MODRNA GSMA Workshop

Amsterdam Verizon office

May 11th & 12th 2017

Participants (subscribed):

Bjorn Hjelm, Verizon

John Bradley, Ping Identity

Philippe Clement, Orange (minutes editor)

Axel Nennker, DT

Bharadwaj Pulugundla, Verizon

Charles Marais, Orange

Gautam Hazari, GSMA

Gonzalo Fernández Rodríguez, Telefonica

Grzegorz Skowron-Moszkowicz, Play (May 11th )

Hubert Mariotte, Orange (May 11th )

James Manger , Telstra (May 12th)

Keith Uber, Ubisecure

Petteri Stenius, Ubisecure

[sercolle@telcel.com](mailto:sercolle@telcel.com)    Sent

Shahram Mohajeri, AT&T

Venkatasivakumar Boyalakuntla, GSMA

Agenda:

* MODRNA WG and related working groups (FAPI) status update
* CPAS work status update
* Technical Topics
  + Finalizing Token retrieval in the backchannel
  + Provider Metadata – Mobile Connect Profile
  + Use of claims value in Resource calls
  + User Agent security
  + Security Considerations for OpenID Connect Account Porting specification
* Future Topics

Mobile Connect Evolved Architecture – Discovery and Dynamic Client Registration

Discussion:

# MODRNA WG and related working groups (FAPI) status update

Different OIF working groups represent an interest for GSMA-Mobile connect work. A Liaison is under construction to exchange between the 2 bodies.

## OIF/MODRNA presentation last week in Mountain View IIW.

Security aspects have been collected regarding Account Porting spec and have to be discussed during this workshop with James. Security parts will have to be detailed.

## Implementers draft

4 drafts are migrated to “implementers draft” following the recent vote and will evolve as modifications are requested.

* Authentication Profile
* Account Porting
* User Questioning API
* Client Initiated Backchannel Authentication

Next step will be to have another version of implementers’ draft, or go directly to final specs. In the case of a more mature spec is provided for one document, a vote on this document can occur, independently of the others.

## FAPI status

For Open Banking, (private) certificates could be used to build software statements in the dynamic registration. A discussion is scheduled between FAPI and Open Banking WG in UK. No document is today visible before public announcement by Open Banking Consortium.

# CPAS work status update

Account porting work is considered closed for CPAS. In case of changes in the specs, CPAS will go back to them. Some proposals rose towards simplification regarding privacy considerations, without modifying the flows.

Error codes: a new version of a technical reference (errors, scopes…) is circulated to be discussed.

Mobile Connect detail record (MCDR): standard structures are requested by some MNOs, to be addressed in CPF.

Back Channel Authentication: An anonymous vote occurred in CPAS. The choice was between:

* MC BC extending JWT Assertion
* MC BC Communication using MC Profile / OIDC Core / CIBA concepts

The CIBA extension has the preference, despite a lack of some participants. None has deployed, it’s a preference that is declared. Remarks from the group emerge regarding the anonymous status of the vote, and the lack of argumentation in it.

In the next CPAS, comments will be extracted and discussed again. MODRNA WG is solicited to assess technically the different possibilities.

* discussion to be established in CPAS on clear arguments
* MODRNA to assess technically the different possibilities

# Technical Topics

## Finalizing Token retrieval in the backchannel

### CIBA draft Status

Context: Access Token retrieval is at stake, whatever the fact the user is in interaction in the flow or not.

### JWT assertion Draft status

Reminder: This spec represents a way for an RP to get an access token in a sync or async mode thanks to a JWT assertion. The advantage is that the request is totally protected. Grant types are added. Identity of the user can be embedded in the JWT assertion if available.

### Global discussion on back channel token retrieval

How do we solve backchannel access when the user is not in the flow ?

2 functions have to be distinguished:

* authentication (and access token retrieval),
* authorization that is used to trigger actions from RP side. In UK Bank case, the RP has to request consent from its own user before starting authorization flow to the bank.

#### Synchronous / Asynchronous

Discussions occur about the conditions in which the RP can start synchronous or asynchronous request to the OP. CIBA spec points out that the choice is done at RP registration moment.

One proposal is discussed about complexifying the code at RP and OP, introducing a test concerning a response type (sync or async) to trigger 2 different processes. This optimization is not adopted by the group, **and only the asynchronous mode is adopted**. The RP can fire a poll request just after the first request. The RP has preliminary registered for polling or push mode. In case of needed optimization, this will be addressed outside Mobile Connect.

