

Example how to use PSD2 contingency mechanism

- 1. Introduction
- 2. Production URLs
- 3. 1. Login sequence example
 - 3.1. C1: Login
 - 3.1.1. Login request example
 - 3.1.2. Login request items explained
 - 3.1.3. Login OK (HTTP 200) response example
 - 3.1.4. Login failed (HTTP 40*) response example
 - 3.2. C2: Login details
 - 3.2.1. Login details request example
 - 3.2.2. Login details response example
 - 3.2.2.1. Login details response explained
 - 3.3. C3: If required: Authenticate using one time passcode
 - 3.3.1. OTP authentication request
 - 3.3.2. OTP authentication response
 - 3.4. C4: Get summary of customer's accounts
 - 3.4.1. Summary request
 - 3.4.2. Summary response
 - 3.5. Important notice about all id:s, they are only valid within session.
 - 3.6. C5: Create payment
 - 3.6.1. Request ibaninfo
 - 3.6.2. Response of the ibaninfo
 - 3.6.3. Create payment, bic needed
 - 3.6.4. Create Payment response, notice "paymentId" and "lastModifiedAt"; those are required in confirmation request
 - 3.7. C6: Confirm payment - with passcodes codes from Aktia paper codes and SMS message content
 - 3.7.1. Confirm payment 1. request - otpCode from Aktia paper codes
 - 3.7.2. Confirm payment 1. response with indication about required SMS. SMS was added 11.6.2020
 - 3.7.3. One time passcode SMS is sent to Aktia customer's mobile number
 - 3.7.4. Confirm payment 2. request - Passcode from SMS text message
- 4. Known issues and solutions

1. Introduction

The Aktia PSD2 Contingency API can be utilized to perform calls related to Account Information Services (AIS) & Payment Initiation Services (PIS), as defined by the PSD2 regulation. The API is available for AISPs, PISPs and ASPSPs: Onboarding can be requested from Aktia TPP Support at openbanking@aktia.fi.

The client authentication in Aktia's contingency mechanism is carried out with the Qualified Website Authentication Certificate (QWAC) to be used in Mutual TLS. All requests are made over https and TLS version 1.2 is mandatory.

All Contingency API operations are defined in a separate Swagger document: "Aktia_PSD2_Contingency_Mechanism_API.yaml".

This document illustrates examples on how to get started, starting with how to get a valid Aktia OpenAM access token for making API calls.

Exhaustive list of requirements to successfully use the API:

- Valid eIDAS SSL certificate (from a Qualified Trust Service Provider)
- OAuth 2.0 client_id / client_secret pair for client authentication (Basic auth)
 - Basic auth is included as a mitigation against potential brute force attacks. TPPs will be provided a valid "Authorization: Basic" header value at Onboarding time by Aktia TPP Support.
- For executing a single call for a specific Aktia customer you need to have the following information from the customer:
 - Netbank / mobile bank user id
 - Netbank / mobile bank password
 - One time paper code responses when asked for specific indexes
 - Additional One time passcode from SMS which is sent to Aktia customer's mobile phone number after successful confirmation one time paper code.

Example cert files:

TPP client certificate:
\$ cat [tpp.example.fi.crt](#)

```
-----BEGIN CERTIFICATE-----  
<CLIENT CERT>  
-----END CERTIFICATE-----
```

TPP private key for the client certificate:
\$ cat [tpp.example.fi.key](#)

```
-----BEGIN RSA PRIVATE KEY-----  
<PRIVATE KEY>  
-----END RSA PRIVATE KEY-----
```

