User Questioning Service Enabler Technical Specification

Version 1.2

06 December 2022

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

The GSMA Identity program focuses on positioning Operators as trusted providers of Identity and attribute services to third party Service Providers. Within this, the programme identifies a set of products that collectively are referred to as Mobile Connect.

This document specifies an optional extension to the Mobile Connect core framework, the User Questioning Service Enabler, which can be used for supporting a range of use cases where a User is being asked to authorise an action or submit a preference (e.g., voting, User surveys etc.).

The User Questioning Service Enabler builds on the User Questioning API originally defined within the OpenID Foundation (OIDF), and defines how this capability should be used within the context of the Mobile Connect framework. An Operator wishing to use this capability will define a Product that utilises the User Questioning Service Enabler, either in isolation or potentially bundled with other Mobile Connect services based on the target use case.

1.2 Scope

In Scope	Out of Scope
• User Questioning Service Enabler specifications • Topics to be addressed when defining a Product based on the User Questioning Service Enabler	• Product definition

1.3 Audience

The target audience for this document are the Mobile Operator service/technical departments who are considering deploying a product based on the User Questioning Service Enabler.

1.4 Conventions

The keywords “must”, “must not”, “required”, “shall,” “shall not,” “should,” “should not,” “recommended,” “may”, and “optional” in this document are to be interpreted as described in RFC2119 [31].

The values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

1.5 Definitions

Term	Description
Authentication Context Class Reference	Value that identifies the Authentication Context Class that the authentication performed satisfied.
Authentication Context Class	Set of authentication methods or procedures that are considered to be equivalent to each other in a particular context.

Authentication Methods References	Identifier for authentication methods used in the authentication.

1.6 Abbreviations

Term	Description
ACR	Authentication Context Class Reference
AMR	Authentication Methods References
API	Application Programming Interface
AT	Access Token
ID GW	Identity Gateway
LoA	Level of Assurance
MC	Mobile Connect
Operator	Mobile Network Operator
OIDF	OpenID Foundation
PCR	Pseudo-Anonymous Customer Reference
RT	Refrest Token
SP	Service Provider
UQ	User Questioning

1.7 References

Ref	Doc Number	Title
[1]	IDY.05	Mobile Connect Technical-Reference
[2]	IDY.04	CPAS Mobile Connect Core Technical Requirements
[3]	IDY.01	Mobile Connect Device Initiated OIDC Profile
[4]	IDY.02	Mobile Connect Server Initiated OIDC Profile

1.8 International Standards references

Ref	Doc Number	Title
[1]	OpenID Connect User Questioning API	http://openid.net/specs/openid-connect-user-questioning-api-1_0.html

2 Functionality overview

The User Questioning Service enables an SP application to send a question to a Mobile Connect User and receive a response in return, digitally-signed by the Operator. In order to ensure that the correct User is responding, the User will be authenticated (using the existing Mobile Connect authenticators) prior to submitting their response – note that based on the prevailing authenticator type being used by the Operator, this may restrict the size of question and the number and size of statements that can be displayed[1] - this is discussed later on. Note also that the User may or may not be interacting with the SP application when the question is asked

The User Questioning Service Enabler is classed within the Mobile Connect Framework as a Resource[2] and hence the SP will need first to acquire an Access Token for the target User before submitting their request to the User Questioning resource. This Access Token can be obtained using different means (for example: using Device-Initiated or Server-Initiated methods[3]).

More details on the end-end flow are included later in this document.

The User Questioning Service Enabler is based on the User Questioning API specified within the OpenId Foundation. The full specification is available at: http://openid.net/specs/openid-connect-user-questioning-api-1_0.html

3 Summary of requirements

No.	Requirement
1	An Access Token provided using Mobile Connect (MC) defined modes by the ID GW shall be used by the Service Provider (SP) when consuming User Questioning.
2	The SP service request must include a Question which will be displayed on an Authenticator advising the User of the Question they are being asked to Respond to.
3	The SP service request must include authenticator and the LoA (single or multi factor) to be used.
4	The SP must provide the Statements in the service request.
5	The Service shall use the authenticator and LoA (single or multi factor authentication) requested and display the Question and Statements when no authenticator limitations exist.
6	When authenticator limitations regarding how Questions and Statements can be presented exist, the Service shall provide options such as mapping schemes and/or error messages.
7	The Service should respond to the SP with the User's response: selected statement, used authenticator and used LoA.
8	If the User cancels or the session times out, the Service should respond to the SP with an appropriate error.

[1] The SIM applet authenticator, as an example, is often limited to present two options with static displays (yes/no) and have character limitation

[2] OAuth 2.0 Resource Server

[3] In the future, other ways (like OAuth2.0) may be included in the scope of Mobile Connect

9	The logging of transactional data must allow for effective fault-finding and problem resolution as well as comply with applicable data protection and privacy laws as well as the Mobile Connect Privacy Principles.
10	User consent for the processing of the response must be handled in accordance with regulation and Mobile Connect privacy policies.

