Strong Customer Authentication

The main principles

Xpollens

PAYMENT INSIDE

Introduction

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

- KYC process during the user's onboarding (please refer to Know your customer | Xpollens API docs)
- Strong authentication process (please refer to Strong customer authentication | Xpollens API docs)

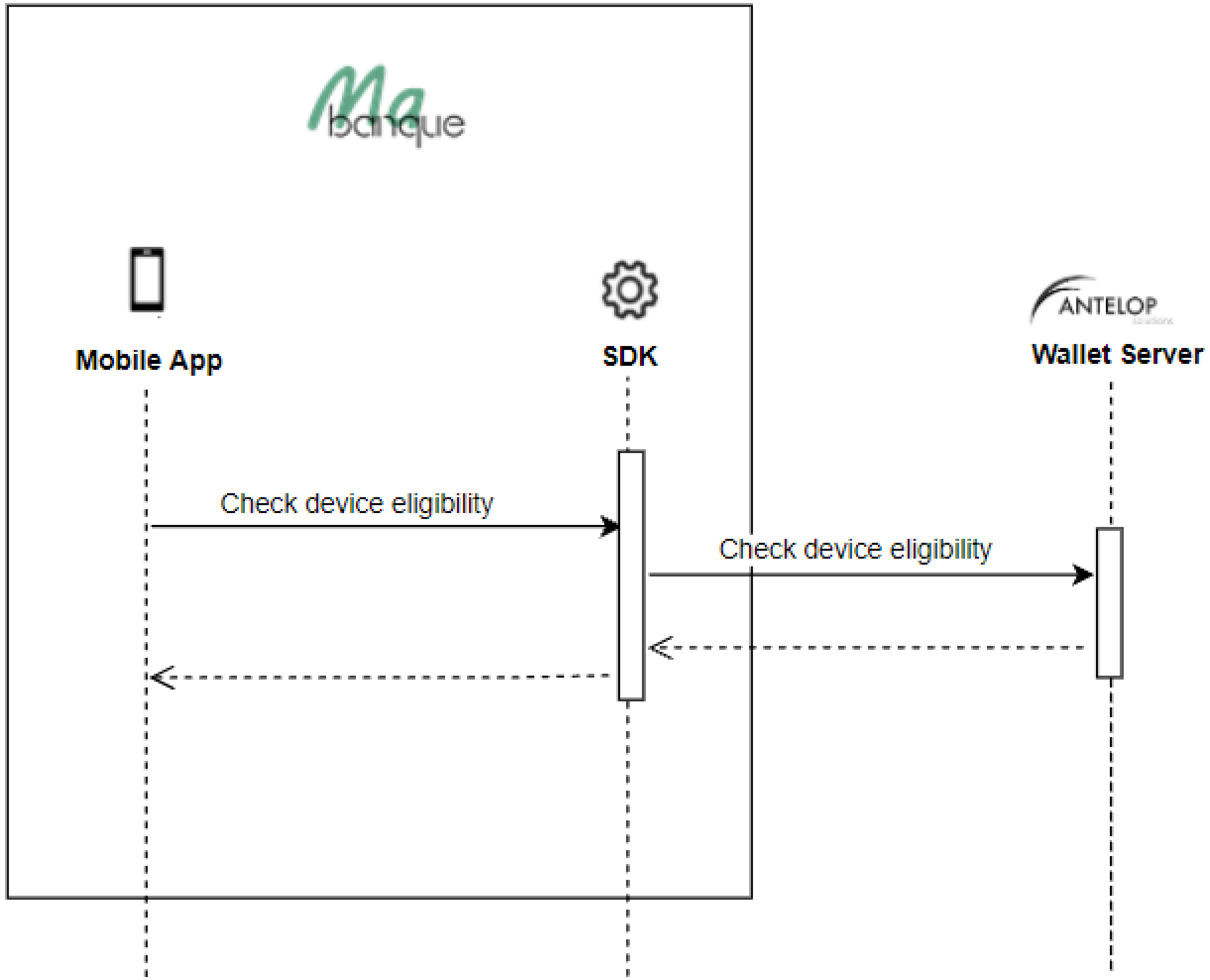
Strong authentication is required for your customers when they perform the following transactions:

- Online card payment
- Sensitive operations
- Secure display

The following slides show the key elements that will allow you to use these features.
However, the first step consists of integrating the provider's SDK in your mobile application. Provider's documentation is available on this link and gives you more details.
https://doc.antelop-solutions.com/latest/wallet/sdk/index.html

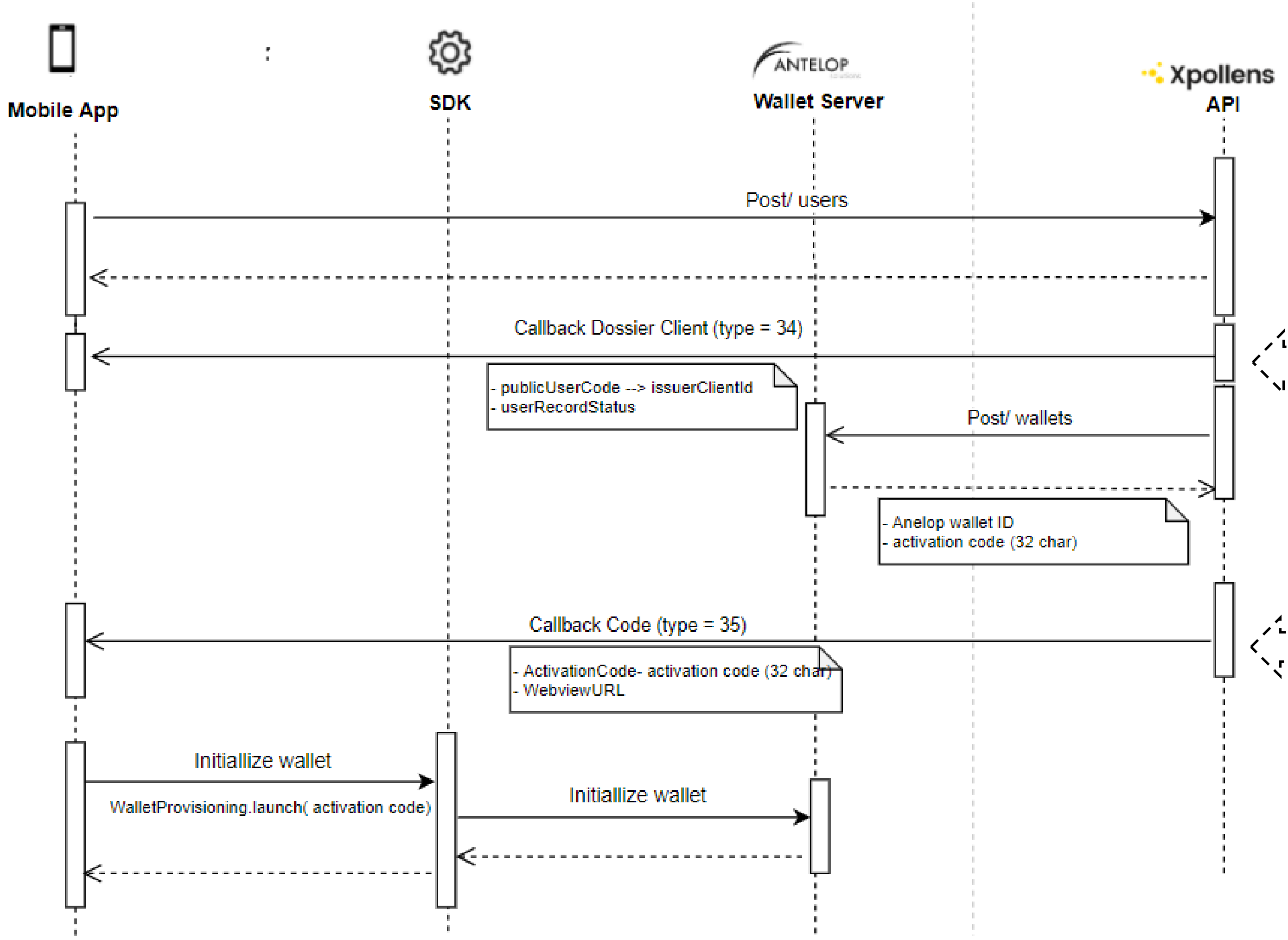
Wallet inititialization

Check mobile eligibility(refer to : https://doc.antelop-solutions.com/latest/wallet/general/getting-started.html , https://doc.antelop-solutions.com/latest/wallet/sdk/wallet_management.html)



