Digilink service technical description
(AUTHENTICATION AND PAYMENT PROCESSING INTERFACE)

version 6.0, 11.11.2019

Table of changes

Date	Protocol Version	Description
2012.08.21	2.0	- Added "Target" field to ESERVICEREQ(6.4) - Added extension with payer name and account number fields ("Name", "AccNo") to <PmtStat> in PMTSTATRESP(6.7) - Added Data Verification recommendations(8)
2014.08.25	2.21	- Removed misleading statement about < and > escaping in 4.1.3
2014.01.27	3.0	Protocol version changed to 3.0 due to Bank' s certificate renewal
2016.04.10	4.0	- Protocol version 4.0 supports Fidavista 1.2. payment format. Optional field <EndToEnd> can be used in PMTREQ messages. <EndToEnd> value is not returned back in PMTRESP and PMTSTATRESP. Value is included in account statement.
	4.1	Added Beneficiary country LT and EE
	4.2.	Amended Priority X – possibility to get immediate answer from the Bank about bank's system availability for payment processing
2017.06.15	5.0	Cryptographic algorythm changed form SHA1 to SHA256
2019.11.11	6.0	Added Location Field, Posible values LV, LT, EE

TABLE OF CONTENT

1. Used terms, abbreviations

Term	Description
External system	System (web page) of the service provider, who uses DIGI::LINK service in accordance with the concluded Agreement.
Agreement	Agreement between "Citadele banka" and the owner of the External system (Service provider) on DIGI::LINK service.
User	User of Citadele Online Banking and the External system web page.
Link	Link created in Citadele Online Banking to the External system.
FiDAViSta	Financial data exchange unified standard. For data exchange DIGI::LINK uses adjusted FiDAViSta standard http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd
AMAI	*Authentication and payment process interface.*
HTTP	*Hyper Text Transport Protocol*
HTTPS	*Secured Hyper Text Transport Protocol*
SSL	*Secure Sockets Layer*
UTF-8	*8-bit UCS/Unicode Transformation Format*.
W3C	*World Wide Web Consortium*
XML	*eXtensible Markup Language* (specially developed to work with network documents).

2. Purpose of the document

Document describes DIGI::LINK service functionality and requirements that developers should observe while creating communication between the External system and Citadele Online Banking.

3. Summary

3.1. DIGI::LINK service provides an opportunity to perform the following actions in Citadele Online Banking:
- 3.1.1. User authentication in Citadele Online Banking when logging in from the External system;
- 3.1.2. authenticated User access to the External system from Citadele Online banking (hereinafter referred to as – Access);
- 3.1.3. processing of payments created in the External system (hereinafter referred to as – Payment);
- 3.1.4. sending message on payment status.

3.2. All the above mentioned actions are based on data exchange between the Bank and the Service provider using public Internet network.

3.3. Service is provided to Citadele Online Banking Latvian users – private customers, who are LR residents, and Estonian and Lithuanian users.

3.4. Available languages: English, Latvian, Russian.

4. Data exchange

4.1. Sending data

4.1.1. HTTPS protocol is used for data exchange. Data is in the XML format, UTF-8 encoding

4.1.2. For sending data of AMAI ***AUTHREQ***, ***AUTHRESP***, ***ESERVICEREQ***, ***PMTREQ*** and ***PMTRESP*** requests, the hidden field "xmldata" (type="hidden") of the form (element <form>) and forward function in the client's browser are used.

4.1.3. Before placing information in the hidden field it should be formatted – symbol " should be replaced with '**"**'. If the '&' symbol is used in any of the fields, then double formatting should be performed – before signing the request the '&' symbol should be replaced with '**&**' and before placing information in the hidden field '**&**' should be replaced with '**&**'.