4 Indicative Architecture

Here is a high level indicative architecture for the User Questioning capability, in the context of the Mobile Connect Framework:

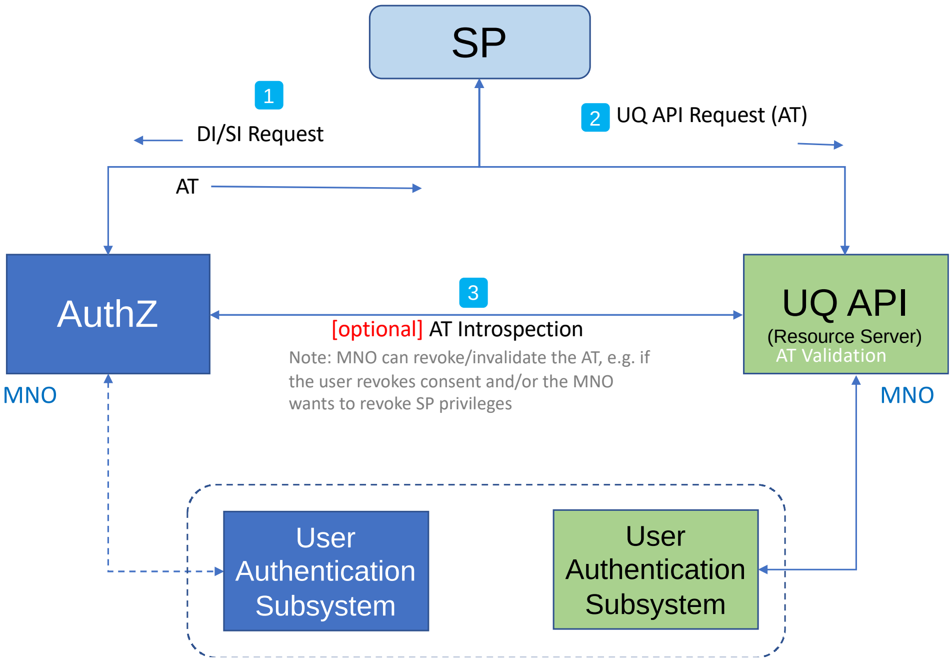

SP
1
DI/SI Request
AT
2
UQ API Request (AT)
AuthZ
MNO
3
[optional] AT Introspection
Note: MNO can revoke/invalidate the AT, e.g. if the user revokes consent and/or the MNO wants to revoke SP privileges
UQ API
(Resource Server)
AT Validation
MNO
User Authentication Subsystem
User Authentication Subsystem

Figure 1 Indicative Architecture

- The User Authentication Subsystem is a logical component, and the same physical system can be implemented by both the logical User Authentication Subsystems in the diagram
- The User Authentication Subsystem connected to the AuthZ component is used for Authenticating the User before sharing the Access Token (when needed)
- The User Authentication Subsystem connected to the UQ API Resource Server component is used for Authenticating the User for the question/answer interaction

5 Usage guidelines

This section provides guidance on how the User Questioning Service Enabler can be used in the definition, deployment and operation of Mobile Connect products.

5.1 Service authorisation

In order to leverage the User Questioning capability to submit a question to a User, the SP must first obtain an Access Token.

5.2 User Questioning flows

The User Questioning enabler supports two mechanisms when the SP issues its request to the User Questioning Resource:

1. Pulled-By-Client Flow: in this flow, the SP will poll the Operator to get the User Questioning Response.
2. Pushed-To-Client Flow: in this flow, the Operator will send the User Questioning Response to the client_notification_endpoint registered by the SP.

The flowing table provides the references for each flow.

Flow	Reference
Pulled-By-Client Flow	http://openid.net/specs/openid-connect-user-questioning-api-1_0.html#rfc.section.1.4.1
Pushed-To-Client Flow	http://openid.net/specs/openid-connect-user-questioning-api-1_0.html#rfc.section.1.4.2

Table 1: User Questioning flows

Generally, it is recommended to use the second flow as this reduces the amount of requests between an SP and Operator.

5.3 User Questioning Request

When submitting a User Questioning request to an Operator, an SP will stipulate a question to display to the User on the User’s Mobile Connect authenticator, and a set of “statements’ that the User can choose from when answering the question.

5.3.1 <question_to_display> and <statements_to_display>

The SP request MUST provide both the Question <question_to_display> and one or more Statements <statements_to_display> from which a User can select when answering the question.

The following table defines the character sets for Question and Statements in the User Questioning Request that SHALL be supported for Mobile Connect. The actual character set used by an SP is implementation dependent.

Character set	Reference
UTF-8	ISO/IEC 10646:2017
GSM7 Default Alphabet	3GPP TS 23.038

Table 2: Character set for <question_to_display> and <statements_to_display>

Some of the Mobile Connect authenticators have limitations that may restrict the length of the question that can be displayed, the number of statements and the length of the statements that can be displayed or the wording of the statements that are displayed.

For example, the SIM Applet authenticator has a limitation of 106 characters[4] for the question when using the character set “GSM7 Default Alphabet” and is limited to two predefined statements, one positive and one negative, and no control exists on the exact wording used within the statements as this is dictated by the design of the SIM applet itself.

As such, the User Questioning service may only support dynamic stipulation of the statements by the SP if alternate authenticators are used, such as a smartphone app authenticator.

These variables and constraints need to be discussed with the SP during the onboarding/contracting phase to ensure that Questions and Statements will be presented correctly. Given the dependencies of User Questioning on the authenticator capabilities, it is beneficial that all Operators within a market deploy the same authenticators and are able to support the same service level (in terms of question size and statement support).