To be compliant with OIDC specs, CPAS must verify the existence of a sector identifier in CIBA.

#### Client and request authentication:

Notice:

* For UK banks, a signed request object will be used.
* In the front channel, the redirect URI allows controlling who emits the request.

In the back channel, the question is raised whether the client MUST be authenticated, and SHOULD always use a signed authorization request object. In this approach, the IdP MUST implement authenticating client by treating the signed authorization request object. The IdP MAY accept another way. Suggestion: Simplify CIBA regarding the authentication of the client to the token endpoint. This shouldn’t impact UQ spec.

Discussion about Pairwise Identifiers: Pairwise Identifiers SHOULD be used. In CIBA notification mode the Client notification endpoint’s URL is used as the default sector\_identifier.  
In CIBA Polling Mode the sector\_identifer MUST be specified at registration time.

Conclusion:

* The request to the Authorization Endpoint MUST be authenticated. Because it is a server to server request the methods for Client Authentication from OpenID Core can be used.  
  The request SHOULD use a signed request object. If the signature algorithm is “none” then still the request MUST be authenticated. When the request object’s signature is valid then this counts as a Client authentication.
* Consensus provided by the group on this proposal, the content of the request object MUST conform to the OpenID Connect request object.
* GSMA to provide CPAS CIBA enhancements to MODRNA before end of May. MODRNA will then revise it towards a new MODRNA CIBA implementers draft for unique reference for both entities.

Discussions occurred about transmitting client secrets in http basic, and regarding the similarities for client authentication towards the authorization and token endpoints.

Open discussions about possible elimination of polling from CIBA for entities that support symmetric keys, when posting back URIs in the sector identifier. The OP should publish a new authentication endpoint file.

A specific endpoint for polling is suggested, published in the discovery document, for optimization aspects.

* Conclusion is to allow:
* Authentication endpoint,
* token endpoint,
* polling endpoint
* Backchannel endpoint.
* Polling endpoint can be the same as the token endpoint.

About discovery, Mobile Connect discovery service provides today RP with all the Issuer endpoints. This is subject to change in the future MC architecture.

Discussions around usage of the binding message with CIBA during the authentication. Remarks are provided on the fact that RP CANNOT control the OP authentication process, and using the binding message for other things can be detrimental to MNO responsibility and liability. 2 things to distinguish for the discussion:

* the design of the authentication screen, that could be agreed between RP and OP with preconfigured messages and graphical elements,
* any message at the total intention of the RP that could be a new surface of attack and MUST be treated separately.

## Provider Metadata – Mobile Connect Profile

The way to design this part will be discussed in CPAS. A JSON Structure will be used for keys, questions about one registration for one or several keys. One IANA registration to be done for a minimum of one key.

## Use of claims values in resource calls

OK to design any API for resource access, but be cautious on any ambiguity (and avoid them) between core OIDC specs and API parameters.

## User Agent Security

Not addressed during the global discussion.

## Security considerations for OIDC Account Porting specification

Reminder of the context: presentation of the AP spec to the IIW in Mountain View. Security concerns have risen along the feedback.

Along the porting, no way exists to do a partial port. A user must be able to trust only a part of all his RPs to apply migration. The ability to not port must be preserved. How the user consents is important, regarding the 2 IdPs. It’s not realistic to authenticate to both MNO at the same time with Mobile Connect.

Discussion on the naming of the function: “Account linking” versus “account porting” versus “account replacement”? , taken into consideration that the objective is to simplify and automate the change at the RP of the couple “Old issuer + old sub” to “New issuer + new sub”.

Investigations are done on the fact that the new OP can instigate the porting at the very first time user connects to it. To be taken into consideration: the danger that a fake IdP could trigger the operation.

* James will update the security section.
* John and Bjorn to share this draft with FAPI and Heart workgroups.

The single porting token has the preference regarding privacy.

AN RP has today the same client ID – client secret for all MNO, this should change in the future architecture.

# Future Topics

## Mobile Connect Evolved architecture – Discovery and Dynamic client registration.

Not addressed, candidates for a next workshop, according intentions of use from both groups.

# Next workshop

Dynamic client registration and discovery architecture will probably be part of it. Deadlines in CPAS work can impact the schedule, to be set in H2 2017.