Strong Customer Authentication

The main principles

V1.4

Xpollens

PAYMENT INSIDE

Introduction

Xpollens offers two kind of usage that require the use of a mobile phone by the customer:

1. **KYC process** during the user's onboarding (please refer to Know your customer | Xpollens API docs)

2. **Strong authentication process** (please refer to Strong customer authentication | Xpollens API docs)

Authentication is required for your end-customers if you are on the Retail B2C market ; it is also required for all key individuals of your professional customers, if you are on the Corporates B2B market. Strong Customer Authentication will occur in two situations :

- Online card payment
- Sensitive Operations (amongst which, some require secure display)

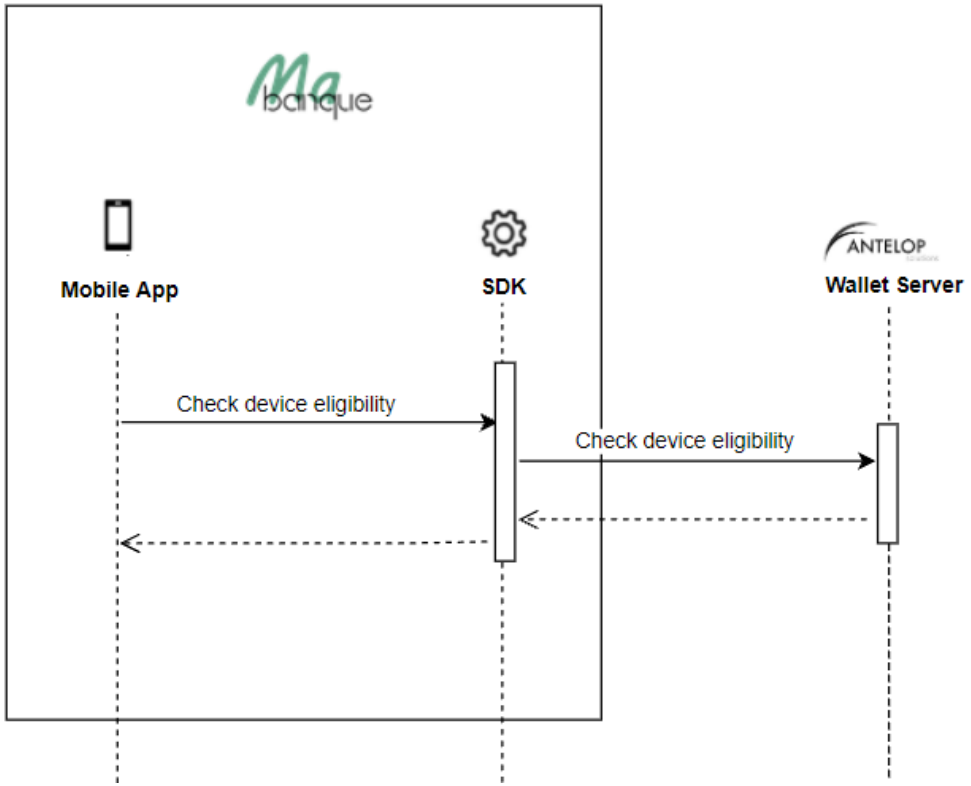
➢ This document aims at presenting the key elements to use these features.

The first step consists of integrating our SDK in your mobile application.
SDK's documentation is available at : https://doc.antelop-solutions.com/latest/wallet/sdk/index.html
Note : To access this online documentation, you shall use the ID / pwd provided by Xpollens, during your Onboarding process.

Wallet initialization

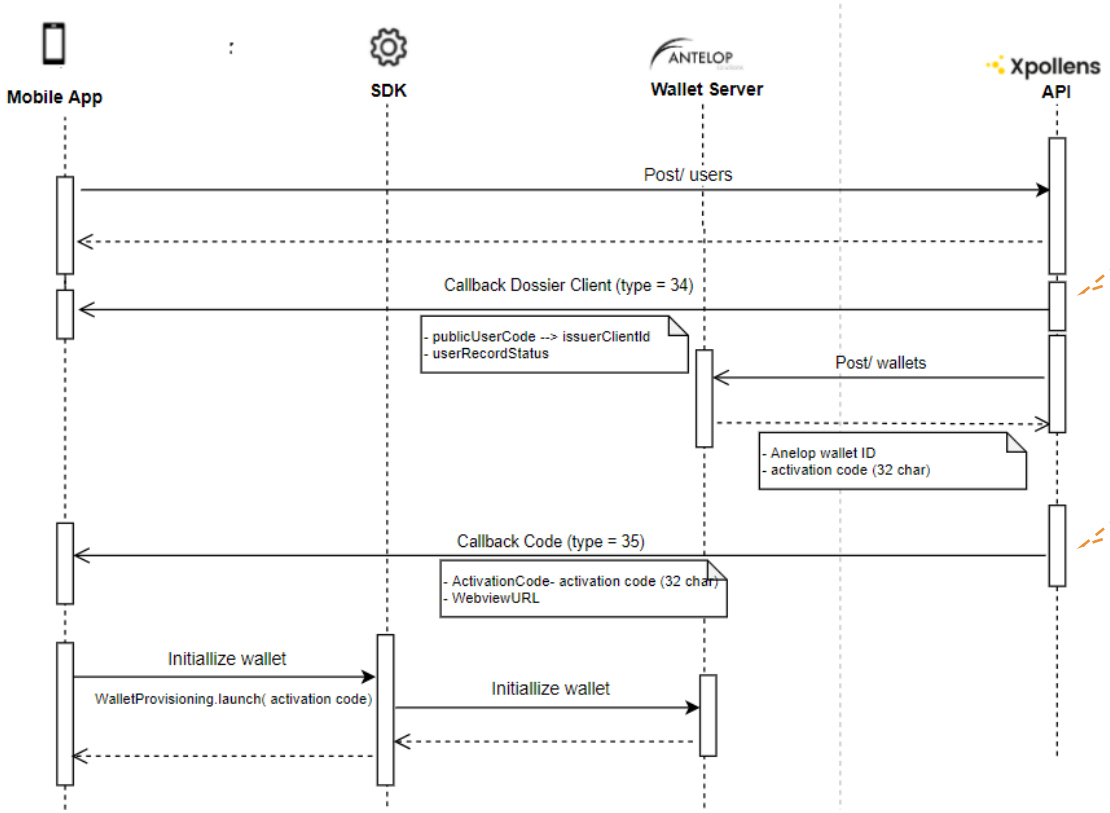
Xpollens
PAYMENT INSIDE

Check mobile eligibility



- https://doc.antelop-solutions.com/latest/wallet/general/getting-started.html
- https://doc.antelop-solutions.com/latest/wallet/sdk/wallet_management.html
- https://doc.antelop-solutions.com/latest/common/sdk-javadoc/index.html