Example:

```
...
<form... >
...
<input id="xmldata" name="xmldata" value="<?xml version=&amp;quot;1.0&amp;quot; encoding=&amp;quot;UTF-8&amp;quot;
standalone=&amp;quot;no&amp;quot;?><FIDAVISTA xmlns=&amp;quot; http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2&amp;quot;
xmlns:xsi=&amp;quot;http://www.w3.org/2001/XMLSchema-instance&amp;quot; xsi:schemaLocation=&amp;quot;
http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd&amp;quot;>
<Header>
<Timestamp>20161101175959000</Timestamp>
```

<From>10000</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/"
xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>AUTHREQ</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f77</RequestUID>
<Version>6.0</Version>
<Language>LV</Language>
<ReturnURL>http://localhost/BankPortPrototype/index.jsp</ReturnURL>
<Location>LV</Location>
<SignatureData><Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-SHA256"/><Reference
URI=""><Transforms><TransformAlgorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#SHA256"/><DigestValue>lwZrJrC85wiY4gDdUfuhX20MPmg=</DigestValu
e></Reference></SignedInfo><SignatureValue>
… …
</SignatureValue><KeyInfo><X509Data><X509SubjectName>CN=Janis Berzins,OU=Sales dept.,O=E-
Shop,L=Riga,ST=Unknown,C=LV</X509SubjectName><X509Certificate> ……
</X509Certificate></X509Data></KeyInfo></Signature></SignatureData>
</Amai>
</Extension>
....
</FIDAVISTA>" type="hidden"/>
...
</form>

4.1.4. *PMTSTATRESP* is sent as HTTP request to the URL, indicated in the Agreement.

4.2. Signing of data

4.2.1. Before sending XML data it should be signed. For this purpose public and private key signature RSA algorithm and SHA256 hashing algorithm are used. To store public and private key, the X.509 certificate is used. This certificate is also used for data exchange between the involved parties, after the Agreement was signed. To format the signed XML data, XDS standard of the Web consortium W3C is used. “Enveloped” signing method will be used, signature will be placed in the “Extension” section.

4.2.2. Certificate requirements:

- Algorithm: SHA256withRSA
- Public key encoding algorithm: RSA
- Public key length: 4096

4.2.3. Certificate can be generated, for example, with the keytool help:
keytool -genkeypair -alias [alias] –keyalg RSA -keysize 4096 -keystore [keystore]
where,
alias – key name of the generated certificate in the certificate store;
keystore – certificate store name. If the store does not exist, it will be created.

4.2.4. Signature requirements: SHA256 algorithm

Signed XML example:

<?xml version="1.0" encoding="UTF-8" standalone="no"?><FIDAVISTA xmlns="
http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation=" http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp>20030905175959000</Timestamp>
<From>10000</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/
http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>AUTHREQ</Request>

<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f77</RequestUID>
<Version>6.0</Version>
<Language>LV</Language>
<ReturnURL>https://www.system-name.lv/Authorization.aspx</ReturnURL>
<Location>LV</Location>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/><SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-SHA256"/><Reference URI=""><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></Transforms><DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#SHA256"/><DigestValue>Yjix9KRLJuL8YTupicqxdf3Jnfw=</DigestValue></Reference
></SignedInfo><SignatureValue>…. … </SignatureValue><KeyInfo><X509Data><X509SubjectName>CN=Janis Berzins,OU=Sales
dept.,O=E-Shop,L=Riga,ST=Unknown,C=LV</X509SubjectName><X509Certificate>.. …
</X509Certificate></X509Data></KeyInfo></Signature></SignatureData>
</Amai>
</Extension>
</Header>
</FIDAVISTA>

4.3. Data encryption

For data encryption SSL protocol is used.

5. Process description

5.1. User authentication in Citadele Online Banking, when logging in from the External system

5.1.1. User, being on the External system web page, selects authentication type - Citadele Online Banking.
5.1.2. The External system creates and signs the AUTHREQ authentication request (see [6.2]) and forward user to Citadele Online Banking page.
5.1.3. Citadele Online Banking receives the request, performs the required verifications and if everything is all right, user is offered to log into Citadele Online Banking with his/her own user name and password.
5.1.4. Citadele Online Banking creates and signs the AUTHRESP response (see [6.3), where depending on verification result and User action (proceed or cancel), the according request processing code is placed (see [7]), and User is forwarded back to the External system web page, which address was received in the AUTHREQ request (see [6.2]).

5.2. Authenticated User forwarding from Citadele Online Banking to the External system

5.2.1. User, being in Citadele Online Banking, clicks one of the Links.
5.2.2. Citadele Online Banking creates and signs the ESERVICEREQ authorization request (see [6.4]), closes Citadele Online Banking User working session and forwards User to the External system web page in accordance with the selected Link.
5.2.3. The External system receives the request, performs the required verifications and if everything is all right authorises the User, using the information received in the request.