5.3.2 <acr>

In order to ensure that the correct User is responding to a question submitted via User Questioning, the User will typically be required to authenticate. When submitting a User Questioning request, the SP has the option of defining the level of assurance (LoA) they require for this User authentication.

The following table defines the <acr> values that SHOULD be used for Mobile Connect.

<acr> values	Reference
2	CPAS04 Authenticator Options v1.2.7
3	CPAS04 Authenticator Options v1.2.7

Table 3: <acr> values

The <acr> indicates the level of assurance (i.e. LoA) and is bound to the security properties of the authenticators used when answering the question.

Note that in the case of <acr> = 2 (LoA2), the User is implicitly authenticated through having possession and control of the mobile phone through which they are being asked to respond to a question. In the case of <acr> = 3, the User must explicitly authenticate (e.g. enter a PIN) to be able to answer the question.

5.3.3 Resource Server Design Guidelines

The realisation of the UQ API Resource Server needs to look into the following design guidelines:

- There needs to be an integration with an Authentication Subsystem. It can reuse the Authentication Subsystem integrated with the AuthZ Server or can use a different one
- It needs to have policy realisation for authenticator selection:
    - Can a fallback happen when a certain Authenticator is not available?

[4] This is the limit if message concatenation is not supported; otherwise the limit is higher

  - Is there a policy of using a specific authenticator when multiple authenticators are available?
  - Is there a minimum LoA for the product in use?

- The integration with the Authentication Subsystem needs to consider the latency involved in the User interaction point (e.g. asynchronous integration can be used)

5.4 User Questioning Response

5.4.1 Statement selected

The statements made by the Questioned User are in a User Statement Token sent to the SP in a User Questioning Response (see section 2 [1])

5.4.2 <amr>

The following table defines the <amr> values that SHOULD be used for Mobile Connect to indicate to the SP the authenticator used.

<amr>	Reference
SIM_OK	CPAS-MC-Technical-Reference 1.0 FINAL
SIM_PIN	CPAS-MC-Technical-Reference 1.0 FINAL
SM_APP_OK	CPAS-MC-Technical-Reference 1.0 FINAL
SM_APP_PIN	CPAS-MC-Technical-Reference 1.0 FINAL
USSD_OK	CPAS-MC-Technical-Reference 1.0 FINAL
USSD_PIN	CPAS-MC-Technical-Reference 1.0 FINAL
SMS_URL_OK	CPAS-MC-Technical-Reference 1.0 FINAL

Table 4: <amr> values

6 Authenticator limitations and considerations

As noted in previous sections, some of the Mobile Connect authenticators have limitations that may restrict the length of the question that can be displayed, the number of statements, the length of the statements that can be displayed or the wording of the statements that are displayed.

For example, the SIM Applet authenticator has a limitation of 106 characters for the question when using the character set “GSM7 Default Alphabet” and is limited to two predefined statements, one positive and one negative, and no control exists on the exact wording used within the statements as this is dictated by the design of the SIM applet itself.

To ensure a positive user experience, it is vital that the Operator clearly states the constraints of the authenticator/s in order to ensure that the SP is able to present the Questions and Statements in a comprehensible manner to the User and agree any fallback mechanism (e.g., where particular authenticators in the market are unable to fully support the SP request) at service setup. The following table defines approaches an SP can take to mitigate authenticator limitations in markets where there are multiple authenticators available. The strategies listed in the table below and chosen when defining the product are exclusive.

SP Strategies	Description
minimal_set	Adhere to a set of display capabilities that every authenticator can handle.
try_and_error	If the authenticator is not displaying what is requested, an error is returned (see section 5 [1]). Based on the error the SP can adapt the request to a less capable authenticator and try again
agreed_statements	The statements that can be supported are static based on the authenticators available in-market. The Operator and SP agree on the mapping that should be used between requested statements and supported statements to ensure that the semantic is respected.(e.g. “Yes”/”No” or ”True”/”False”…)
adapt_statements	The statements are not restricted, but if an authenticator has a limitation, it can display fallback statements that are different from the requested statements. These fallback displayed statements must be defined in the Product and should have a simple semantic (e.g. “yes”/“no”). The partner is responsible to accept these fallback statements and to determine if they make sense regarding the question. The fallback statements are the same for all services and all questions in a given Product.

Table 5: SP strategies to mitigate authenticator limitations

The following table defines possible options for mitigating a range of different limitations.

Limitation	Options
If the authenticator is unable to display the “question_to_display”	• minimal_set • try_and_error
Restriction on the display of “statements_to_display”	• minimal_set • try_and_error
No control on the real display of the “statements_to_display” N.B. This happens when what is displayed to the User can not be dynamically chosen by the Operator. For instance, differing implementations on mobile phones can lead to discrepancies of the display of the positive/negative buttons.	• agreed_statements • adapt_statements

Table 6: Strategies to mitigate each limitation

7 Errors

The errors that shall be used with the UQ API are defined in OIDF specification section 5 [1].

However, if an SP wants to use UQ API for a non-registered User, the following error should be used (to be defined how the Operators forward a redirection URL so that the SP redirects the User to the MC registration performed by the Operator).