Wallet inititialization



The “Dossier Client” callback (type =34) is described further

The “activation code“ callback (type = 35) is described further

- https://doc.antelop-solutions.com/latest/wallet/general/getting-started.html
- https://doc.antelop-solutions.com/latest/wallet/sdk/wallet_management.html

Authentication patterns

The Customer Authentication is based on Authentication Patterns, which define the possible combinations of authentication methods to authenticate for a given operation.

The authentication pattern used by Xpollens when creating the wallet is « **BIOORPIN** ».

For more details, please refer to : https://doc.antelop-solutions.com/latest/wallet/sca/sca-intro.html#_authentication_patterns

Callback « Dossier Client » : type = 34

This callbacks provides info about the user's onboarding status (called user record)

Field	Format	Required (Y/C/O)	Description
type	string	Y	Callback type = 34
appUserid	string	Y	User Reference
publicUserCode	string	Y	Corresponds to issuerClientID in our partner's (Antelop) system. It is used to create the wallet in its system.
userRecordStatus	String	Y	Status of the user record : 1 = initialized 2 = inProgress 4 = validated 5 = refused

Example :


```
{
  "type" : "34"
   "appUserid" : "toto12344"
   "publicUserCode" : "1234der14ft2"
    "userRecordStatus" : "InProgress"
}
```

Callback Code : type = 35

This callbacks provides the activation code required in the wallet enrolment process

Field	Format	Required (Y/C/O)	Description
type	string	Y	Callback Type
AppUserId	string	Y	User Reference
ActivationCode	string	C	Code use to activate wallet (32 char)
ErrorMessage	string	C	Error message if an error occurs
ExtraData	Json object	Y	Contains the webview URL

Example :


```
{
   "type": "35",
   "AppUserId":"Au007",
   "ActivationCode":"5743c6747156074e5aebcbaec6f8b4a8",
   "ErrorMessage": null
}
```

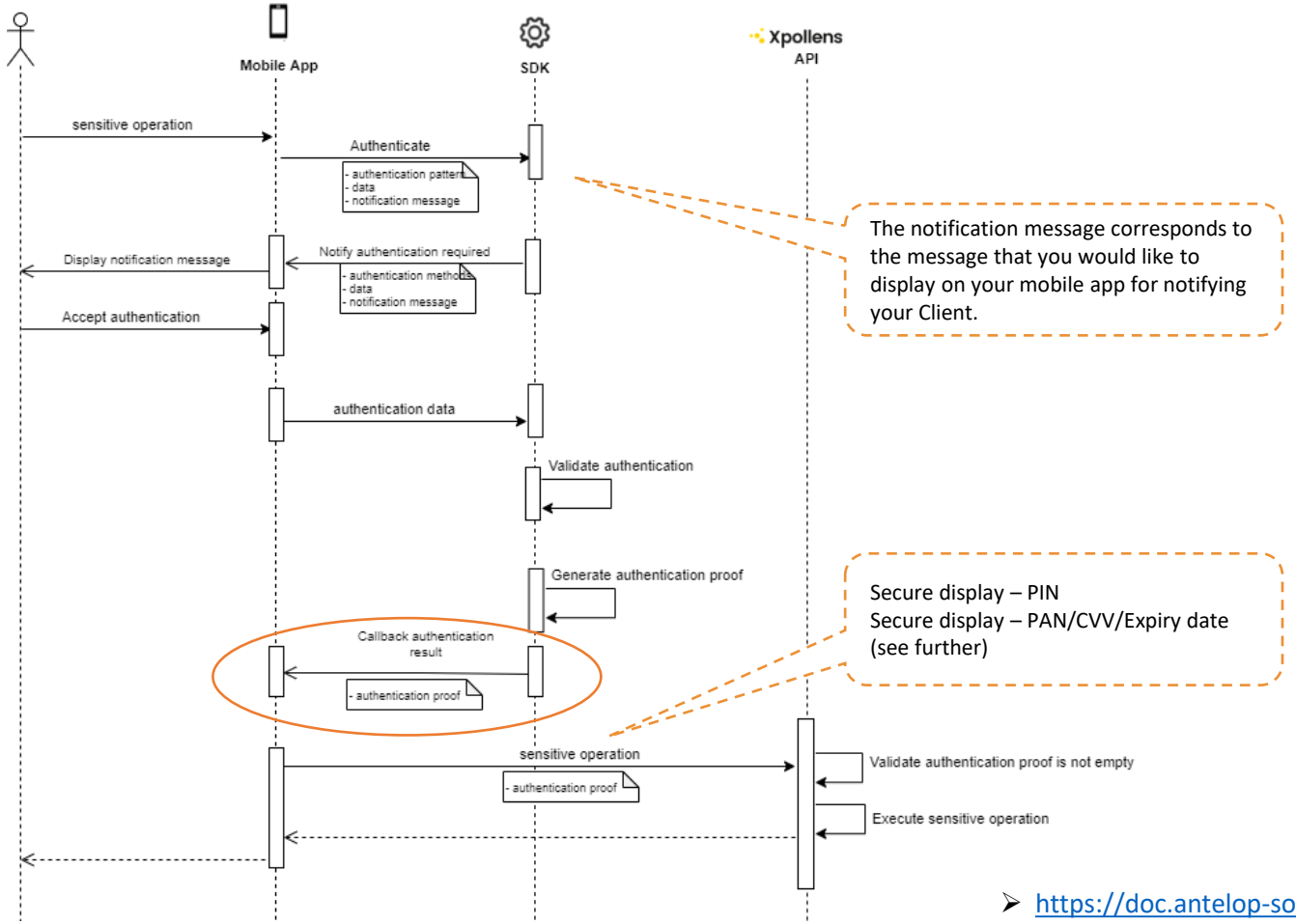
Mobile initiated authentication

Refer to https://doc.antelop-solutions.com/latest/wallet/sca/sca-intro.html#_mobile_initiated_authentication