Wallet inititialization

Initialize the wallet(refer to : https://doc.antelop-solutions.com/latest/wallet/general/getting-started.html , https://doc.antelop-solutions.com/latest/wallet/sdk/wallet_management.html)



Mobile App
:
SDK
ANTELOP
Wallet Server
Xpollens
API
Post/ users
Callback Dossier Client (type = 34)
- publicUserCode --> issuerClientId
- userRecordStatus
Post/ wallets
- Anelop wallet ID
- activation code (32 char)
Callback Code (type = 35)
- ActivationCode- activation code (32 char)
- WebviewURL
Initiallize wallet
WalletProvisioning.launch(activation code)
Initiallize wallet

The calback Dossier Client is described in the following slide

The calback Code is described in the following slide

Authentication patterns

The Customer Authentication are 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

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

Field	Format	Required (Y/C/O)	Description
type	string	Y	Callback type = 34
appUserid	string	Y	User Reference
publicUserCode	string	Y	Corresponds to issuerClientID at Antelop. It is used to authenticate the User.
userRecordStatus	String	Y	Corresponds to the onboarding status

Callback Code : type = 35

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

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

KYC process

Xpollens
PAYMENT INSIDE

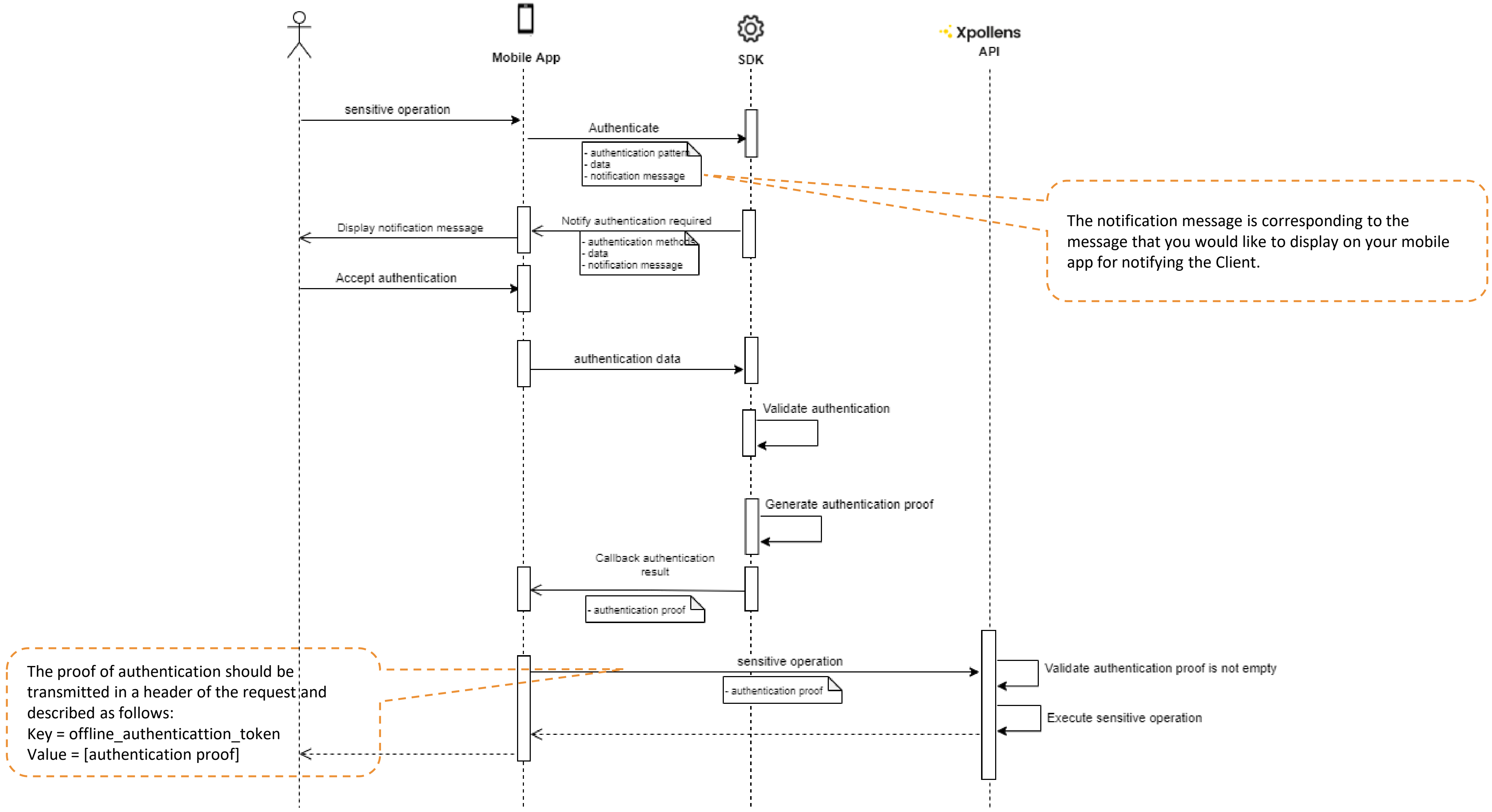
Webview URL

When creating the wallet, Xpollens gives the webview URL in the "issuerData" field. This information is sent to the SDK and available to the application by using the *getIssuerData()* method.

Mobile initiated authentication

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

Flow chart



The notification message is corresponding to the message that you would like to display on your mobile app for notifying the Client.

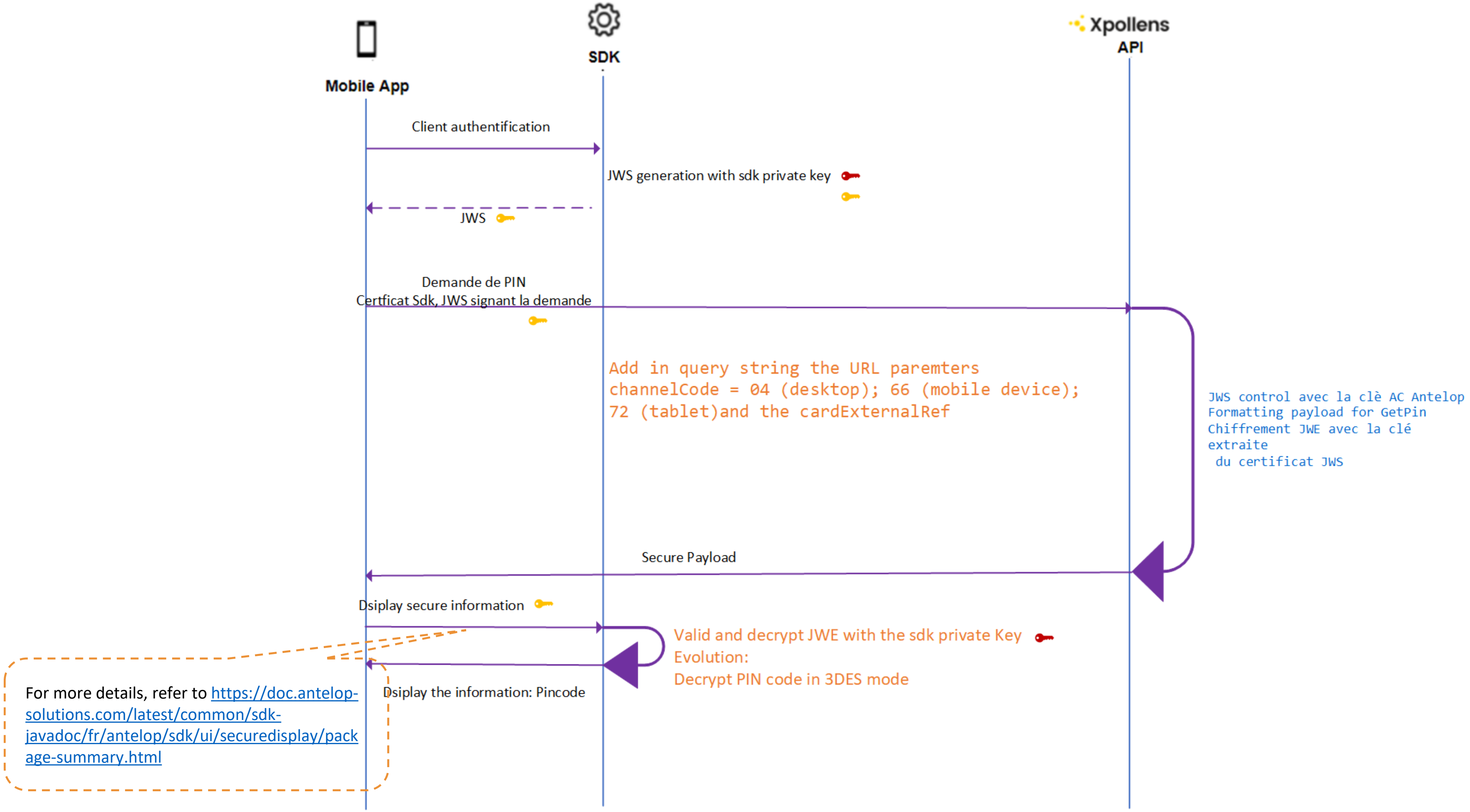
The proof of authentication should be transmitted in a header of the request and described as follows:
Key = offline_authenticattion_token
Value = [authentication proof]