8 Summary of configurable options when defining a Product that uses the User Questioning Service Enabler

As noted in the previous sections, the User Questioning Service Enabler has the flexibility to support a range of different use cases. When defining a Product (and agreeing with an SP on the utilisation of the Product), there are a number of decision points that need to be taken into account:

Topic	Choices
User Questioning flow	Choice among: • Pulled-By-Client Flow • Pushed-To-Client Flow
Character set for “question_to_display” and “statements_to_display” in the request	Exclusive choice among: • UTF-8 • GSM7 Basic Character Set
Maximum number of characters for “question_to_display” in the request	Negotiated between Operator and SP to reflect target authenticator
Maximal number of characters for elements of “statements_to_display	Negotiated between Operator and SP to reflect target authenticator Note that only 2 statements reflecting a positive and negative User response may be supported in the case of a SIM applet
Maximal number of statements	Negotiated between Operator and SP to reflect target authenticator Note that only 2 statements reflecting a positive and negative User response may be supported in the case of a SIM applet
<acr>	Choice among the following depending on the authenticator used by the Operator(s): • 2 • 3
<amr>	Choice among the following depending on the authenticator used by the Operator(s): • SIM_OK • SIM_PIN • SM_APP_OK • SM_APP_PIN • USSD_OK • USSD_PIN • SMS_URL_OK • SEAM_OK

Table 7: Defining a Product based on the User Questioning Service Enabler

9 Use cases

This section covers a set of use cases for how the User Questioning Service Enabler can be used. These use cases do not constitute an exhaustive list. These use cases are presented for information only and depend on Operator's implementation.

9.1 Banking authorization

The Bank (SP) wants to use User Questioning during an online banking session for the User to authorise setting up a new payee.

9.1.1 Precondition

The User has registered for Mobile Connect. The Bank has the User's MSISDN and Operator details.

The Bank has requested an Access Token for User Questioning until it's revoked or expired. The Operator ID GW authorization server has provided an Access Token (AT) which the Bank can use with the Mobile Connect User Questioning API.

In this market, there is a mix of authenticators used by the Operators (SIM Applet and Smartphone Apps (SAA) for example).

The Bank has created the following Question for setting up a new payee:

"Do you want to add xxxx xxxx as a new payee to your account xxxx xxxx?" and the associated statements "I agree", "I disagree".

The table below defines the product parameters defined for this use case:

Topic	Choices
User Questioning flow	Pushed-To-Client Flow
"user_id_type[5]" in the request	msisdn
Character set for "question_to_display" and "statements_to_display" in the request	GSM7 Basic Character Set
Maximum number of characters for "question_to_display" in the request	93
Maximal number of characters for elements of "statements_to_display	10
Minimum number of statements	2
Maximum number of statements	2
ACR	3
AMR	SIM_PIN ,SM_APP_PIN

Table 8: Parameters for setting up a new payee use case

However, in some cases the Operator will use the SIM_Applet (User handset not supporting the SAA or SAA not installed by the end User for example). In order to take into account the SIM Applet limitations, the Operators and the SPs have to predefine the policies to be used. For example, the policies can be the following:

Policy	Value
`minimal_set`	
`agreed_statements`[6]	“I agree” & “I disagree”

Table 9 : Sample policy

9.1.2 Use case flow

1. The User is navigating on the Bank’s website and creates a new payee. The SP gives the User the options to authenticate this change via OTP or Mobile Connect. The User selects Mobile Connect.
2. The Bank uses MC User Questioning with the User MSISDN and passes the following to the Operator:
   - Question “Do you want to add xxxx xxxx as a new payee to your account xxxx xxxx?”
   - Statements “I agree” and “I disagree”
3. a) If the Operator uses the SAA, the Operator presents the Question and Statements[7] to the User in the SAA

   Option 1: The User clicks on “I agree”, enters their PIN and presses OK

   Option 2: The User presses “I disagree” enters their PIN and presses OK

   Option 3: The User presses “Cancel” (even if he clicks on anything else before)

[7] In case the Statement/s or Questions break the boundary conditions of the User’s authenticator the Operator will provide an error-code that will allow the SP to understand what to do next.

