Orange draft-user-questioning

OIF MODRNA

Nicolas Aillery

Charles Marais

Workshop in Paris

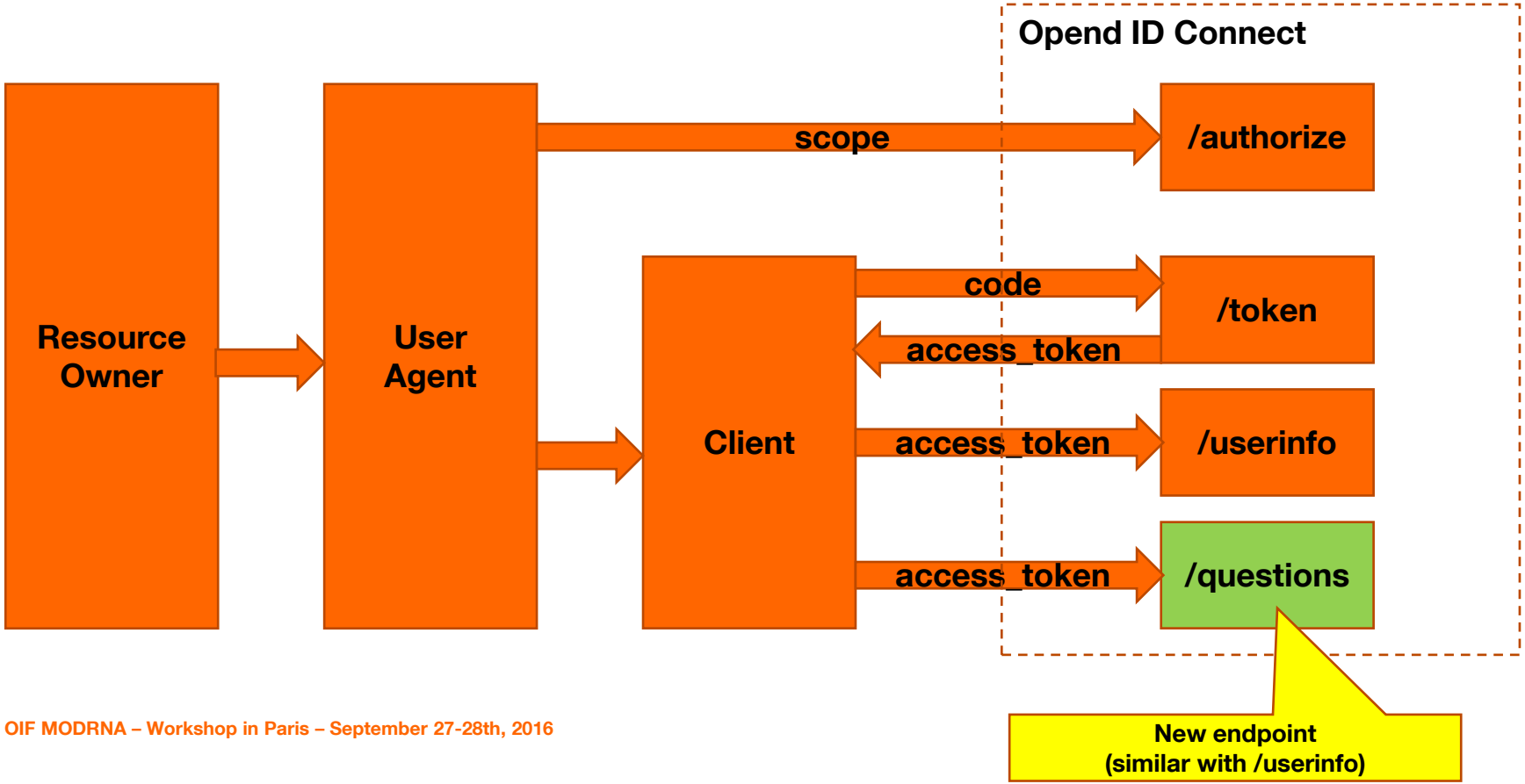
September 27-28th, 2016

orange™

In Brief

- The User Questioning API is requested with a question, interacts with the User to get his statement (out of scope) and responds with a signed user statement
  - It's a server-to-server API
  - It's protected by an Oauth Access Token (i.e. Client is authenticated)
  - The questioned User is identified either by a user_id (e.g. MSISDN) or by the Access Token (e.g. autorisation code grant, JWT assertion, ROPC grant, …)
  - The User Statement is delivered in a « User Statement Token »
  - The User Statement Token is a signed JWT