Sensitive operations

	Sensitive operations	Endpoints	Documentation
Card management	- Get Pin - Get Display Card		Swagger (release spr 43) Channel code. List of values: 04 = by computer 66 = by phone 72 = by tablet

These operations are initiated by the mobile application and they use the secure interface module to display information.
For more details, refer to https://doc.antelop-solutions.com/latest/wallet/secureInterface/introduction.html

GET/ pin flow chart


Mobile App
SDK
Xpollens
API
Client authentification
JWS generation with sdk private key
JWS
Demande de PIN
Certficat Sdk, JWS signant la demande
Secure Payload
Dsiplay secure information
Dsiplay the information: Pincode

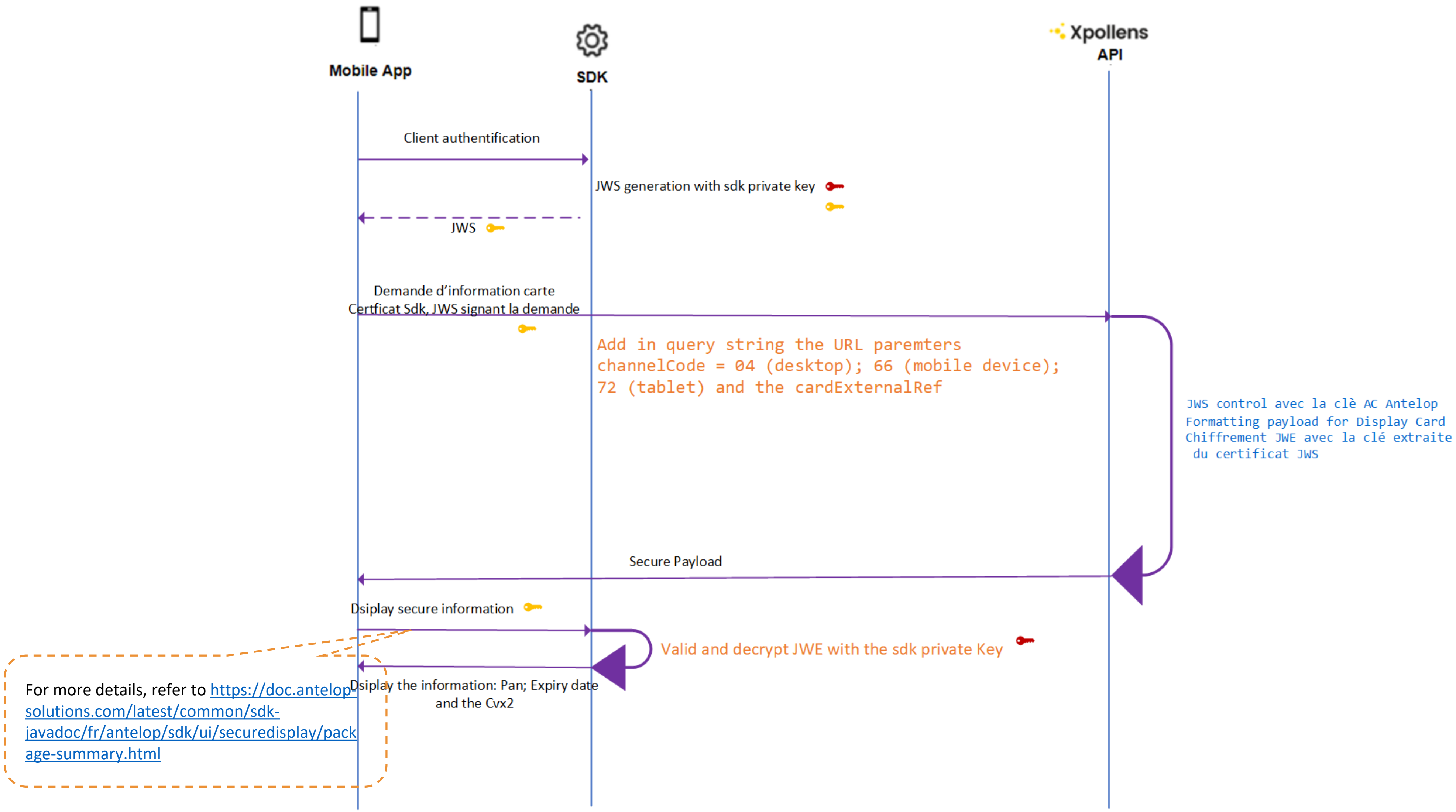
Add in query string the URL paremters channelCode = 04 (desktop); 66 (mobile device); 72 (tablet)and the cardExternalRef

```
JWS control avec la clè AC Antelop
Formatting payload for GetPin
Chiffrement JWE avec la clé
extraite
 du certificat JWS
```