5.3. Payment processing

5.3.1. User, being on the External system web page, selects a payment type for the service – Citadele Online Banking.
5.3.2. The External system creates and signs the PMTREQ payment request (see [6.5]) and forwards User to Citadele Online Banking page.
5.3.3. Citadele Online Banking receives the request, performs the required verifications and if everything is all right, the User is offered to log into Citadele Online Banking with his/her own user name and password.
5.3.4. If the payment status is set to X (express), then immediate bank's core system availability for payment processing is done.

5.3.5. If verification result is unsuccessful or the User cancels registration, Citadele Online Banking creates and signs the PMTRESP response (see [6.6]) with the code 200 (see [7]) and the User is forwarded back to the External system web page, which address was received in the PMTREQ request.
5.3.6. After successful authorization payment order with information from the PMTREQ payment request is created for the User. The User can change the following information in the payment order: account, from which the payment is being performed and the document number.
5.3.7. If the User rejects a payment or activates back Link, Citadele Online Banking creates and signs the PMTRESP response with code 200 (see [7]) and User is forwarded back to the External system portal page, which address was received in the PMTREQ request.
5.3.8. After successful payment confirmation by the customer, Citadele Online Banking proceeds with payment execution, creates and signs the PMTRESP response with code 100 (see [7]) and the User is forwarded back to the External system web page, which address was received in the PMTREQ request.

Important! PMTRESP with the code 100 does not confirm successful payment processing. This means that customer has confirmed the payment and it is delivered to the Bank's system for further processing. The final status of the payment (executed, rejected) is provided with PMTSTATRESP message and is described in next chapter.

5.4. Message on payment status

5.4.1. After payment execution or its rejection in "Citadele banka", Citadele Online Banking creates the PMTSTATRESP message on payment status (see [6.7]), places in there payment status value, signs the message and sends it to the External system URL address indicated in the Agreement.
5.4.2. If the External system address is not accessible, attempts to send this message are repeated at least every hour during at least three days.

6. Data description

6.1. Data structure

6.1.1. Adjusted FiDAViSta standard is used for data exchange (http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd).
6.1.2. To transfer AMAI specific information, "Amai" element of the "Extension" element in the "Header" section is used.
6.1.3. "Amai" element scheme:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns="http://online.citadele.lv/XMLSchemas/amai/"
targetNamespace="http://online.citadele.lv/XMLSchemas/amai/" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="Amai">
<xs:complexType>
<xs:sequence minOccurs="0" maxOccurs="1">
<xs:element name="Request" minOccurs="1" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="AUTHREQ"/>
<xs:enumeration value="AUTHRESP"/>
<xs:enumeration value="ESERVICEREQ"/>
<xs:enumeration value="PMTREQ"/>
<xs:enumeration value="PMTRESP"/>
<xs:enumeration value="PMTSTATRESP"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="RequestUID" minOccurs="1" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="5"/>
<xs:maxLength value="36"/>
</xs:restriction>
```

```
</xs:simpleType>
</xs:element>
<xs:element name="Version" minOccurs="1" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="3"/>
<xs:maxLength value="5"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Language" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="LV"/>
<xs:enumeration value="RU"/>
<xs:enumeration value="EN"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="ReturnURL" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="0"/>
<xs:maxLength value="254"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="PersonCode" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="11"/>
<xs:maxLength value="11"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Person" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="0"/>
<xs:maxLength value="200"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Code" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="100"/>
<xs:enumeration value="200"/>
<xs:enumeration value="300"/>
<xs:enumeration value="400"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="Message" minOccurs="0" maxOccurs="1">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:minLength value="0"/>
<xs:maxLength value="254"/>
```

```
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="SignatureData" minOccurs="0" maxOccurs="1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

Element	Length		Type	Mandatory	Symbols allowed	Description
	Min	Max				
Request	6	11	xs:string	Yes	Possible values: AUTHREQ AUTHRESP ESERVICEREQ PMTREQ PMTRESP PMTSTATRESP	AMAI request name
RequestUID	5	36	xs:string	Yes	0-9|A-Z|a-z|-	Request unique identifier
Version	3	5	xs:string	Yes	0-9|.	Version
Language	2	2	xs:string	No	Possible values: LV RU EN LT ET	Language
ReturnURL	0	254	xs:string	In the AUTHREQ, PMTREQ requests	0-9|A-Z|a-z|/.-	Return URL
PersonCode	11	11	xs:string	In the ESERVICEREQ, AUTHRESP requests	0-9	Person code
Person	0	200	xs:string	In the ESERVICEREQ, AUTHRESP requests	A-Z|Ā-Ž	Person
Code	3	3	xs:string	In the AUTHRESP, PMTRESP requests	Possible values: 100 200 300 400	Error message code (see [7])
Message	0	254	xs:string	Mandatory, if Code=300	0-9|A-Z|a-z|.,()	Error message
SignatureData				Yes		Element for placing a signature