User Questioning in Open ID Connect



Use Cases

Use Cases (1/2)

1. **Confirm password change**

   Do you allow your password to be modified on Site.org?
   (Accept) (Deny)

2. **Carrier billing transaction approval**

   Do you allow Orange pay 10 euros to Merchant.org, on your bill?
   (Accept) (Deny)

3. **Customer interactions**

   We have no more Diet Cola. Do you allow to get Cola Zero instead?
   (Accept) (Deny)

   Your flight is cancelled. Do you accept to be moved to the next flight ?
   (Accept) (Deny)

4. **Bot prevention for online sales**

   A bot is buying a concert ticket on your name. Do you allow this purchase?
   (Accept) (Deny)

5. **Parental control of purchase of access to content**

   Do you allow Junior to rent 'Saw V'?
   (Accept) (Deny)

Use Cases (2/2)

Authorisation of risky card transaction (3-D Secure)

6

```
Do you allow your Bank to pay 10 euros to Merchant.org, on your card 4975xxxx1234?
(Accept) (Deny)
```

```
Do you allow your Bank to pay 10 euros to Merchant.org, on your card 4975xxxx1234?
Enter "158497" on Merchant.org to allow it.
```

Corporate expenses approval by manager

7

```
Do you allow the following corporate expenses "Champagne to OIF workshop attendees" for Ph. Clément?
(Accept) (Deny)
```

Health record transfer approval between medical entities

8

```
Do you allow Dr. House to send your medical details to Dr. Lecter ?
(Accept) (Deny)
```

Add new payee to online banking

9

```
Do you allow Mr Blue to be added to your payees on Bank.com?
(Accept) (Deny)
```

Collection of delivered items

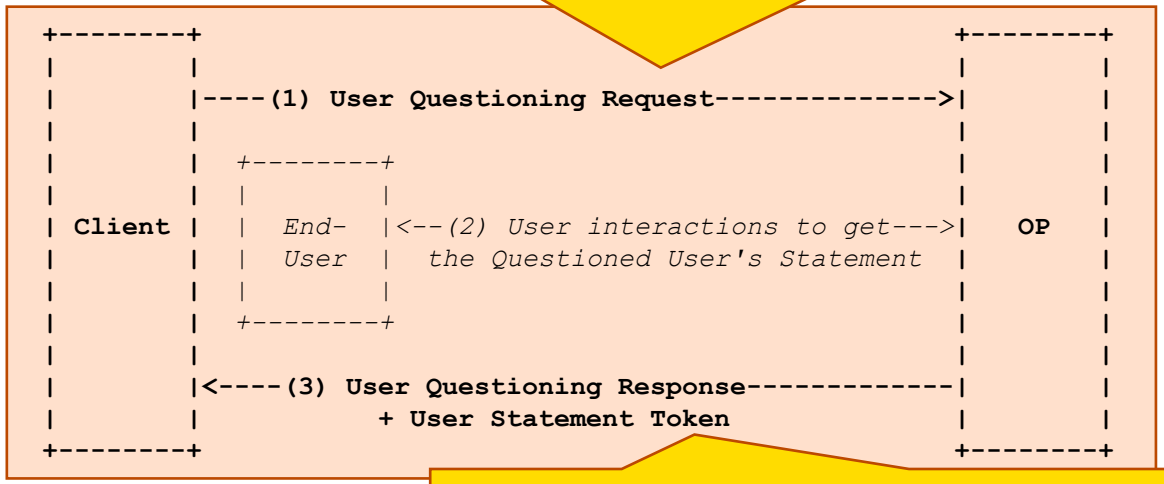
10

```
Do you allow Mr Red to get your parcel at the Post Office ?
(Accept) (Deny)
```