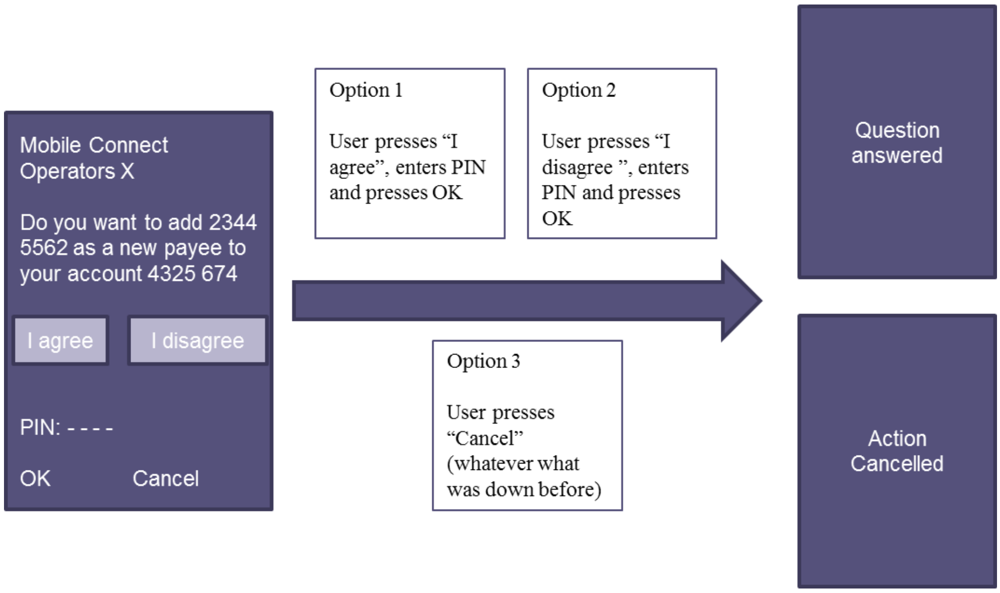

Mobile Connect
Operators X
Do you want to add 2344 5562 as a new payee to your account 4325 674
I agree
I disagree
PIN: - - - -
OK
Cancel
Option 1
User presses "I agree", enters PIN and presses OK
Option 2
User presses "I disagree ", enters PIN and presses OK
Option 3
User presses "Cancel" (whatever what was down before)
Question answered
Action Cancelled

Figure 2: Example of Smartphone App Use when setting up a new payee.

3. b) If the Operator uses the SIM Applet, the Operator presents the Question and Statements to the User.

Option 1: To validate their answer, the User enters their PIN and presses OK.

Option 2: To answer negatively to the question, the User presses Cancel.

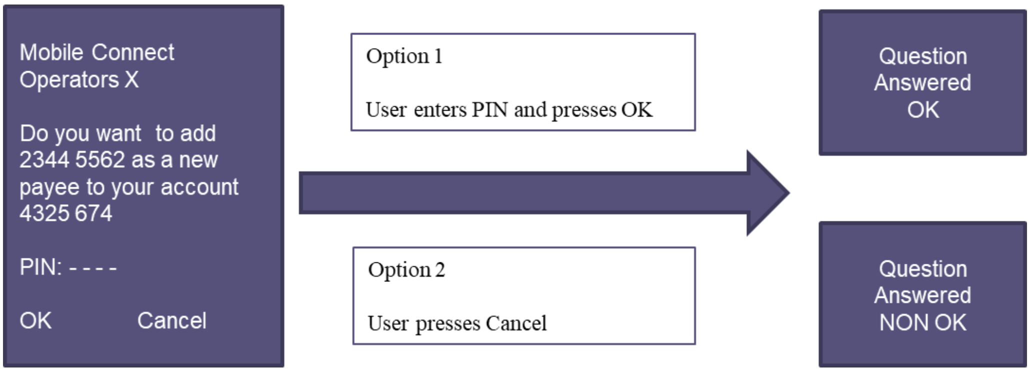


Figure 3: Example of SIM-Applet Use when setting up a new payee.

4. The Operator then provides a response to the SP containing the User's answer, proof of the answer, authenticator type used (amr) and level of assurance achieved (acr)

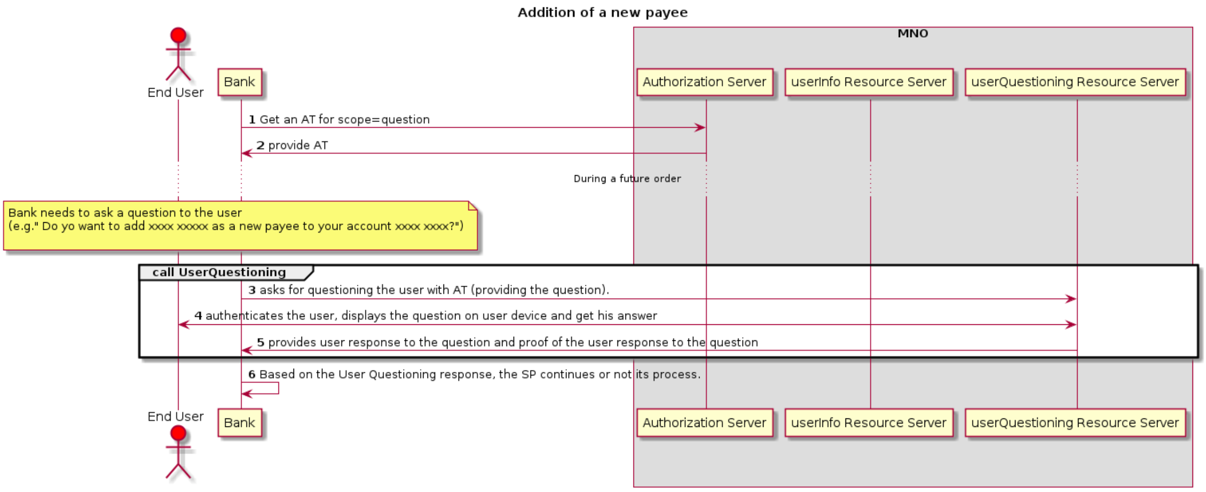

Addition of a new payee
MNO
End User
Bank
Authorization Server
userInfo Resource Server
userQuestioning Resource Server
1 Get an AT for scope=question
2 provide AT
During a future order
Bank needs to ask a question to the user
(e.g." Do yo want to add xxxx xxxxx as a new payee to your account xxxx xxxx?")
call UserQuestioning
3 asks for questioning the user with AT (providing the question).
4 authenticates the user, displays the question on user device and get his answer
5 provides user response to the question and proof of the user response to the question
6 Based on the User Questioning response, the SP continues or not its process.
End User
Bank
Authorization Server
userInfo Resource Server
userQuestioning Resource Server

Figure 4: Flow chart for setting up a new payee use case

9.2 Voting use case

A Community (SP) wants to use User Questioning to collect which candidate a User wants to vote for as president.