6.1.4. Having received a request in Citadele Online Banking or in the External system, the following verifications should be performed:

- XML signature verification;
- If the difference between the value indicated in the “Timestamp” element and current time exceeds 15 minutes, the request is not processed;
- If during last 15 minutes a request with the value indicated in the “RequestUID” element had been already registered, the request is not processed.

6.1.5. When creating a request in Citadele Online Banking, information in the “Timestamp” element is written just before XML signing and sending to the External system. Signature is placed in the “SignatureData” element.

6.2. Authentication request AUTHREQ

Request is created upon the following template:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>AUTHREQ</Request>
<RequestUID></RequestUID>
<Version>6.0</Version>
<Language></Language>
<ReturnURL></ReturnURL>
<Location>LV</Location>
<SignatureData/>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

Element	Descripton	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example "20161101175959000" Length: 17
From	Contract identifier assigned for the External system.	
Request	Request.	AUTHREQ
RequestUID	Request unique identifier.	Length: 5-36
Version	Version.	6.0
Language	Language. Possible values: LV, RU, EN, LT, ET.	Length: 2
ReturnURL	Return URL. Is used to go back to the External system web page.	Length: 0 - 254
Location	Location. Possible values: LV, LT, EE.	Length: 2
SignatureData	Element for placing a signature.	

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp>20030905175959000</Timestamp>
<From>10000</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>AUTHREQ</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f77</RequestUID>
<Version>6.0</Version>
<Language>LV</Language>
<ReturnURL>https://www.system-name.lv/Authorization.aspx</ReturnURL>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

6.3. Authentication confirmation AUTHRESP

Confirmation is created upon the following template:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>AUTHRESP</Request>
<RequestUID></RequestUID>
<Version>6.0</Version>
<Language></Language>
<PersonCode></PersonCode>
<Person></Person>
<Code></Code>
<Message></Message>
<SignatureData/>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

Element	Description	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example "20161101175959000" Length: 17
From	Identifier assigned for Citadele Online Banking.	
Request	Request.	AUTHRESP
RequestUID	Request unique identifier.	Value received in the *AUTHREQ* request.
Version	Version.	6.0
Language	Language. Possible values: LV, RU, EN, LT EE.	Length: 2
PersonCode	Person code (without a dash)	Length: 11
Person	Person – last name, first name.	Length: 0-200
Code	Authorisation request processing code (see. [7]).	Length: 3
Message	Message corresponding to the processing code.	Length: 0-254
SignatureData	Element for placing a signature.	

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp>20161101175959000</Timestamp>
<From>10001</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
```

<Request> AUTHRESP</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f77</RequestUID>
<Version>6.0</Version>
<Language>LV</Language>
<PersonCode>01010112345</PersonCode>
<Person>BĒRZIŅŠ JĀNIS</Person>
<Code>100</Code>
<Message></Message>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
</FIDAVISTA>

6.4. Request to access the External system ESERVICEREQ

Request is created upon the following template:

<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>ESERVICEREQ</Request>
<RequestUID></RequestUID>
<Target></Target>
<Version>6.0</Version>
<Language></Language>
<PersonCode></PersonCode>
<Person></Person>
<SignatureData/>
</Amai>
</Extension>
</Header>
</FIDAVISTA>

Element	Description	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example “20161101175959000” Length: 17
From	Identifier assigned for Citadele Online Banking.	
Request	Request.	ESERVICEREQ
RequestUID	Request unique identifier.	Length: 5-36
Target	Request target contract id	
Version	Version.	6.0
Language	Language. Possible values: LV, RU, EN, LT, ET.	Length: 2
PersonCode	Person code (without a dash)	Length: 11
Person	Person – last name, first name.	Length: 0-200
SignatureData	Element for placing a signature.	

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp>20161101175959000</Timestamp>
<From>10001</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>ESERVICEREQ</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f75</RequestUID>
<Target>10007</Target>
<Version>6.0</Version>
<Language>LV</Language>
<PersonCode>01010112345</PersonCode>
<Person>BĒRZIŅŠ JĀNIS</Person>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

6.5. Payment request PMTREQ

Request is created upon the following template:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTREQ</Request>
<RequestUID></RequestUID>
<Version>6.0</Version>
<Language></Language>
<ReturnURL></ReturnURL>
<Location></Location>
<SignatureData/>
</Amai>
</Extension>
</Header>
<PaymentRequest>
<ExtId></ExtId>
        <EndToEndId></EndToEndId>
<DocNo></DocNo>
<TaxPmtFlg>N</TaxPmtFlg>
<Ccy></Ccy>
<PmtInfo></PmtInfo>
<BenSet>
<Priority>N</Priority>
<Comm>OUR</Comm>
```