Valid and decrypt JWE with the sdk private Key
Evolution:
Decrypt PIN code in 3DES mode

For more details, refer to https://doc.antelop-solutions.com/latest/common/sdk-javadoc/fr/antelop/sdk/ui/securedisplay/package-summary.html

GET/ card display flow chart



Mobile App

SDK

Xpollens API

Client authentification

JWS generation with sdk private key

JWS

Demande d'information carte
Certficat Sdk, JWS signant la demande

```
Add in query string the URL paremters
channelCode = 04 (desktop); 66 (mobile device);
72 (tablet) and the cardExternalRef
```

```
JWS control avec la clè AC Antelop
Formatting payload for Display Card
Chiffrement JWE avec la clé extraite
 du certificat JWS
```

Secure Payload

Dsiplay secure information

Valid and decrypt JWE with the sdk private Key

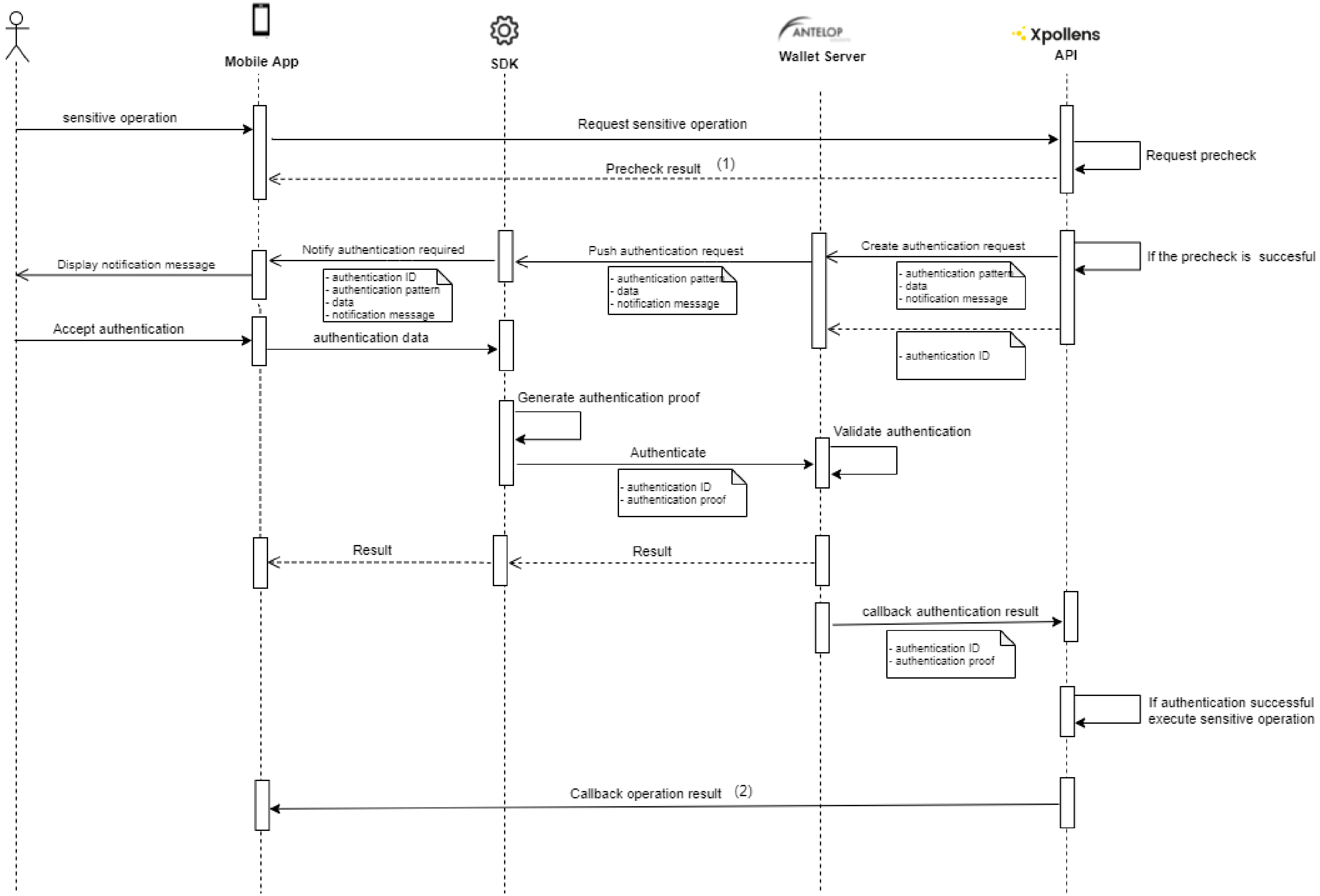
Dsiplay the information: Pan; Expiry date
and the Cvx2

For more details, refer to https://doc.antelop-solutions.com/latest/common/sdk-javadoc/fr/antelop/sdk/ui/securedisplay/package-summary.html

Server initiated authentication

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

Flow chart



Mobile App

SDK

ANTELOP

Wallet Server

Xpollens

API

sensitive operation

Request sensitive operation

Request precheck

Precheck result (1)

Create authentication request

- authentication pattern
- data
- notification message

If the precheck is succesful

- authentication ID

Push authentication request

- authentication pattern
- data
- notification message