Xpollens
PAYMENT INSIDE

Mobile initiated authentication flow chart

In this workflow, the user's strong authentication is processed through the SDK **prior to the Xpollens API call**. The authentication proof shall be then provided as an input (header) of the corresponding Xpollens APIs (Secure PIN display, Secure PAN/CVV/Expiry date Display) wich work in a **synchronous** mode.

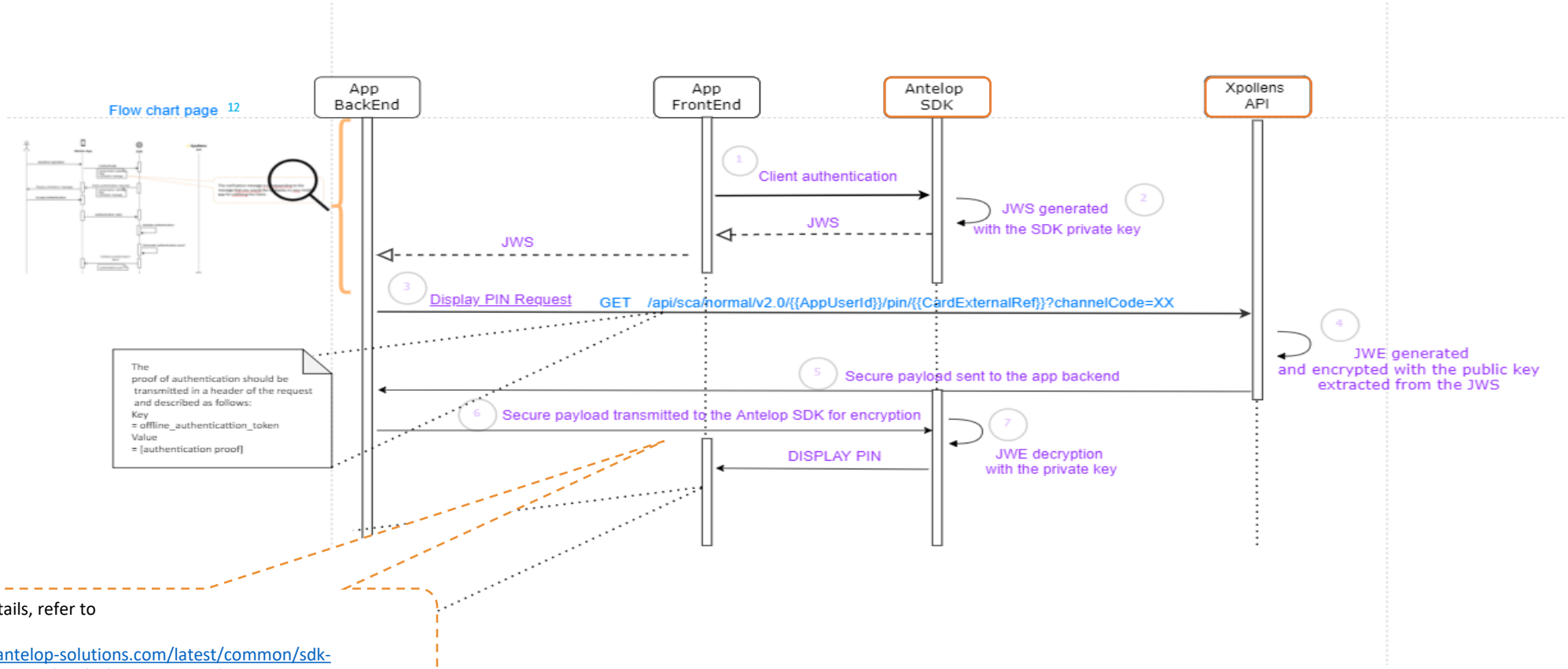


- *Note* : Xpollens APIs which require the mobile initiated authentication contain « /sca/normal » in the signature
- **The authentication proof** (= JWS token = offline_authentication_token) contains a public key used by Xpollens to encypher sensitive data (PIN, PAN&CVV)
- The SDK will then use the private key to decypher the secure payload, and display the sensitive info on the mobile app

➢ https://doc.antelop-solutions.com/latest/wallet/sca/sca-intro.html#_mobile_initiated_authentication

Secure Display – Pin Display flow chart

Display the Xpollens card PIN on the user's mobile device



For more details, refer to

https://doc.antelop-solutions.com/latest/common/sdk-javadoc/fr/antelop/sdk/ui/securedisplay/package-summary.html

Secure Display – Pin Display

- **Pre-requisites**:
  - Get the « offline_authentication_token » through the SDK
  - Card status should be 'sent' or 'Activated'

- **EndPoint** : **GET** /api/sca/normal/v2.0/{{AppUserId}}/pin/{{CardExternalRef}}/?channelCode=XX

- **Inputs:**

Field	Format	Required (Y/C/O)	Settings	Description
offline_authentication_token	string	Y	header	The proof of authentication (or JWS) should be transmitted in the header of the request and described as follows: Key = offline_authenticattion_token Value = [authentication proof]
CardExternalRef	string	Y	path	Card Reference attributed by the partner. Card status should be 'sent' or 'Activated'
AppUserId	string	Y	path	User Reference attributed by the partner
channelCode	string	Y	**path**	The channel used to display the PIN. List of possible values: 04 = by computer 66 = by phone 72 = by tablet