9.2.1 Precondition

The User has activated Mobile Connect using the Smartphone App Authenticator (SAA).

The Community has the User’s MSISDN and Operator details.

The User has previously navigated to the Community website and selected to vote using Mobile Connect. The Community created the account and stored the received Access Token and Refresh Token[8] for future use.

The Operator has given the Community the following details on how to use the SAA:

Topic	Choices
User Questioning flow	Pulled-By-Client Flow
“user_id_type”[9] in the request	not applicable
Character set for “question_to_display” and “statements_to_display” in the request	UTF8
Maximum number of characters for “question_to_display” in the request	2000
Maximal number of characters for elements of “statements_to_display	40
Minimal number of statements	1
Maximal number of statements	5
ACR	3
AMR	SM_APP_PIN

Table 10: Parameters for voting use case

As for this use case, the Operator will only use an SAA, there is no known limitation for the authenticator. So, there is no need to define a specific policy (for question to display or statements to display)

The Community has created the following Question for the Presidential election:

”Which candidate do you vote for as the Community President?”

The Community has also created the Statements

1. “MrXX”
2. “MrYY”
3. “MrZZ”

[8] The Refresh Token is used to get a fresh access_token without interaction with the end user when needed.

9.2.2 Use case flow

1) The User enters the Community voting website. The User selects to vote using MC.
2) The Community needs to ask a Question to the User ”Which candidate do you vote for as community president?” The Statements are “MrXX”, “MrYY”, “MrZZ”?
3) The Community asks for questioning the User with the previously received Access Token (providing the Question and Statements)
4) The Operator triggers the SAA on the mobile of the User presenting the Question and the Statements.
5) Option 1: The User selects one statement, enters the PIN and presses “Validate Your Choice”. The answer is sent from the SAA on the mobile.
   Option 2: The User presses “Refuse To Answer”. The answer is sent from the SAA on the mobile

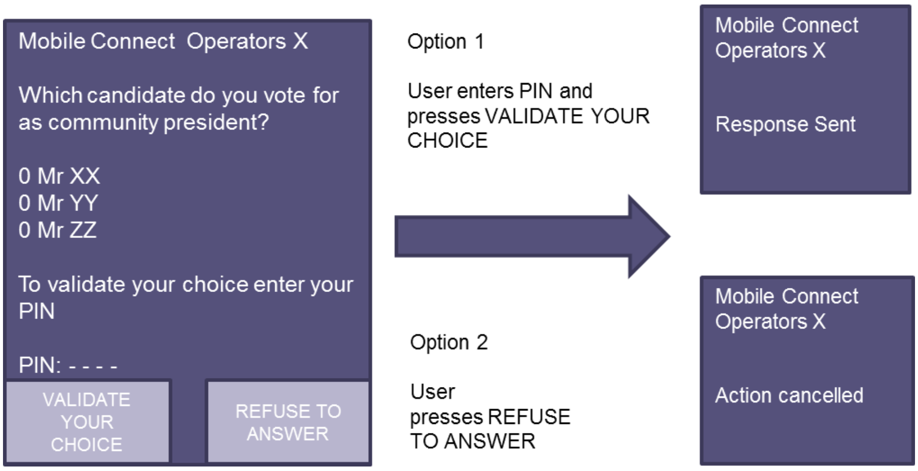

Mobile Connect Operators X
Which candidate do you vote for as community president?
0 Mr XX
0 Mr YY
0 Mr ZZ
To validate your choice enter your PIN
PIN: - - - -
VALIDATE YOUR CHOICE
REFUSE TO ANSWER
Option 1
User enters PIN and presses VALIDATE YOUR CHOICE
Option 2
User presses REFUSE TO ANSWER
Mobile Connect Operators X
Response Sent
Mobile Connect Operators X
Action cancelled

Figure 5: User flow for casting a vote.

6) Operator provides the answer and the proof of the answer to the SP

The flow-chart for the use case is the following:

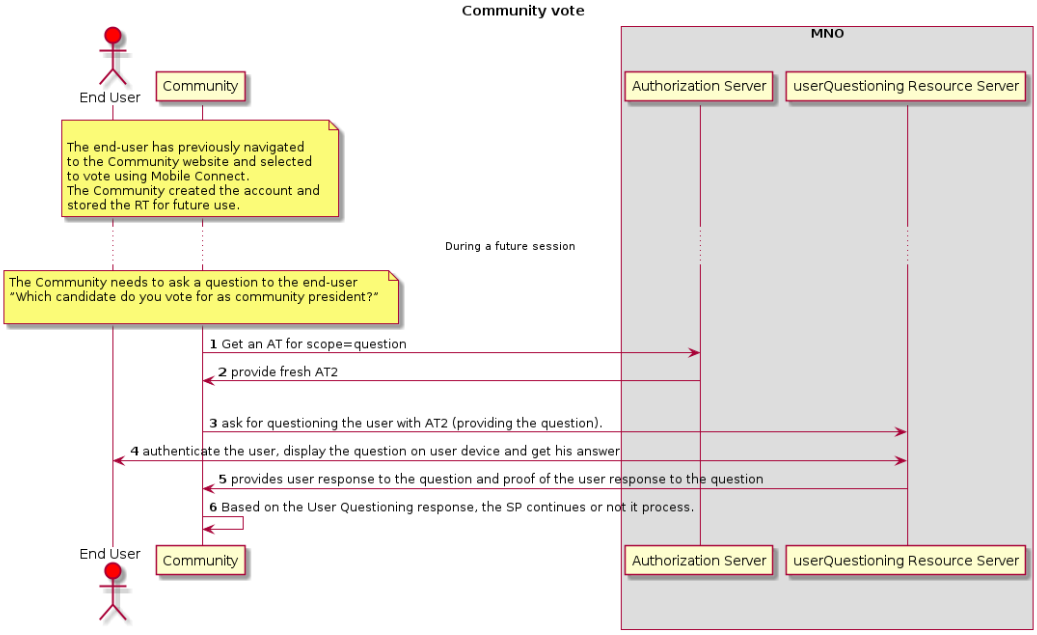

Community vote
MNO
End User
Community
Authorization Server
userQuestioning Resource Server
The end-user has previously navigated to the Community website and selected to vote using Mobile Connect.
The Community created the account and stored the RT for future use.
During a future session
The Community needs to ask a question to the end-user “Which candidate do you vote for as community president?”
1 Get an AT for scope=question
2 provide fresh AT2
3 ask for questioning the user with AT2 (providing the question).
4 authenticate the user, display the question on user device and get his answer
5 provides user response to the question and proof of the user response to the question
6 Based on the User Questioning response, the SP continues or not it process.
End User
Community
Authorization Server
userQuestioning Resource Server

Figure 6: Flow chart for “voting use case”

9.3 Ingredient choice use case using SMS+URL

A delivery restaurant (SP) wants to use User Questioning to ask the User which type of pepper they prefer for their pizza.

9.3.1 Precondition

The User has registered for Mobile Connect and has got an account with the SP.

The Operator ID GW authorization server has provided an Access Token (AT) and a Refresh Token (RT), the latter can be used to get a fresh Access Token when the initial one has expired. These Access Tokens can be used by the SP with the Mobile Connect User Questioning API.

The table below defines the product parameters defined for this use case

Topic	Choices
User Questioning flow	Pulled-By-Client Flow
“user_id_type” in the request	Not applicable
Character set for “question_to_display” and “statements_to_display” in the request	UTF8
Maximum number of characters for “question_to_display” in the request	2000
Maximal number of characters for elements of “statements_to_display	50
Minimal number of statements	2
Maximal number of statements	10
ACR	2
AMR	SMS_URL_OK, SEAM_OK

Table 11: Parameters for ingredient choice use case

As for this use case, the Operator will use SMS+URL only. It means that the Operator will send an SMS to the User. This SMS will contain a link to a page hosted on a Operator server where the Question and the Statements will be displayed.

The SP has created the following Question for the pepper choice:

”Do you prefer red or green pepper on your pizza. Please Select One”

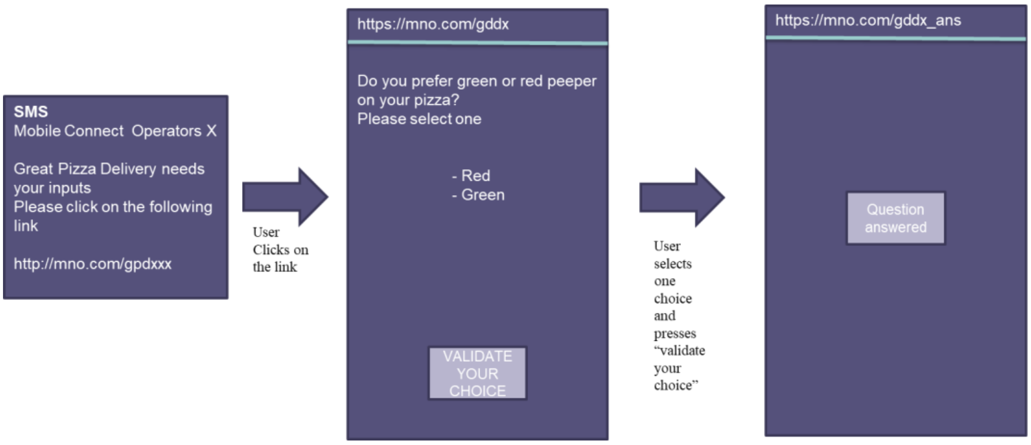
The SP has also created the Statements

- Red
- Green

9.3.2 Use case flow

1) Previously, the User has created an account on the SP website using MC Device Initiated Profile and agreed to be contacted by the SP. This means that the SP has got an Access Token and a Refresh Token from the Operator to be used for UQ API for this User
2) The User orders a pizza with peppers.

3) The SP needs to ask a Question to the User ”Do you prefer red or green pepper on your pizza? Please Select One”. The Statements are “Red”, “Green”
4) [Optional] If the SP only has an expired Access Token, it must use its Refresh Token to get a fresh Access Token.
5) The SP asks for questioning the User with the previously received Access Token (providing the Question and Statements)
6) The Operator sends an SMS to the User containing a link to an Operator webpage where the question and the statements will be displayed.
7) The User clicks on the link, selects one of the statements and validates its choice.