Notify authentication required

- authentication ID
- authentication pattern
- data
- notification message

Display notification message

Accept authentication

authentication data

Generate authentication proof

Authenticate

- authentication ID
- authentication proof

Validate authentication

Result

Result

callback authentication result

- authentication ID
- authentication proof

If authentication successful execute sensitive operation

Callback operation result (2)

Sensitive operations

The authentication of the following operations are initiated by Xpollens server.

	Sensitive operations	Endpoints	Documentation
User	- Modify a User - Send User's accepted gcu	- PUT /api/sca/v1.1/users/{userid}/ - POST /api/sca/v1.1/users/{AppUserId}/cgu - POST /api/sca/v2.0/users/{AppUserId}/cgu	S-money-API-Users-BiB-v2.7
Transfert	- 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	S-money-API-SCT-BiB-v2.3
Card management	- Create card - Refabricate card	- Post /api/sca/v2.0/card/{{holder}} - Post /api/sca/v2.0/card/refabricate/{{holder}}	S-money-API-Cards-BiB-v1.33-en
Transaction management	Get history items	GET /api/sca/v1.1/users/{appUserId}/historyitems	S-money-API-OperationsHistory-BiB-v1.4
Compliance	Fatca/eai	PATCH /api/sca/v2.0/user/{appUserId}/fatcaEai	S-money-API-FatcaEai Xpollens-v1.0

Synchronous operation response

In the strong customer authentication worflow, the authentication response is immediatly return to the partner as the http response of the request (flow chart → (1)) .