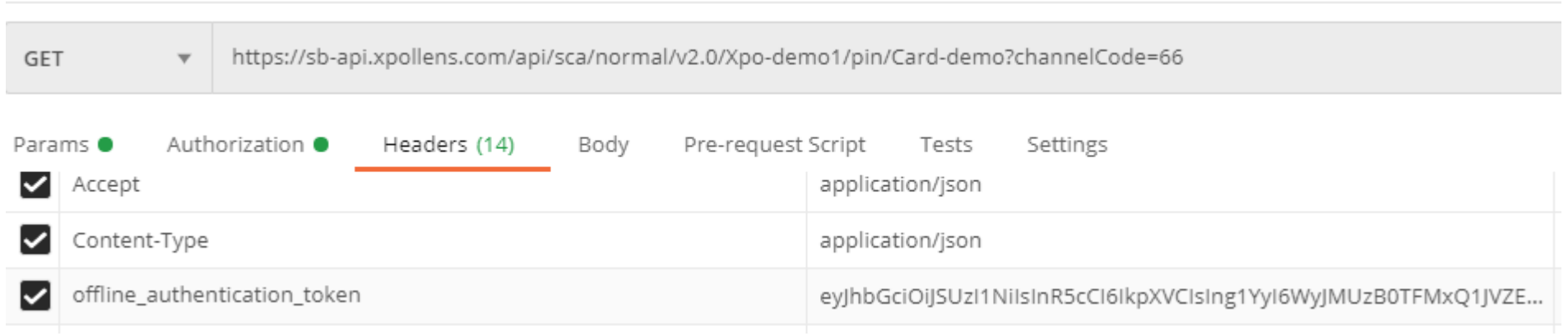
- **Output:**

Field	Format	Description
secure_payload	string	The secure payload containing the PIN, to be sent to the Antelop SDK for decryption & secure display

Secure Display – Pin Display

- **Example:**

URL: https://sb-api.xpollens.com/api/sca/normal/v2.0/Xpo-demo1/pin/Card-demo?channelCode=66

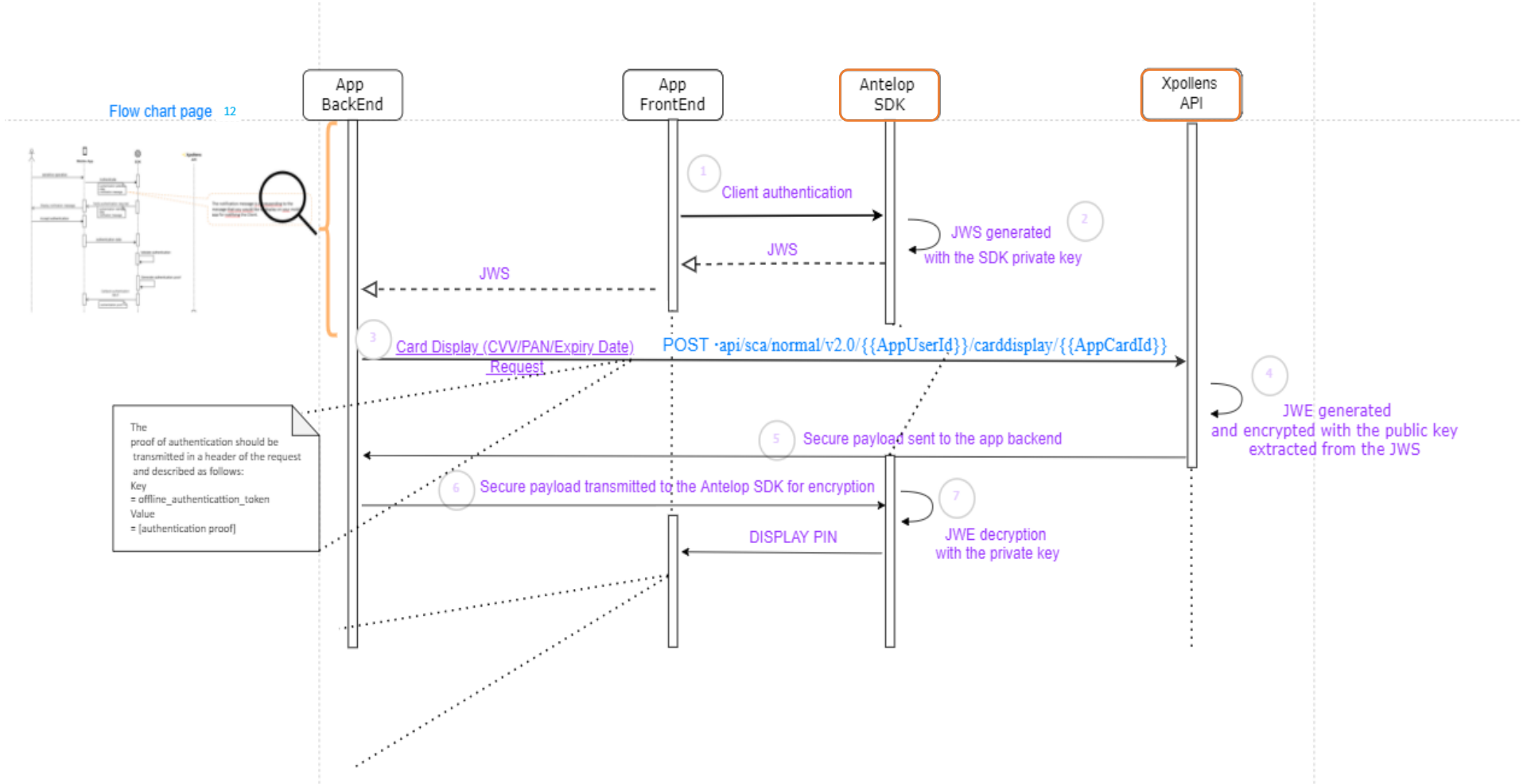


Example of Secure payload (or JWE) generated:

"{\"secure_payload\":\"eyJhbOrTOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIn0.lx1ZYYz3ummyrlusRwJRMMf6-mLCsPSAVboqjary9UYaCT_MCd312Bos7kiLLa-RCFYMpD4lDZp53iYnelrMJ6DK8-ISt7dwHX6auXDdlFPccs0N8T9MQ-t-ONWZFhR2dmP26GSpZuaAgFqNMmov8nJeF_B1CbzmTYS9DKYOofSDUAtWfB4lmjH8btVhkvCMHVcYkQSVam_yqhzA4ISp_k6zg9ej_I05Sz5cyuCIGZ069aBHUNOcoa-n88b63BZjYhLhkdZEZWsPkJ7UN075EzGR9jM8-rU3Y-zhtzjwK6pX7GFL-KNH_cFWXczQ-nAZ4ilaxgSWsPF5w3Yi7tpTdSBwyB8jJTRZg8BvW-m9-suKhGABKVbkf_hnld0ZISAwMebTxrh2wqxs9ct52vADlUCgaCd2R5N5YKgPEeTiP3WB99R0_vFigm2yKoGFmVsg2-BzBhj3BT_algbFALVmqM4PM62bFOGKgXBa18xORP4zJWqVdajSBZY2ViMHAsNz.owRHkohCu665_Yyl.jMGJ5Ff9-jwTglUo2SQUmq-2dO2mVBlYrUbq5Cyl48AgtDnvgXTlwOlMiEXWsHm4UrEs19T83VPxshWQc0Pb2vYU_v5WGCi9a-0NmJ_pmCgSySxF_LcA_mla_7YasbK81yA2cKrywsMkZrKpSC0DrLzGCPsgzmJ2Sf27_VzLHtDwMU5ic1tPdvytS_yBepurQx2TVb5W3eb4olMh6rY5tlst27p6g3rQPZP564jedD9omdhgX47rUNboDtANR-CuU6BcYdDkaqrS9nHd5aFQlJERKplp7WWvGYObSIAf-vEzp3ao5EQwApJM-0hH8ph1Db9r5mtCXNU7jh0gAobQm5AYKDoOoQYaekT4-OsxRxCqmvxgvBNUMTWaa_iEePrSastokw3D_0Lz2PnSr4IhDPeZh0ktjtsvFe1QjyFtcGVQiHOE26J7L5rc9h2pNcITX96o8FQrHEn4apZ3YdyLrmrW520eqZDjjAHLUHrFzMt6mO0MjfO8gSSRiqSz__ZoOjx2gqQh2PmcCY9zgVFx43pnjfpNLem5omThS-vL4_8OIORlsxZSAkknoK2WHDRsCFcn1KZxwK4L4_iKZ8NVoRXeiAN2i0artKK0uM9ZAOSZ9ZP95U2NK_715jYZp-bRNvRcCogOc8JwBpTSJTwarEAli3_T1PzD0WM3coDQTRPo3PE9YLj0h6MWn5f6RQzfWuLZIHAyL20q0Jd_4ABSaFlfEURLhjN9EmD0-eV3CIh_vUljU5NZ6ZK0PMlEFUYyJ_Lp2pjV1n4kZhJbn1Yst5rmUNNeyIWaSIbjWJtEEpSaLCli4zmjlJBQ85mnGLx5fEHkbJ0siAMm-85-xLGS9m7qEDsapqlDcwwRKJmWa5yJlexcl1GDgaEsyfhmGkH2NvRnT7QEXW-Uhn6iQTCNQOuq6sLr.-AM3KAeyPrbl7tN28IcDyQ\"}"

Card Display flow chart

Display the Xpollens card PAN/Expiry Date/CVV on the user's mobile device



kage-summary.html

Secure display – Card Display (CVV,PAN, Expiry date)

- **Pre-requisites** :
  - Get the « offline_authentication_token » through the SDK
  - Card status should be 'sent' or 'Activated'

- **EndPoint** : **POST** api/sca/normal/v2.0/{{AppUserId}}/carddisplay/{{CardExternalRef}}

- **Inputs**:

Field	Format	Required (Y/C/O)	Settings	Description
offline_authentication_token	string	Y	Header	The proof of authentication (or JWS) should be transmitted in the header of the request and described as follows: Key = offline_authenticattion_token Value = [authentication proof]
CardExternalRef (= AppCardId)	string	Y	path	Card Reference attributed by the partner. The card status should be 'sent' or 'Activated'
AppUserId	string	Y	path	User Reference attributed by the partner
channelCode	string	Y	**BODY**	The channel used to display the PAN/CVV/Expiry Date. List of possible values: 04 = by computer 66 = by phone 72 = by tablet

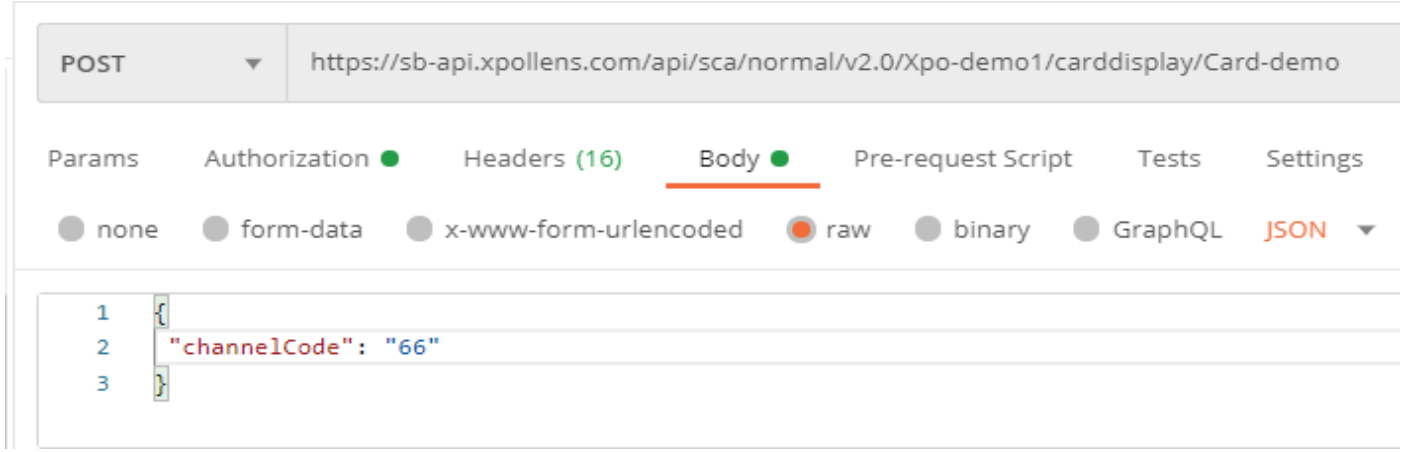
- **Output**:

Field	Format	Description
secure_payload	string	The secure payload containing the PAN/CVV/Expiry Date, to be sent to the Antelop SDK for decryption & secure display

Secure Display – Card Display (CVV,PAN, Expiry date)

- **Example:**

URL: POST https://sb-api.xpollens.com/api/sca/normal/v2.0/Xpo-demo1/carddisplay/Card-demo



Example of Secure payload (or JWE) generated:

"{\"secure_payload\":\"eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIn0.lx1ZYYz3ummyrlusRwJRMMf6-mLCsPSAVboqjary9UYaCT_MCd312Bos7kiLLa-RCFYMpD4lDZp53iYnelrMJ6DK8-lSt7dwHX6auXDdlFPccs0N8T9MQ-t-ONWZFhR2dmP26GSpZuaAgFqNMmov8nJeF_B1CbzmTYS9DKYOofSDUAtWfB4lmjH8btVhkvCMHVcYkQSVam_yqhzA4ISp_k6zg9ej_I05Sz5cyuCIGZ069aBHUNOcoa-n88b63BZjYhLhkdZEZWsPkJ7UN075EzGR9jM8-rU3Y-zhtzjwK6pX7GFL-KNH_cFWXczQ-nAZ4ilaxgSWsPF5w3Yi7tpTdSBwyB8jJTRZg8BvW-m9-suKhGABKVbkf_hnId0ZISAwMebTxrh2wqxs9ct52vADIUCgaCd2R5N5YKgPEeTiP3WB99R0_vFigm2yKoGFmVsq2-BzBhj3BT_algbFALVmqM4PM62bFOGKqXBa18xORP4zJWqVdajSBZY2ViMHAsNz.owRHkohCu665_Yyl.jMGJ5Ff9-jwTglUo2SQUmq-2dO2mVBlYrUbq5Cyl48AgtDnvgXTIwOlMiEXWsHm4UrEs19T83VPxshWQc0Pb2vYU_v5WGCi9a-0NmJ_pmCgSySxF_LcA_mIa_7YasbK81yA2cKrywsMkZrKpSC0DrLzGCPsgzmJ2Sf27_VzLHtDwMU5ic1tPdvytS_yBepurQx2TVb5W3eb4olMh6rY5tlst27p6g3rQPZP564jedD9omdhgX47rUNboDtANR-CuU6BcYdDkaqrS9nHd5aFQlJERKplp7WWvGYObSIAf-vEzp3ao5EQwApJM-0hH8ph1Db9r5mtCXNU7jh0gAobQm5AYKDoOoQYaekT4-OsxRxCqmvxgvBNUMTWaa_iEePrSastokw3D_0Lz2PnSr4IhDPeZh0ktjtsvFe1QjyFtcGVQiHOE26J7L5rc9h2pNcITX96o8FQrHEn4apZ3YdyLrmrW520eqZDjjAHLUHrFzMt6mO0MjfO8gSSRiqSz__ZoOjx2gqQh2PmcCY9zgVFx43pnjfpNLem5omThS-vL4_8OIORIsxZSAkknoK2WHDRsCFcn1KZxwK4L4_iKZ8NVoRXeiAN2i0artKK0uM9ZAOSZ9ZP95U2NK_715jYZp-bRNvRcCogOc8JwBpTSJTwarEAli3_T1PzD0WM3coDQTRPo3PE9YLj0h6MWn5f6RQzfWuLZIHAyL20g0Jd_4ABSaFIfEURLhjN9EmD0-eV3CIh_vUIjU5NZ6ZK0PMIEFUYyJ_Lp2pjV1n4kZhJbn1Yst5rmUNNeyIWaSIbjWJtEEpSaLCli4zmjIJBQ85mnGLx5fEHkbJ0siAMm-85-xLGS9m7qEDsapqlDcwwRKJmWa5yJIexcl1GDgaEsyfhmGkH2NvRnT7QEXW-Uhn6iQTCNQOuq6sLr.-AM3KAeyPrbI7tN28IcDyQ\"}"