Technical overview

Overview

```
GET /questions?
user_id=33612345678
&user_id_type=MSISDN
&question_to_display=An%20example%20message%20to%20display
&wished_qcr=2
Host: server.example.com
Accept: application/json
Authorization: Bearer SlAV32hkKG
```

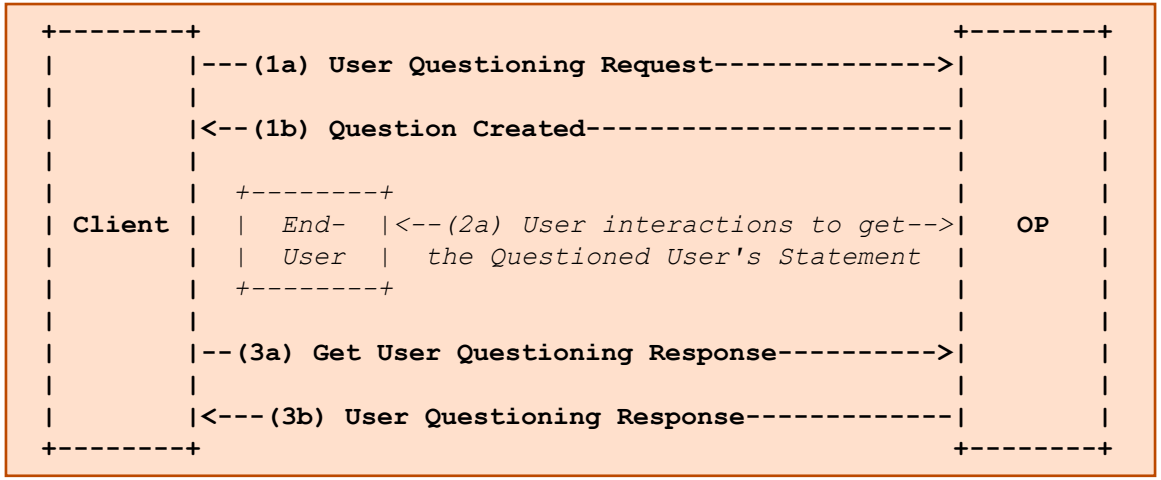


User Statement Token

```
{   "issuer":"https://server.example.com",
    "audience":"cLiEnT_Id_AzErTy",
    "id":"84c1d9d6-62e5-4803-ac0e-36b858c",
    "statement":"accepted",
    "statement_date":"1311282975",
    "user_id"="33612345678",
    "user_id_type"="MSISDN"
    "question_displayed":"An example message to display",
    "used_qcr":"2",
    "used_qmr":"CLICK_OK"}
```