Aktia's side CA certificates:
\$ cat mobile-auth.aktia.fi.ca.bundle.crt

```
-----BEGIN CERTIFICATE-----  
MIIDrzCCApegAwIBAgIQCDVgVpBCRrGhdWrJWZHHsJANBgkqhkiG9w0BAQUFADBhMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEExB3d3cuZGlnaWNLcnQuYy29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWw9vdcBDQTAEfw0WnjExMTAwMDAwMDBaFw0zMTEwMTAwMDAwMDBaMGEXCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYXNlbnVBAStEHD3dy5kaWdpY2VydC5jb20xIDAeBgNVBAMTF0RpZ2lDZXXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTolEqUkkPC3eQyaKl7hL0llsB CSDMAZ0ntTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97nh6Vfe63SKMI2tavegw5BmV/S10fvBf4q77uKnD0f3p4mVmFaG5cIzJLv07A6Fpt43C/dxCl/AH2hdmORBBYmgl1GNXR0r5H4idq9Joz+EkIYlVUX7Q6hL+hgkPMFT7PTl9sdl6gSzeRntwi5m30FBqOasv+zbMUZBfHWymeMr/y7vrtC0LUq7dBMtoM10/4gdW7jVg/tRvoSSiicNoxBN33shbyTapOB6jtsJletX+jkMOVjWIDAQABO2MwYTA0BgNVHQ8BAf8EBAMCAAYwDwYDVR0TAAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVBR TLTm8KPiGxvd17I90VUwHwYDVR0jBBGwFoAUA95QNVBR TLtm8KPiGxvd17I90VUwDQYJKOZiHvcNAQEFEbQADggEBAMucN6PIEIK+t1EnE9SsPTfTfTleXkIoyQY/Esr hMatudXH/vTBHl jLuG2cenTnmCmrEbXjckChzUyImZOMkXDiqW8cVpOp/2PV5Adg060/nVsJ8dW041P0jmP6P6fBtGbfYmbW0W5Bjftttep3Sp+dWOIrwCBAI+0tKIJF PnlUkiaY4IBIqDfV8NZ5YBberOgOzW6sRbc4L0na4UU+Krk2U886UAb3LuJEV0ls YSEY1QSteDws0oBrp+uvFRTP2InBuThs4pFsiV9kuXclVzDAGYsj4dzp30d8tbQk CAUw7C29C79Fv1C5qfPrmAESrciIxp0X40KPMbp1ZWVbd4=
```

```
-----END CERTIFICATE-----
```