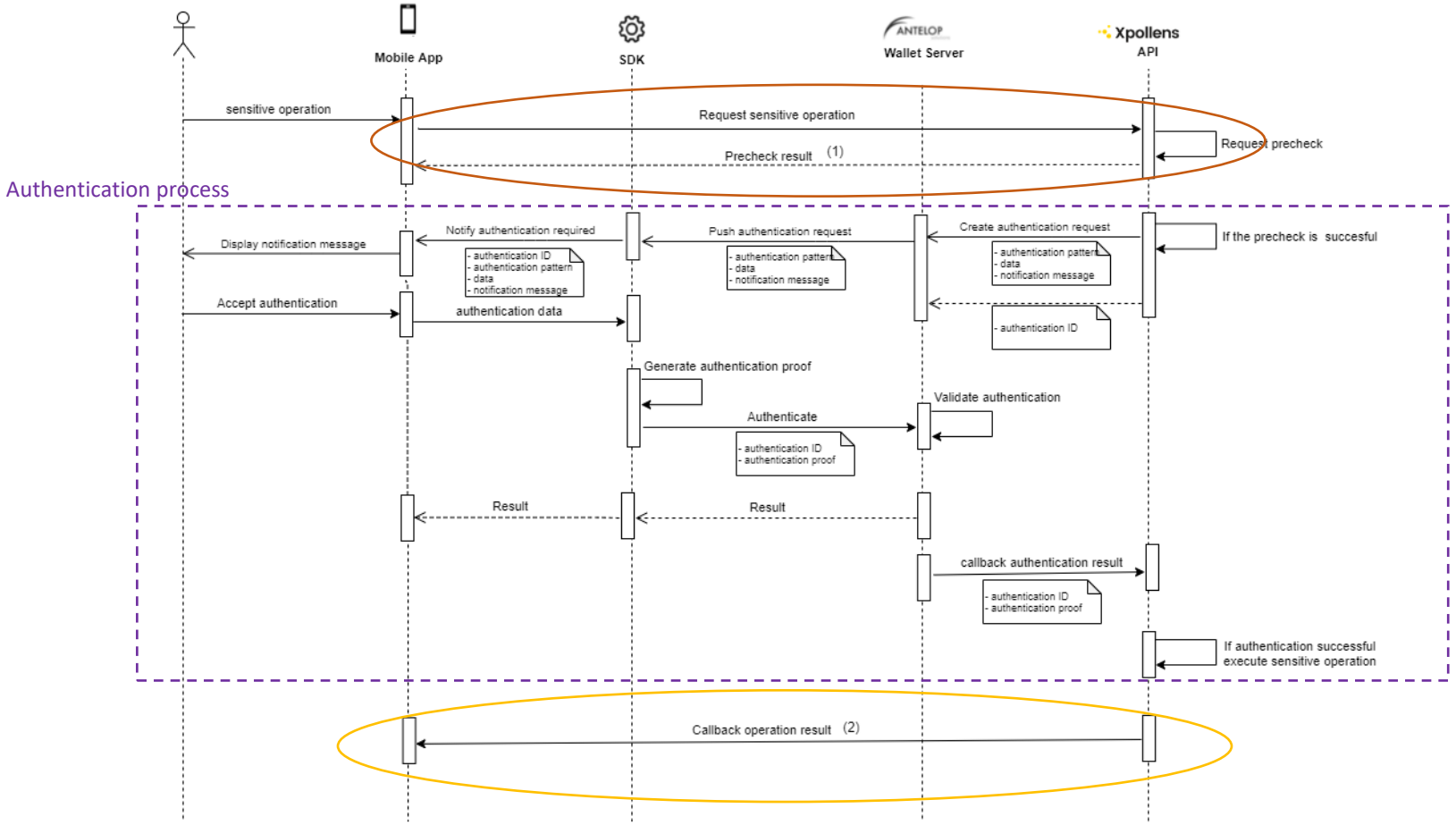
Server initiated authentication

Refer to https://doc.antelop-solutions.com/latest/wallet/sca/sca-intro.html#_server_initiated_authentication

Xpollens
PAYMENT INSIDE

Server initiated authentication flow chart

In this workflow, the user's strong authentication **is initiated via Antelop Wallet server, post Xpollens API call**.



- The user's authentication occurs during the API process, **and the sensitive operation result is provided in 2 steps :**
1. **Synchronous reponse** : « Precheck result » to inform the client pre-checks are OK, Authentication process is about to occur followed by the Xpollens sensitive operation processing
2. **Asynchronous Authentication Status + Sensitive operation return provided through the Callback type 36**

- Xpollens APIs using the server initiated authentication are described in the next page.
- In this case, you do not manage **the authentication proof :** it is not provided as an input of the sensitive operation Xpollens API.
- « callback type = 36 » is described further

Sensitive operations

Xpollens
PAYMENT INSIDE

List of Xpollens « sensitive operations » APIs requiring the Server initiated Auhtentication workflow :

	Sensitive operations	Xpollens Endpoints	Documentation
User's onboarding	• Modify a User • Send User's accepted gcu	• PUT /api/sca/v1.1/users/{userid}/ • POST /api/sca/v2.0/users/{AppUserId}/cgu	See webdoc : https://docs.xpollens.com/ Please note that the corresponding EndPoints currently described in the webdoc do not include "/sca/" into the signature, **but should use the signature with /sca/ in order to be functional for our Agent Clients**. Keep also in mind the fact that the sensitive operation return will be provided through the callback type = 36 (instead of synchronous return).
Transfer	• Create a bankaccount • Modify bankaccount • Create sct • Create sct recurrent • Create sct planned	• POST /api/sca/v1.1/users/Appuserid/bankaccounts • PUT /api/sca/v1.1/users/Appuserid/bankaccounts • POST /api/sca/v1.1/users/{appuserid}/sct • POST /api/sca/v1.1/users/appuserid/sct • POST /api/sca/v1.1/users/appuserid/sct	
Card management	• Create card • Refabricate card	• Post /api/sca/v2.0/card/{{holder}} • Post /api/sca/v2.0/card/refabricate/{{holder}}	
Transaction management	• Get transaction history	• GET /api/sca/v1.1/users/{appUserId}/historyitems	
Compliance	• Provide FATCA/EAI info	• PATCH /api/sca/v2.0/user/{appUserId}/fatcaEai	

Synchronous operation Response

Synchronous response corresponding to the « Pre-checks » related to the sensitive operation Xpollens API.