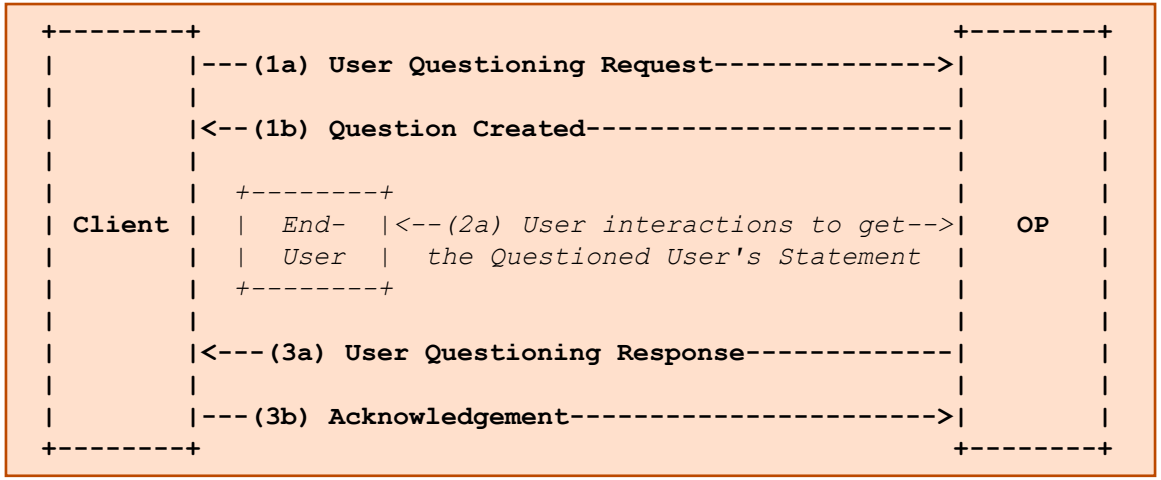
Pulled-By-Client Flow

The Client polls the OP for the User Statement Token



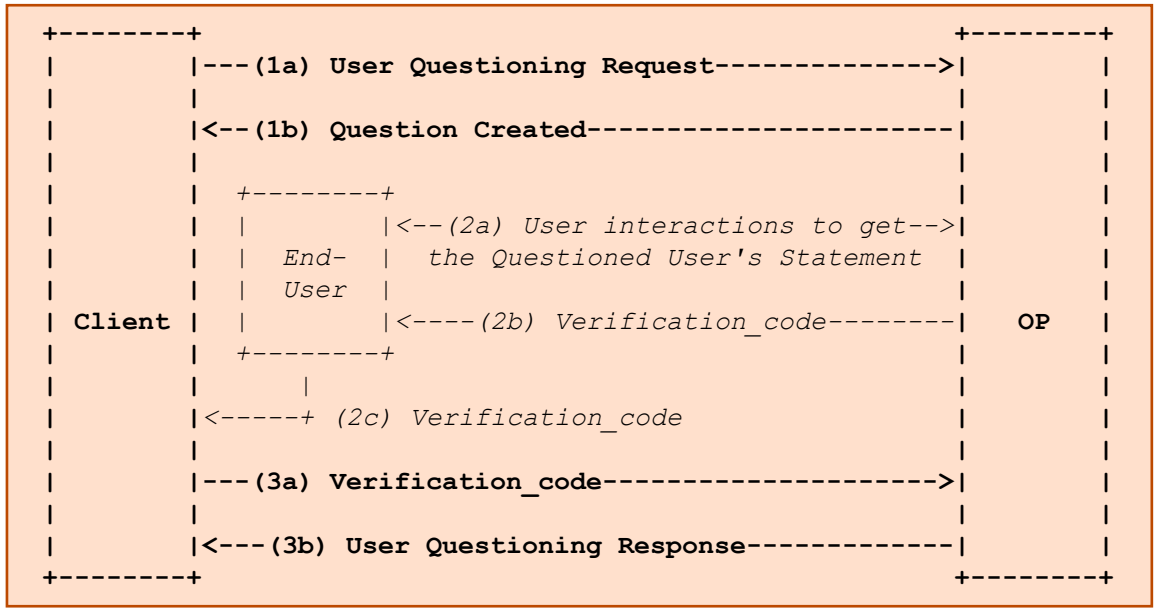
Pushed-To-Client Flow

The OP sends the User Statement Token to the Client



Terminated-By-Client Flow

The Client supplies the OP with a verification_code in order to get the User Statement Token



Pending issues

- XML2RFC
  a.k.a. has anyone got a WYSIWYG editor ? ;)
- Poll rate
  a.k.a. how to handle high rate polling ?
- user_id in the User Statement Token
  a.k.a. which user_id should be included in the User Statement Token ?
- Terminated-By-Client Flow
  a.k.a. how to handle 3-D Secure ‘SMS OTP’ ?
- Accept / Deny has a poor semantic
  a.k.a. how to handle questions like ‘yes/no?’, ‘which?’, ‘how much?’…?