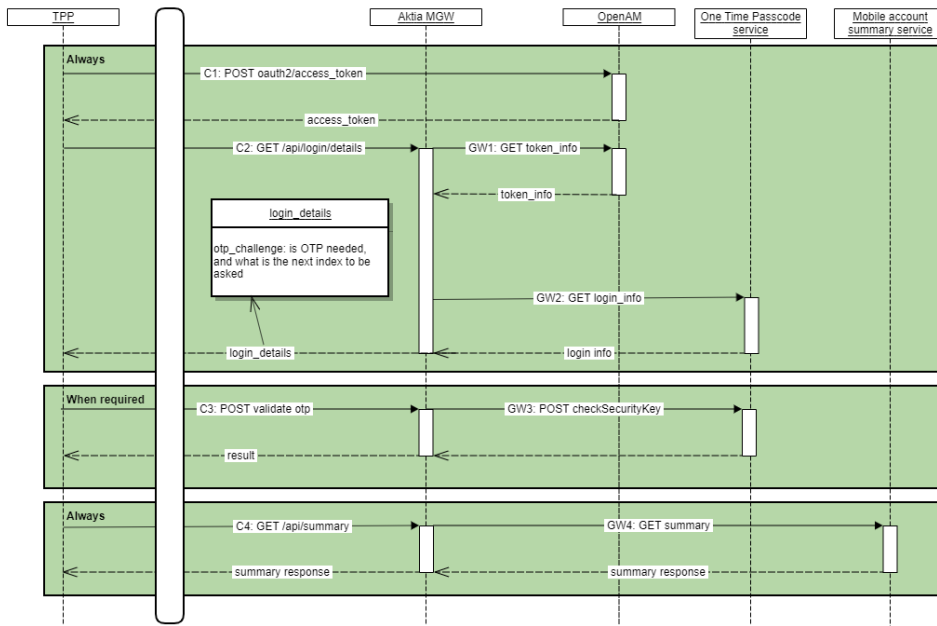
```
-----BEGIN CERTIFICATE-----  
MIIElDCCA3ygAwIBAgIQAF2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLEExB3d3cuZGlnaWNLcnQuYy29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWw9vdcBDQTAEfw0mZAZMDgxMjAwMDBaFw0zMTEwMTAwMDAwMDBaMGEXCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYXNlbnVBAStEHD3dy5kaWdpY2VydC5jb20xIDAeBgNVBAMTF0RpZ2lDZXXJ0IFNIQTIGU2VjdXJlIFNlcnZlcjBDQ0CCASiWdQYJKOZiHvcNAQEFEbQADggEPADCCAAQOCggEB ANyuWJBNwcQwFZAl1W248ghX1LFy949v/cUP6ZCWA104Yok3wZtAkC24RmDYXZK83nf36QYSvx6+M/hpzTc8z15CilodTgyu5pnVILR1WN3vaMTIal6yrBvSxquU3R0bd KpPDKC55gIDvEwRqFDulm5K+wgdlTvza/P96rtxcflUxDog5B6TXvi/TC2rSsd9f/ld0Uzs1gN2ujkSYS58009rg1/RrKatEp0tYhG2SS4HD2n0LEpdIkarFDRdNzGX kuJnVA075ME/OV4uuPNcfhCohkEAjUVmR7ChZc6gqikJTVOX6+guqw9ypzAO+sf0 /RR3w6RbKffCs/mC/bdFWJscAwEAAOCaVowggFWMBIGAlUdEwEB/wQIMAYBAF8CAQAwdgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY aHR0cDovL29jc3AuZGlnaWNLcnQuYy29tMHsGAlUdHwR0MHlWn6A1oDOGmWh0dHA6 Ly9jcmwzLmRzZ21jZXXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwWn6A1 oDOGmWh0dHA6Ly9jcmw0LmRzZ21jZXXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD QS5jcmwWpQYDVR0gBDYwNDAYBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzoI8v d3d3LmRzZ21jZXXJ0LmNvbS9DUFMwHQYDVR0OBBIIEFA+AYRyCMWHLyjnJUY4tCzh xtniMB8GAlUdIwQYMBAAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB CwUAA4IBAQJApT9L0jFcPbZ+Q1waRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqip1 5TlPHo0lbyYoiQm5vuh7ZPHLGLGTUq/sELfeNqzqPlt/yGFUzZgTHb07DjcllGA 8MXW5dRNJ2Srm8c+cfTil7gzbcKTB+6WohsYffZcTEDts8Ls/3HB40f/1LkAtDdC 2ldJ6m6K7hQGrn2iWziIqBtVlFtyRRfjs8sjX7tN8CplTm5grZD0o0rWahaPit c+LJMto4JQtV05od8Gig7S5BNO98pVAdvzr508EIDObtHopYJes4d60tbvVS3bR0 j6tJLp07kzQoH3j0lOrHvdPJbRzeXDLz
```

```
-----END CERTIFICATE-----
```

2. Production URLs

Production URLs will be provided at Onboarding by Aktia TPP Support (openbanking@aktia.fi).

3. 1. Login sequence example



3.1. C1: Login

Note: This document assumes cURL version 7.55.1 or higher.

3.1.1. Login request example

Login curl example

```
curl -X POST \
--header "Authorization: Basic VALUE WILL BE PROVIDED BY AKTIA" \
--header "Content-Type: application/x-www-form-urlencoded" \
--cacert mobile-auth.aktia.fi.ca.bundle.crt \
--cert tpp.example.fi.crt --cert-type pem \
--key tpp.example.fi.key --key-type pem \
--data "grant_type=password&username=12345678&password=REMOVED&scope=aktiaUser" \
<login-base-url>/oauth2/mobileauth/access_token
```

3.1.2. Login request items explained

Login request item	Value	Explanation
--header Authorization: Basic	minor_step_for_hacker_bigger_step_for_a_robot	Basic auth is included as a mitigation against potential brute force attacks. TPPs will be provided a valid "Authorization: Basic" header value"
--header Content-Type:	application/x-www-form-urlencoded	Represents an URL encoded form
--cacert	mobile-auth.aktia.fi.ca.bundle.crt	Tells cURL to use the specified certificate file to verify the peer. The file may contain multiple CA certificates. The certificate(s) must be in PEM format. These CA certificates are used to verify the certs of remote servers that cURL connects to.
--cert	tpp.example.fi.crt (EXAMPLE)	TPP's client certificate