- If OK, Authentication process is about to occur followed by the Xpollens sensitive operation processing (flow chart → (1)).
- If KO, http response code is the one of the sensitive operation called with pre-checks KO & the Reason of the failure is provided into the “Reason” field

Field		Format	Description
Header	AuthenticationId	long	Id of the Authentication Operation
	AppUserId	string	User Reference
	RequestDate	DateTime	Effective end date for the operation
	Status	enum	Authentication Status List of possible values: • Pending (if pre-checks OK) • Failed (if pre-checks KO)
	Reason	string	**http Code** of the sensitive Operation if pre-checks KO (see the corresponding API documentation)
Payload		Binary	• **null** if pre-checks OK • Payload response of the sensitive operation if pre-checks KO (see the corresponding API documentation)

Example :


```
{
"Header":
  {
    "AuthenticationId": 1234,
    "AppUserId":"Au007",
    "RequestDate":"2021-02-19T16:18:41.4570774+00:00"
    "Status":"Pending",
    "Reason": null,
  },
  "Payload": null
}
```

Callback type = 36 : return of the sensitive operation

Xpollens PAYMENT INSIDE

Asynchronous Authentication Status + Sensitive operation return provided through the Callback type 36 (flow chart → (2))

Field		Format	Required (Y/C)	Description
Header	AuthenticationId	long	Y	Id of the Authentication Operation
	Type	string	Y	Callback Type
	AppUserId	string	Y	User Reference
	AuthenticationResultDate	DateTime	Y	Effective authentication result date
	RequestProcessedDate	DateTime	C	Effective end date for the operation
	RequestResponseCode	int	Y	Http status code of the operation
	Status	enum	Y	AuthenticationStatus List of possible values: • Pending • Failed
	Reason	string	C	TIMEOUT: customer did not authenticate in due time CANCELED: customer canceled the authentication request, FAILED: customer did not successfully authenticate
Payload		Binary	Y	Result of the operation

Example of a Callback type=36 for a call to EndPoint
« POST /api/sca/v2.0/users/{AppUserId}/cgu»


```
"Header": {
        "AuthenticationId": "549ee806-fbb4-4ad9-a20e-d2fb279bc610",
        "Type": 36,
        "AppUserId": "RgdmCHYJ2",
        "AuthenticationResultDate": "2022-02-04T07:50:27+00:00",
        "RequestProcessDate": "2022-02-04T07:50:27.6650131+00:00",
        "RequestResponseCode": 200,
        "RequestDate": "2022-02-04T07:48:51.899405+00:00",
        "Status": "Succeeded",
        "Reason": null
    },
    "Payload": "{\"card\":true,\"partner\":true,\"account\":true}"
```

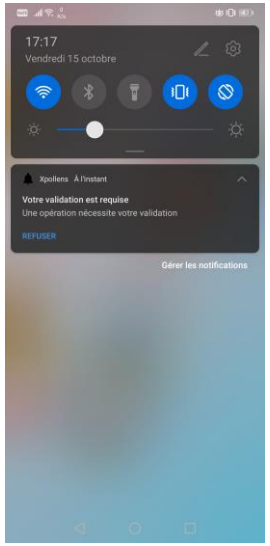
Authentication process : Notification message for sensitive operations

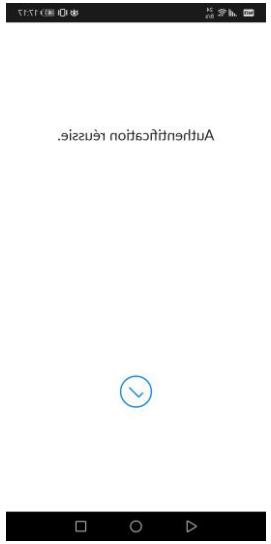
This corresponds to the notification sent by the SDK to the mobile App in order to ask for a strong authentication for a sensitive operation

The notification must be implemented in RAW_LIST format.
Note : The message displayed to the user depending the operation type cannot be modified and is in **French** (cf. next page)

```
{
 "notificationMessage": "Une opération sensible requiert votre validation",
 "message": "Opération sensible à confirmer",
 "format":"RAW_LIST",
 "data":[
    {"title" : "Opération", "value":"Acceptation des CGU"},
    {"title": "Compte", "value" : %Nom_partenaire}
 ]
}
```

list of sensitive operations, as well as the notification messages to display on the mobile are descrived in next page





Please refer to webdoc :
https://docs.xpollens.com/docs/kyc/identification

Authentication process : notification msg / sensitive operations

Sensitive operation	Operation	Operation details
Ajout/Modif de bénéficiaire	Ajout d'un Bénéficiaire	Nom: %Nom_Bénéficiaire IBAN: %IBAN_Masqué_Bénéficiaire
Ajout/Modif de bénéficiaire	Modification d'un Bénéficiaire	Nom: %Nom_Bénéficiaire IBAN: %IBAN_Masqué_Bénéficiaire)
Accéder aux informations de compte	Consultations des opérations	Compte: %Nom_Partenaire
Virement	Virement immédiat	Montant: %Montant %Devise Bénéficiaire: %Nom_Bénéficiaire
Virement	Virement planifié	Montant: %Montant %Devise Bénéficiaire: %Nom_Bénéficiaire Date planifiée: %Date_Future
Virement	Virement récurrent	Montant: %Montant %Devise Bénéficiaire: %Nom_Bénéficiaire Récurrence: Tous les %Quantile du mois
Commande d'une carte	Commande d'une Carte	Type: Carte VISA %Type \n %Nom_Partenaire
Modif. d'une donnée perso	Modification Donnée Personnelle	Rue: %adresse
Acceptation des CGUc	Acceptation des CGU	Compte: %Nom_Partenaire
Déclaration Fatca / eai	Déclaratifs Fiscaux	Compte: %Nom_Partenaire
Affichage PIN	Affichage Code PIN	Carte: %Nom_Partenaire
Choix Wish PIN	Choix d'un nouveau Code PIN	Carte: %Nom_Partenaire
Affichage PAN & CVV2	Affichage de votre Carte	Carte: %Nom_Partenaire

Please refer to webdoc : https://docs.xpollens.com/docs/kyc/identification

Notification message for online payment

The notification must be implemented in PURCHASE format.


```
{
 "notificationMessage": "Une opération sensible requiert votre validation",
 "message": "Paiement en ligne à confirmer",
 "format":"PURCHASE",
 "amount":"74,12 €",
 "merchant":"WWW.OUI.SNCF"
}
```


Please refer to webdoc : https://docs.xpollens.com/docs/kyc/identification