SMS
Mobile Connect Operators X

Great Pizza Delivery needs your inputs
Please click on the following link

http://mno.com/gpdxxx

https://mno.com/gddx

Do you prefer green or red peeper on your pizza?
Please select one

- Red
- Green

https://mno.com/gddx_ans

Figure 7: User flow for ingredient choice.

8) The User is authenticated by the fact that he clicks on the embedded link in the SMS. Optionally, if the User device is connected on the Operator radio network, the Operator can confirm that it is the same MSIDSN that received the SMS. In this case, the Operator provides the answer, the proof of the answer to the SP and SMS_URL_OK+SEAM_OK as amr.

The flow-chart for the use case is the following:

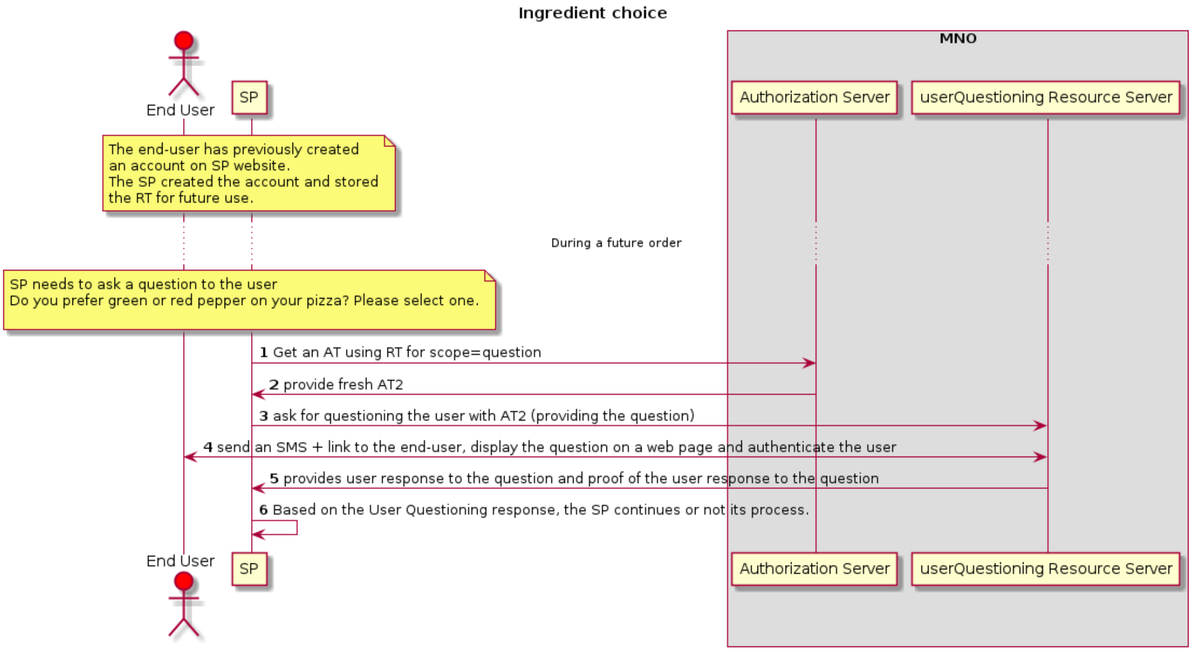

Ingredient choice
MNO
End User
SP
Authorization Server
userQuestioning Resource Server
The end-user has previously created an account on SP website.
The SP created the account and stored the RT for future use.
During a future order
SP needs to ask a question to the user
Do you prefer green or red pepper on your pizza? Please select one.
1 Get an AT using RT for scope=question
2 provide fresh AT2
3 ask for questioning the user with AT2 (providing the question)
4 send an SMS + link to the end-user, display the question on a web page and authenticate the user
5 provides user response to the question and proof of the user response to the question
6 Based on the User Questioning response, the SP continues or not its process.
End User
SP
Authorization Server
userQuestioning Resource Server

Figure 8: Flow chart for “ingredient choice use case”

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	26/03/2018	New document	IDY/TG	Nicolas Aillery / Charles Marais (Orange)
0.2	3/04/2018	First release	IDY/TG	Nicolas Aillery / Charles Marais (Orange)
0.3	25/04/2018	First update after reviews	IDY/TG	Nicolas Aillery / Charles Marais (Orange)
0.4	02/05/2018	Second update after reviews	IDY/TG	Nicolas Aillery / Charles Marais (Orange)
0.7	22/06/2018	Review follwing call GSMA Orange	IDY/TG	Gautam/Niklas (GSMA)
0.8	04/07 2019	Review following Operator meeting	IDY/TG	Hubert (Orange)/Niklas (GSMA)
1.2	12/02/2020	Added the content for v1.2	IDY/TG	Gautam Hazari (GSMA)
1.2	27/01.2020	TG Apprval	TG	Yolanda Sanz, GSMA

A.2 Other Information

Type	Description
Document Owner	IDG
Editor / Company	Hubert Mariotte/Orange

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com.

Your comments or suggestions & questions are always welcome.