--cert-type	pem	Certificate file type (DER/PEM/ENG)
--key	tpv.example.fi.key (EXAMPLE)	TPP's private key for the client certificate
--key-type	pem	Private key file type (DER/PEM/ENG)
--data	grant_type=password&username=12345678&password=REMOVED &scope=aktiaUser	Tells that username password pair will be used for authentication
	<login-base-url>/oauth2 /mobileauth/access_token	Endpoint for fetching Access Tokens

3.1.3. Login OK (HTTP 200) response example

Login curl example response

```
{ "access_token": "b674c095-764e-4646-aec3-becd8833f7e3", "scope": "aktiaUser", "token_type": "Bearer", "expires_in": 3599 }
```

Login response item	Value	Explanation
access_token	b674c095-764e-4646-aec3-becd8833f7e3	The OpenAM session token, required for subsequent API calls
scope	"aktiaUser"	Name of the scope, fixed value as specified
token_type	"Bearer"	
expires_in	3599	Max time how long the token is valid, seconds

3.1.4. Login failed (HTTP 40*) response example

```
{ "error_description": "Resource owner authentication failed", "error": "invalid_grant" }
```

This happens if user provided invalid username and password combination, OR used credentials which are not eligible, for example used account was locked.

Please note that for security purposes exact error details are NOT revealed on response. It states always simply "resource owner authentication failed". In case this occurs, instead of tried values customer should provide valid and eligible username and password pair.

3.2. C2: Login details

3.2.1. Login details request example

Get details for login and user account

```
##Get details for login and user account##
$ curl
-X GET "<api-base-url>/api/login/details"
-H "accept: application/json"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
```

3.2.2. Login details response example

Login details response

```
{ "domainSettings": {
  "pinTouchActivationAvailable": true,
  "pinTouchTermsPdfUrl": "https://www.aktia.fi/documents/10556/50573/helppo-kirjautuminen-kayttoehdot-fi.pdf",
  "ownTransferWithoutOtp": true,
  "otpChallenge": {
    "otpRequired": true,
    "otpInfo": { "nextOtpIndex": "E4",
      "currentOtpCard": "HJ11111",
      "fixedOtpCard": false,
      "nextOtpCard": null,
      "readMessagesWithoutOtp": true,
    },
  },
  "userAccountInfo": {
    "customerName": "Surname Name1 Name2 Name3",
    "passwordUpdateRequired": false,
    "accountLocked": false,
    "updateOrCreateKYCInfo": false,
    "customerType": "PERSON",
    "customerServiceInfo": {
      "serviceClass":
        "Asiakaspalvelu", "phone": "010247010", "openHours": "8 - 20",
      "personalAdvisor": { "name": null, "phone": null,
        "advisorServiceClass": "AdvisorServiceClass.PRODUCT.name" },
      "termsAcceptanceInfo": { "mustAcceptTerms": false }
    }
  }
}
```

3.2.2.1. Login details response explained

Data item	Type	details
otp challenge		One time passcode information
<ul style="list-style-type: none">otp required	boolean	if true, then C3 step is mandatory in order to proceed
<ul style="list-style-type: none">otpInfo		
<ul style="list-style-type: none"><ul style="list-style-type: none">nextOtpIndex	string	Index from where in the paper card the next otp should be asked
<ul style="list-style-type: none"><ul style="list-style-type: none">currentOtpCard	string	Paper card identifier. If SMS OTP is required, this field is used to denote the Customer's masked phone number (with 3 last digits legible).
<ul style="list-style-type: none"><ul style="list-style-type: none">fixedOtpCard	boolean	
<ul style="list-style-type: none"><ul style="list-style-type: none">nextOtpCard	string	
user account info		
<ul style="list-style-type: none">customerName	string	
<ul style="list-style-type: none">passwordUpdateRequired	boolean	if true, customer can't proceed, have to change in other channel
<ul style="list-style-type: none">accountLocked	boolean	if true, Customer's account is locked and can't use service

terms acceptance info		
<ul style="list-style-type: none"> • mustAcceptTerms 	boolean	if true, customer can't proceed, have to accept in other channel

3.3. C3: If required: Authenticate using one time passcode

3.3.1. OTP authentication request

if needed authenticate using one time passcode

```
##Authenticate using one time passcode##
$ curl
-X POST "<api-base-url>/api/login/otp/authenticate"
-H "accept: application/json"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
-H "Content-Type: application/json"
-d "{ \"otpCode\": \"858831\"}"
```