<Amt></Amt>
<BenAccNo></BenAccNo>
<BenName></BenName>
<BenLegalId></BenLegalId>
<BenCountry>LV</BenCountry>
</BenSet>
</PaymentRequest >
</FIDAVISTA>

Element	Description	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example "20161101175959000" Length: 17
From	Contract identifier assigned for the External system.	
Request	Request.	PMTREQ
RequestUID	Request unique identifier.	Length: 5-36
Version	Version.	6.0
Language	Language. Possible values: LV, RU, EN, LT, ET.	Length: 2
ReturnURL	Return URL. Is used to go back to the External system web page.	Length: 0 -254
Location	Location. Possible values: LV, LT, EE.	Length: 2
SignatureData	Element for placing a signature.	
PaymentRequest	*Payment data.*	
ExtId	Payment unique identifier in the External system.	
DocNo	Payment number.	
<EndToEndId>	End to end ID	Optional 0..35 xs:string
TaxPmtFlg	Flag showing whether a payment is a tax payment or not.	N
Ccy	Payment currency.	Possible values: EUR
PmtInfo	Payment details (information to a beneficiary).	Mandatory field. Symbols allowed: A-Z| a-z| Ā-Ž | ā-ž |0-9|()+. /:- ',
BenSet	*Payment beneficiary data.*	
Priority	Payment priority.	N – Standard priority. If the bank system is unavailable, the payment is accepted (PMTRESP is successful) and processed after the system is opened (it is placed in the waiting list). At the time of opening the system, the payment is processed and the corresponding PMTSTATRESP generated and sent to Merchant system. X – Urgent priority. If the bank system is unavailable, the payment is rejected and PMTRESP with code 400 -

		service is not available – sent to Merchant system. Customer is informed about unsuccessful payment. PMTSTATRESP is not generated.
Comm	Commission type.	OUR
Amt	Payment amount.	Decimals after "." 12345.00 23.45
BenAccNo	Beneficiary account number.	In Latvian IBAN format
BenName	Beneficiary name.	Symbols allowed: A-Z| a-z| Ā-Ž | ā-ž |0-9|()+. /:- ',
BenLegalId	Beneficiary registration number or tax payer ID.	Symbols allowed: A-Z| a-z| 0-9|()+. /:-',"& Max length: 13
BenCountry	Country, where beneficiary is registered, code.	LV, EE, LT

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTREQ</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f79</RequestUID>
<Version>6.0</Version>
<Language>LV</Language>
<ReturnURL>https://www.system-name.lv/Authorization.aspx</ReturnURL>
<Location>LV</Location>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
<PaymentRequest>
<ExtId>1234567890</ExtId>
<DocNo>10033</DocNo>
<TaxPmtFlg>N</TaxPmtFlg>
<Ccy>LVL</Ccy>
<PmtInfo>Pakalpojumu apmaksa</PmtInfo>
<BenSet>
<Priority>N</Priority>
<Comm>OUR</Comm>
<Amt>1.45</Amt>
<BenAccNo>LV54PARX0000000300001</BenAccNo>
<BenName>Valsts kase</BenName>
<BenLegalId>11223344556</BenLegalId>
<BenCountry>LV</BenCountry>
</BenSet>
</PaymentRequest>
```

</FIDAVISTA>

6.6. Payment confirmation PMTRESP

Confirmation is created upon the following template:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTRESP</Request>
<RequestUID></RequestUID>
<Version>6.0</Version>
<Code></Code>
<Message></Message>
<SignatureData/>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

Element	Description	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example “20161101175959000” Length: 17
From	Identifier assigned for Citadele Online Banking.	
Request	Request.	PMTRESP
RequestUID	Request unique identifier.	Value received in the *PMTREQ* request.
Version	Version.	6.0
Code	Authorisation request processing code (see [7]).	Length: 3
Message	Message corresponding to the processing code.	Length: 0 - 250
SignatureData	Element for placing a signature.	

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp>20161101175959000</Timestamp>
<From>10001</From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTRESP</Request>
<RequestUID>7387bf5b-fa27-4fdd-add6-a6bfb2599f79</RequestUID>
<Version>6.0</Version>
<Code>100</Code>
```

```
<Message></Message>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
</FIDAVISTA>
```