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

Field	Format	Required	Description
Header	Header	Y	Authentication details
Payload	Binary	Y	Reason for operation request failed

Header

Field	Format	Required (Y/C/O)	Description
AuthenticationId	long	Y	Id of the Authentication Operation
AppUserId	string	Y	User Reference
RequestDate	DateTime	C	Effective end date for the operation
Status	enum AuthenticationStatus	Y	Status of the authentication
Reason	string	C	Reason for operation request failed

enum AuthenticationStatus

Values	Description
Pending	
Failed	

Xpollens
PAYMENT INSIDE

Callback operation result

In the strong customer authentication worflow, the authentication callback is used to notify partner of the result of the operation and authentication status.(flow chart → (2)) .

```
{
"Header": {
 "AuthenticationId": "1240b556-604e-4b5d-9bc1-73b649fc992e",
 "Type": 36,
 "AppUserId": "49807005J",
 "AuthenticationResultDate": "2021-05-18T12:47:25+00:00",
 "RequestProcessedDate": "2021-05-18T12:47:14.4008694+00:00",
 "RequestResponseCode": 201,
 "Status": "Succeeded",
 "Reason": null
},
"Payload": ""
}
```

Field	Format	Required	Description
Header	Header	Y	Authentication details
Payload	Binary	Y	Result of the operation

Header

Field	Format	Required (Y/C/O)	Description
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 AuthenticationStatus	Y	Status of the authentication
Reason	string	C	TIMEOUT: customer did not authenticate in due time CANCELED: customer canceled the authentication request, FAILED: customer did not successfully authenticate

enum AuthenticationStatus

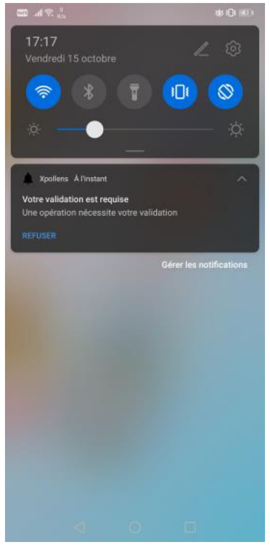
Values	Description
Succeeded	
Failed	

Notification message for sensitive operations

The notification must be implemented in RAW_LIST format.

```
{
 "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}
 ]
}
```

You will find in the following slide, the list of sensitive operations, as well as the notification messages to display on the mobile



17:17
Vendredi 15 octobre

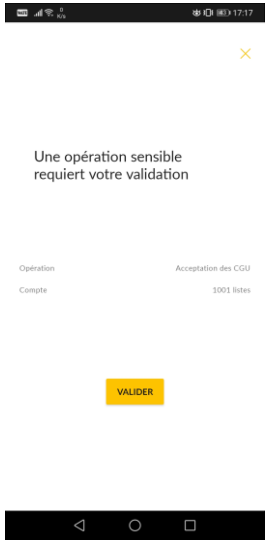
Xpollens À l'instant

Votre validation est requise

Une opération nécessite votre validation

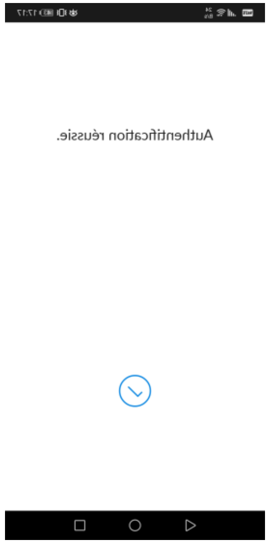
REFUSER

Gérer les notifications



Une opération sensible
requiert votre validation

Opération	Acceptation des CGU
Compte	1001 listes



Authentification réussie.

Notification message for 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

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"
}
```