3.3.2. OTP authentication response

Response

```
{ "otpAccepted": true, "otpInfo": { "nextOtpIndex": "E9", "currentOtpCard": "H11111", "fixedOtpCard": false, "nextOtpCard": null } }
```

3.4. C4: Get summary of customer's accounts

3.4.1. Summary request

Returns summary of customer's accounts

```
##Returns summary of customer's accounts##
$ curl
-X GET "<api-base-url>/api/summary"
-H "accept: application/json"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
```

3.4.2. Summary response

Returns summary of customer's accounts

```
{ "frontPageHighlight": { "showHighlight": false, "idType": null, "id": null, "totalAmount": null },
  "accountSummary": { "accountSummaryList": [
    { "id": "8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4",
      "name": "Oma tili",
      "primaryOwnerName": "Testi Teemu Markus Erik",
      "iban": "FI7340550012203328", "bic": "HELSFIHH",
      "accountType": {
        "accountType": "Käyttötili", "categoryCode": "CURRENT_ACCOUNT", "productCode": "1410", "longTermSavings": false },
      "balance": 2.44, "balanceTotal": 2.44,

      "duePaymentsTotal": 0.00, "hideFromSummary": false, "sortingOrder": 1,
      "fabInfo": { "fabOperations": [
        { "fabOperationCode": "COPY_IBAN", "fabOperation": "Kopioi tilinumero" },
        { "fabOperationCode": "NEW_PAYMENT", "fabOperation": "Uusi maksu" },
        { "fabOperationCode": "OWN_TRANSFER", "fabOperation": "Oma tilisiirto" } ] },
      "parties": [ { "name": "Testi Teemu Markus Erik", "customerTypeCode": "PRIVATE", "roleCode": "PRIMARY_OWNER" } ] },
      "paymentsToDoItemCount": 0,
      "paymentAccounts": { "paymentAccounts": [ { "id": "8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4",
        name": "Oma tili", "iban": "FI73 4055 0012 2033 28", "balance": 2.44, "defaultPaymentAccount": true },
        "ownTransferFromAccounts": [ { "id": "8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4", "name": "Oma tili", "iban": "FI73 4055 0012 2033 28", "balance": 2.44 },
        "ownTransferToAccounts": [ { "id": "8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4", "name": "Oma tili", "iban": "FI73 4055 0012 2033 28", "balance": 2.44 } ] } ] } ] }
```

3.5. Important notice about all id:s, they are only valid within session.

For example paymentAccounts: [{"id": "8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4",

As a security mechanism, all elements, which have id:s in REST api have "pseudo id"s, which are valid only within same session.

3.6. C5: Create payment

3.6.1. Request ibaninfo

IbanInfo returns bic and some details

```
#curl -X GET "<api-base-url>/api/payments/ibanInfo?iban=FI5155610440062071"
-H "accept: application/json;charset=UTF-8"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
```

3.6.2. Response of the ibaninfo

IbanInfo returns bic and some details

```
{ "iban": "FI51 5561 0440 0620 71",
  "bic": "OKOYFIHHXXX",
  "sepaPaymentPossible": true,
  "einvoiceAgreementPossible": false,
  "einvoiceIban": null,
  "fastForwardPossible": false,
  "fastForwardIban": null }
```

3.6.3. Create payment, bic needed

IbanInfo returns bic and some details

```
{ $ curl
-X POST "<api-base-url>/api/payments"
-H "accept: application/json;charset=UTF-8"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
-H "Content-Type: application/json;charset=UTF-8"
-d "{\"amount\":\"0.10\",\"dueDate\":\"2019-09-11\",\"fastForward\":false,\"messageText\":\"Eka PSD2 fallback\",
\"newTemplate\":false,\"payer\":{\"accountId\":\"
8A04019F870973400A945908C062CA044C94689D70BEA79ED43B9A31336FA7B4\",\"accountName\":\"Oma tili \",\"bic\":\"
HELSFIHH\",\"iban\":\"FI7340550012203328\",\"payerName\":\"Testi Teemu Erik Testi\"},\"receipt\":false,\"
recipient\":{\"bic\":\"OKOYFIHHXXX\",\"iban\":\"FI5155610440062071\",\"name\":\"Testi Henriksson\"},\"
referenceNumber\":\"\",\"repetition\":{\"duration\":{\"untilFurtherNotice\":false},\"repetitionCode\":\"
ONCE\"}}}"
```