6.7. Message on a payment status PMTSTATRESP

Message is created upon the following template:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTSTATRESP</Request>
<Version>6.0</Version>
<SignatureData/>
</Amai>
</Extension>
</Header>
<PmtStat>
<ExtId></ExtId>
<DocNo></DocNo>
<StatCode></StatCode>
<BookDate></BookDate>
<Extension>
        <AccNo></AccNo>
        <Name></Name>
</Extension>
</PmtStat>
</FIDAVISTA>
```

Element	Description	Value
Timestamp	Date and time of creation in the YYYYMMDDHHMMSSsss format.	Example "20161101175959000" Length: 17
From	Identifier assigned for Online Banking.	
Request	Request	PMTSTATRESP
Version	Version	6.0
SignatureData	Element for placing a signature.	
PmtStat	*Payment status*	
ExtId	Payment identifier reference.	Value received in the *PMTREQ* request.
DocNo	Payment number.	Value received in the *PMTREQ* request.
StatCode	Payment status code: E – executed in the bank (booked); R – cancelled;	

BookDate	Payment execution date (only for executed payments).	
AccNo	Payer account number	
Name	Payer account name	

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<FIDAVISTA xmlns="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2 http://ivis.eps.gov.lv/XMLSchemas/100017/fidavista/v1-2/fidavista.xsd">
<Header>
<Timestamp></Timestamp>
<From></From>
<Extension>
<Amai xmlns="http://online.citadele.lv/XMLSchemas/amai/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://online.citadele.lv/XMLSchemas/amai/ http://online.citadele.lv/XMLSchemas/amai/amai.xsd">
<Request>PMTSTATRESP</Request>
<Version>6.0</Version>
<SignatureData>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
...
</Signature>
</SignatureData>
</Amai>
</Extension>
</Header>
<PmtStat>
<ExtId>1234567890</ExtId>
<DocNo>10033</DocNo>
<StatCode>E</StatCode>
<BookDate>2008-11-01</BookDate>
<Extension>
        <AccNo>LV12PARX12345443233</AccNo>
        <Name>John Doe</Name>
</Extension>
</PmtStat>
</FIDAVISTA>
```

7. Request processing codes

Codes	Description
100	Request is successfully processed.
200	User cancelled an operation.
300	System error. In this case description of an error can be found in the ‘’Message” section.
400	Service is not available. The bank’s system is closed and the payment can’t be processed immediately (EndOfDay process, technical upgrades, technical maintenance works, etc.). This error is only possible if PMTREQ is sent with Priority = X.

8. Data verification

8.1. General rules

Partner should perform the following checks:

- XML has valid signature;

- Xml must be signed with a valid Citadele Online Banking/External system certificate - The certificate the XML (x509Certificate field) is signed is the same that is provided by the bank;
- RequestUID" must be correct;
- PMTRESP/AUTHRESP/ESERVICEREQ should not have "RequestUID" that was already processed by partner system (protection against code replay attack);
- RequestUID should be the same as corresponding PMTREQ/AUTHREQ previously sent by partner system (the partner system should check that it is receiving response for the request that it has sent);
- Difference between the value indicated in the "Timestamp" element and current time should not exceed 15 minutes.

8.2. ESERVICEREQ

In addition to general rules "Target" field must be present for AMAI v2.0
"Target" value must match Contract identifier assigned for the External system.

8.3. PMTSTATRESP

ExtId value must be the same as ExtId sent in PMTREQ, otherwise payment in PMTSTATRESP should be considered irrelevant.
If PMTSTATRESP with ExtId was already processed please return http status code 200, in other case digilink will send you this PMTSTATRESP again and again.