Poll rate

a.k.a. how to handle high rate polling ?

Possible approaches:

- give an example of convenient rate (e.g. 3 seconds) in the draft
- when the rate is too high,
  - notify the Client (e.g. HTTP 429 Too Many Requests)
  - notify the Client with a rate limit
  - warn and ban the Client

user_id in the User Statement Token

a.k.a. which user_id should be included in the User Statement Token ?

Proposal:

User Questioning Request	User Statement Token (in User Questioning Response)
AT (Client) + MSISDN	client_id + MSISDN
AT (Client) + sub	Rejected. If the Client has a sub, it can get a AT (Client + RO) using the JWT Profile for Oauth,
AT (Client + RO)	client_id
AT (Client + RO) + MSISDN	Rejected. The MSISDN must be removed.
AT (Client + RO) + sub	Rejected. The sub must be removed.

Terminated-By-Client Flow (1/2)

a.k.a. how to handle 3-D Secure ‘SMS OTP’ ?

What is 3-D Secure?

- it’s a protocol used to secure online credit card transactions
- it’s branded ‘Verified by Visa’, ‘MasterCard SecureCode’, …

What is 3-D Secure ‘SMS OTP’?

- the user enters his credit card number, on his web browser
- the user receives a SMS including an OTP, on his mobile
- the user enters the OTP on the bank site, on his web browser

Why is there a Terminated-By-Client Flow?

- SMS OTP is required by Banks
- but, SMS OTP is not mentioned by GSMA CPAS4

Terminated-By-Client Flow (2/2)

a.k.a. how to handle 3-D Secure ‘SMS OTP’ ?

Two approaches:

- **3-D Secure is in the scope**
  - The draft-user-questioning includes the ‘Terminated-By-Client Flow’
  - The draft-user-questioning is more complicated
  - But, interactions requiring a code given by the End-User to the Client are standard
  - And, such interactions add security (explicit user action, same user on both devices)

- **3-D Secure is out of scope**
  - The ‘Terminated-By-Client Flow’ can be removed
  - Option 1: The SMS OTP interactions are hidden in “(2) User interactions to get the Questioned User's Statement”, but, there is a need for another specification to standardize these interactions as they impacts each Client and each OP. The OP can use SMS OTP as fallback.
  - Option 2: The SMS OTP interactions are managed by the Client (OTP created by the Client, included in the question and validated by the Client). The Client can use SMS OTP as fallback (the OP can not).

Accept / Deny has a poor semantic

a.k.a. how to handle questions like ‘yes / no?’, ‘which?’, ‘how much?’…?

In the current draft, there are two possible statements:
- accepted / denied

Even for boolean answer, it’s not enough. Some questions would get other answers:
- yes / no
- true / false
- granted / denied

How could we had more semantic in the possible responses?

There are two aspects:
- defining the type of wanted statement
  - e.g. boolean, free text, free number, choice, multiple choice, …
- defining the real display of the question and statements
  - e.g. « Accept /Deny » is different from « Agree / Disagree » and from « Yes / No »

Possible Evolutions

Possible Evolutions

- **Multiple choices in Statement**

```
How was your purchasing experience at Store?
(Excellent) (Not so bad) (Poor)
```

```
Who do you want for President?
(Mr Blue) (Mr Red) (Mr Green)
```

- **Multiple values in Statement**

```
To complete your order, do you need any sauce? (multiple choice)
(Ketchup) (Mustard) (Barbecue)
```

```
Your order should have been delivered. Can you confirm?
(OK, I got my parcel) (No, I got nothing) (I wanna be called by a sale representative)
```

- **Free number in Statement**

```
Thanks for donating to Charity.org. How much do you want to give this year?
[__50] euros (Donate) (Not this year)
```

- **Free text in Statement**

```
Can you enter numberplate so that we can order compliant tires?
[__DE-234-AZ] (Submit) (Cancel)
```

Thanks