3.6.4. Create Payment response, notice "paymentId" and "lastModifiedAt"; those are required in confirmation request

Response

```
{ "result": {"successful": true,
"failReasons": []},
"paymentId": "9D7A682C7BD0F64E19448B66D5B5252AF602D142C911B9D917B7750F40AB412A",
"invoiceAgreementResult": null,
"savePaymentTemplateResult": null,
"lastModifiedAt": "2020-06-11T12:29:57" }
```

3.7. C6: Confirm payment - with passcodes codes from Aktia paper codes and SMS message content

3.7.1. Confirm payment 1. request - otpCode from Aktia paper codes

Response

```
curl
-X POST "<api-base-url>/api/payments/confirm"
-H "accept: application/json;charset=UTF-8"
-H "Authorization: Bearer b674c095-764e-4646-aec3-becd8833f7e3"
-H "Accept-Language: fi"
-H "Content-Type: application/json;charset=UTF-8"
-d "{\"otpCode\":\"147747\",\"payments\": [{\"lastModifiedAt\":\"2020-06-11T12:29:57\",\"paymentId\":\"
9D7A682C7BD0F64E19448B66D5B5252AF602D142C911B9D917B7750F40AB412A\"}]}"
```

3.7.2. Confirm payment 1. response with indication about required SMS. SMS was added 11.6.2020

If OTP was wrong, or additional SMS was required

Response

```
method="POST", uri="/api/payments/confirm", headers="[accept-language=en // possible value en,sv,fi determines language of the localized contend
{
  "otpResponse" : {
    "otpAccepted" : false,
    "otpInfo" : {
      "nextOtpIndex" : "SMS",
      "currentOtpCard" : "+358408234567", // due backward compatibility this field is used when additional SMS confirmation is required. Customer's own mobile number where the SMS was delivered. Customer have given that to Aktia through other channels. The number is masked in Production (with the last 3 numbers legible).
      "fixedOtpCard" : false,
      "nextOtpCard" : null
    }
  },
  "confirmedPaymentIds" : [ ],
  "failedPayments" : [ {
    "id" : "9D7A682C7BD0F64E19448B66D5B5252AF602D142C911B9D917B7750F40AB412A",
    "failReasonCode" : "WRONG_OTP_CODE", // due backward compatibility the enumeration was not changed, for example reasonCode "SMS_REQUIRED" would be more suitable
    "failReason" : "Additional confirmation with SMS required."
  } ],
  "einvoiceAgreementCreatedPaymentIds" : [ ],
  "failedEinvoiceAgreementsForPayments" : [ ]
}
```

3.7.3. One time passcode SMS is sent to Aktia customer's mobile number

3.7.4. Confirm payment 2. request - Passcode from SMS text message

Response

```
method="POST", uri="/api/payments/confirm", headers="[accept-language=en
{
  "otpCode": "762845",
  "payments": [
    {
      "lastModifiedAt": "2020-06-11T12:29:57",
      "paymentId": "9D7A682C7BD0F64E19448B66D5B5252AF602D142C911B9D917B7750F40AB412A"
    }
  ]
}
{
  "otpResponse" : {
    "otpAccepted" : true,
    "otpInfo" : {
      "nextOtpIndex" : "81",
      "currentOtpCard" : "HJ60A566",
      "fixedOtpCard" : false,
      "nextOtpCard" : null
    }
  },
  "confirmedPaymentIds" : [ "9D7A682C7BD0F64E19448B66D5B5252AF602D142C911B9D917B7750F40AB412A" ], // Payment is now successfully confirmed
  "failedPayments" : [ ],
  "einvoiceAgreementCreatedPaymentIds" : [ ],
  "failedEinvoiceAgreementsForPayments" : [ ]
}
```

4. Known issues and solutions

- Calls are failing.
 - Make sure User Agent is present in the headers.