a request (file) to EVP

The content of a request must be encoded as follows:

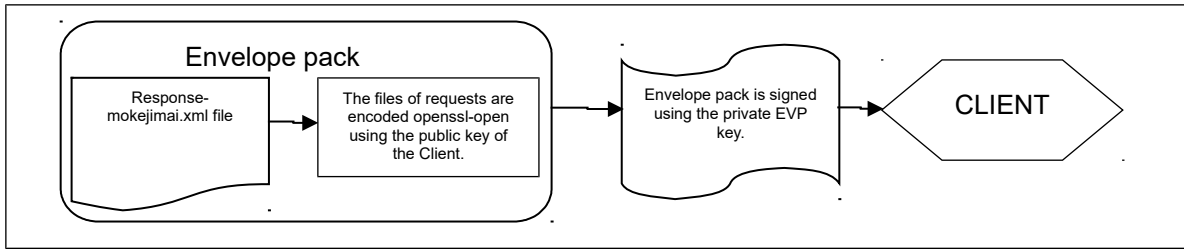
1. The files of requests are encoded openssl-seal using the public key of EVP.
2. Envelope pack is signed by the private key of the Client's service.



Sending a response to the Client

The content of a request must be encoded as follows:

1. The files of requests are encoded openssl-seal using the public key of the Client.
2. Envelope pack is signed by the private key of the EVP service.



Structure of sent ENVELOPE pack

```

<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-envelope-v1.xsd">
  <Envelope>
    <Keys>
      <Key>Generated key, encrypted with public key and encoded in Base64</key>
    </Keys>
    <Data>Data, encrypted with generated key and encoded in Base64</Data>
  </Envelope>
</TGW>
  
```

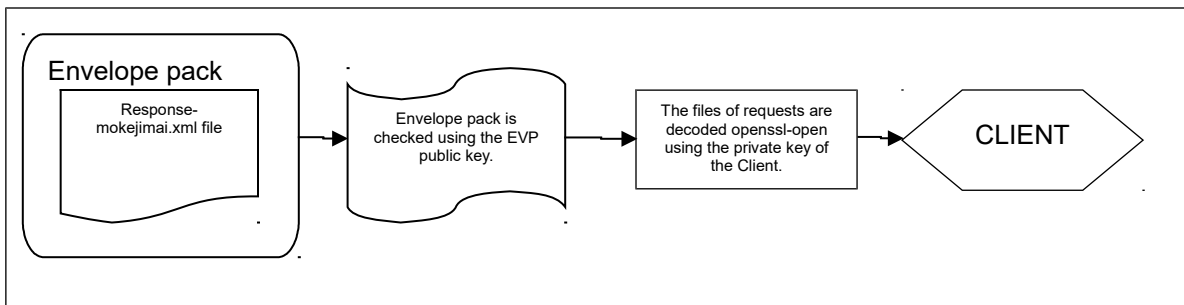
Explanation of parameters

XML message element	Type of data	Insistence	Description
Envelope	Complex view	1..1	Sent pack
Envelope/Keys	Complex view	1..1	View of encoded keys
Envelope/Keys/Key	AN	1..*	Encoded key to data
Envelope/Data	AN	1..1	Encoded data

Decoding of the response to a request

The response is decoded as follows:

1. Envelope pack is checked using the EVP public key.
2. The files of requests are decoded openssl-open using the private key of the Client.



Formation of requests

Generation of X-Sign parameter

In order to ensure the integrity of the data, a request is signed with the private key of a Client, interlinking timestamp, nonce and the content of the request, using ':' symbol.

Examples of error messages

The response is sent to PUT, GET, DELETE requests.

Example of unsuccessful response

```
<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-response-
v1.xsd">
  <Response>
    <Failure>
      <Code></Code>
      <Message></Message>
    </Failure>
  </Response>
</TGW>
```

Used error messages (the list is being specified)

Error message	Description
-	-

Example of successful response

```
<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-response-
v1.xsd">
  <Response>
    <Success/>
  </Response>
</TGW>
```

Example and parameters of a payment transfer's XML request

```
<?xml version="1.0" encoding="UTF-8"?>
<TransferRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-
v1.xsd">
  <Transfer>
    <Id>Id</Id>
    <Date>YYYY-MM-DD</Date>
    <Amount>0.0</Amount>
    <Currency>Currency</Currency>
    <Details>Details</Details>
    <Payer>
      <Iban>Iban</Iban>
      <Name>Name</Name>
      <Code>Code</Code>
    </Payer>
    <PayerBic>PayerBic</PayerBic>
    <PrimaryPayer>
      <Iban>Iban</Iban>
      <Name>Name</Name>
      <Code>Code</Code>
    </PrimaryPayer>
    <Beneficiary>
      <Iban>Iban</Iban>
      <Name>Name</Name>
```



```

<Code>Code</Code>
<BankAddress>BankAddress</BankAddress>
<BeneficiaryAddress>BeneficiaryAddress</BeneficiaryAddress>
</Beneficiary>
<BeneficiaryBic>BeneficiaryBic</BeneficiaryBic>
<FinalBeneficiary>
  <Iban>Iban</Iban>
  <Name>Name</Name>
  <Code>Code</Code>
</FinalBeneficiary>
<ReferenceNumber>ReferenceNumber</ReferenceNumber>
<ReferenceToPayer>ReferenceToPayer</ReferenceToPayer>
<ReferenceToBeneficiary>ReferenceToBeneficiary</ReferenceToBeneficiary>
<BeneficiaryBankName>BeneficiaryBankName</BeneficiaryBankName>
</Transfer>
</TransferRequest>

```

Explanation of parameters

XML message element	Type of data	Insistence	Description
Transfer	Complex view	1..1	Single transaction
Transfer/Id	AN(1-50)	1..1	Unique payment transfer number
Transfer/Date	D	1..1	Date of payment transfer. Format YYYY-MM-DD
Transfer/Amount	N	1..1	Sum of payments. Format: 10.00
Transfer/Currency	A(3)	1..1	Currency names standard [1] according to ISO 4217
Transfer/Details	AN(1-300)	1..1	Purpose of payment transfer.
Transfer/Payer	Complex view	1..1	Payer
Transfer/Payer/Iban	AN(4-35)	1..1	Payer's IBAN account number [4] according to ISO 13616
Transfer/Payer/Name	AN(1-200)	1..1	Payer's name and surname / Company name
Transfer/Payer/Code	N(1-11)	0..1	Payer's personal number / Company registration number
PayerBic	AN(8-11)	0..1	Payer's bank identification code (SWIFT) [2]
Transfer/PrimaryPayer	Complex view	0..1	Primary payer. Please indicate if the payer is only an agent.
Transfer/PrimaryPayer/Iban	AN(4-35)	1..1	Primary payer's IBAN account number [4] according to ISO 13616
Transfer/PrimaryPayer/Name	AN(1-200)	1..1	Primary payer's name and surname / Company name
Transfer/PrimaryPayer/Code	N(1-11)	0..1	Primary payer's personal number / Company registration number
Transfer/Beneficiary	Complex view	1..1	Payment beneficiary
Transfer/Beneficiary/Iban	AN(4-35)	1..1	Beneficiary's IBAN account number [4] in accordance to ISO 13616
Transfer/Beneficiary/Name	AN(1-200)	1..1	Beneficiary's Name Surname / Company name
Transfer/Beneficiary/Code	N(1-11)	0..1	Beneficiary's personal code / Company code
Transfer/Beneficiary/AccountNumber	AN(1-50)	0..1	Beneficiary's account number. Not IBAN
Transfer/Beneficiary/Country	A(2)	0..1	Beneficiary's bank's country
Transfer/Beneficiary/VO	N(5)	0..1	VO code (for transfers from Russia)
Transfer/Beneficiary/INN	N(10-12)	0..1	INN code (for transfers from Russia)
Transfer/Beneficiary/KPP	N(9)	0..1	KPP code (for transfers from Russia)
Transfer/Beneficiary/CorrespondentBankAccount	AN(1-50)	0..1	Beneficiary's bank's correspondence account number
Transfer/Beneficiary/CorrespondentBankName	AN(1-200)	0..1	Beneficiary's correspondent bank's name
Transfer/Beneficiary/CorrespondentBankSwift	AN(8-11)	0..1	Beneficiary's correspondent bank's identification code (SWIFT) [2]
Transfer/Beneficiary/BankAddress	AN(1-200)	0..1	Beneficiary bank address
Transfer/Beneficiary/BeneficiaryAddress	AN(1-200)	0..1	Beneficiary address

Transfer/BeneficiaryBic	AN(8-11)	0..1	Beneficiary's bank identification code (SWIFT) [2]
Transfer/ FinalBeneficiary	Complex view	0..1	Final beneficiary. Please indicate if the payer is only an agent.
Transfer/ FinalBeneficiary/ Iban	AN(4-35)	1..1	Final beneficiary's IBAN account number [4] according to ISO 13616
Transfer/ FinalBeneficiary/ Name	AN(1-200)	1..1	Final beneficiary's name and surname / Company name
Transfer/ FinalBeneficiary/ Code	N(1-11)	0..1	Final beneficiary's personal number / Company registration number
Transfer/ ReferenceNumber	N(1-28)	0..1	Payment code
Transfer/ ReferenceToPayer	AN(1-16)	0..1	Beneficiary's code in the payer's information system
Transfer/ ReferenceToBeneficiary	AN(1-16)	0..1	Payer's code in the beneficiary's information system
Transfer/BeneficiaryBankName	AN(1-200)	0..1	Beneficiary bank name
Transfer/ChargeType	A	0..1	Payment type. Possible variants: sha (SHA) and our (OUR)

Collection of the payment status (after processing) and sending of confirmation

Payment in progress

```
<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-response-
v1.xsd">
  <TransferStatus id="">
    <Transfer id="">
      <Status>
        <Running/>
      </Status>
    </Transfer>
  </TransferStatus>
</TGW>
```

Successful payment

```
<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-response-
v1.xsd">
  <TransferStatus id="">
    <Transfer id="">
      <Status>
        <Success/>
      </Status>
    </Transfer>
  </TransferStatus>
</TGW>
```

Unsuccessful payment

```
<?xml version="1.0" encoding="UTF-8"?>
<TGW xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="tgw-response-
v1.xsd">
  <TransferStatus id="">
    <Transfer id="">
      <Status>
        <Failure>
          <Code></Code>
          <Message></Message>
        </Failure>
      </Status>
    </Transfer>
  </TransferStatus>
</TGW>
```

Used error messages (the list is being specified)

Error message	Description
-	-

Confirmation of information

After a payment response from EVP is received, always send the confirmation of receipt with DELETE request.

Contact information

Regarding the installation of the service, API inaccuracies or other information related with the service,

please contact:

EVP International, UAB
Mėnulis str. 7, Vilnius LT-04326

support@paysera.com