Out of Band Authentication Adapter

Adapter Loading Process

The ActiveAccess ACS performs Out Of Band (OOB) challenges through OOB Adapters, which connect the existing OOB authentication system with ActiveAccess. During 3DSecure 2.0 challenge flows where OOB Authentication is required, the `ACS` will trigger the external OOB process and perform interactions with the Cardholder via the OOB Adapters.

For this purpose, the `ACS` communicates with the existing `OOB-System` via a middleware, known as the OOB Adapter. The OOB Adapter can be either loaded locally by the ACS or communicated via HTTP calls, known as the Native API and REST API versions respectively.

ActiveAccess supports two variants of the OOB flow — Standard and Alternative — both compliant with EMV® 3-D Secure guidelines.

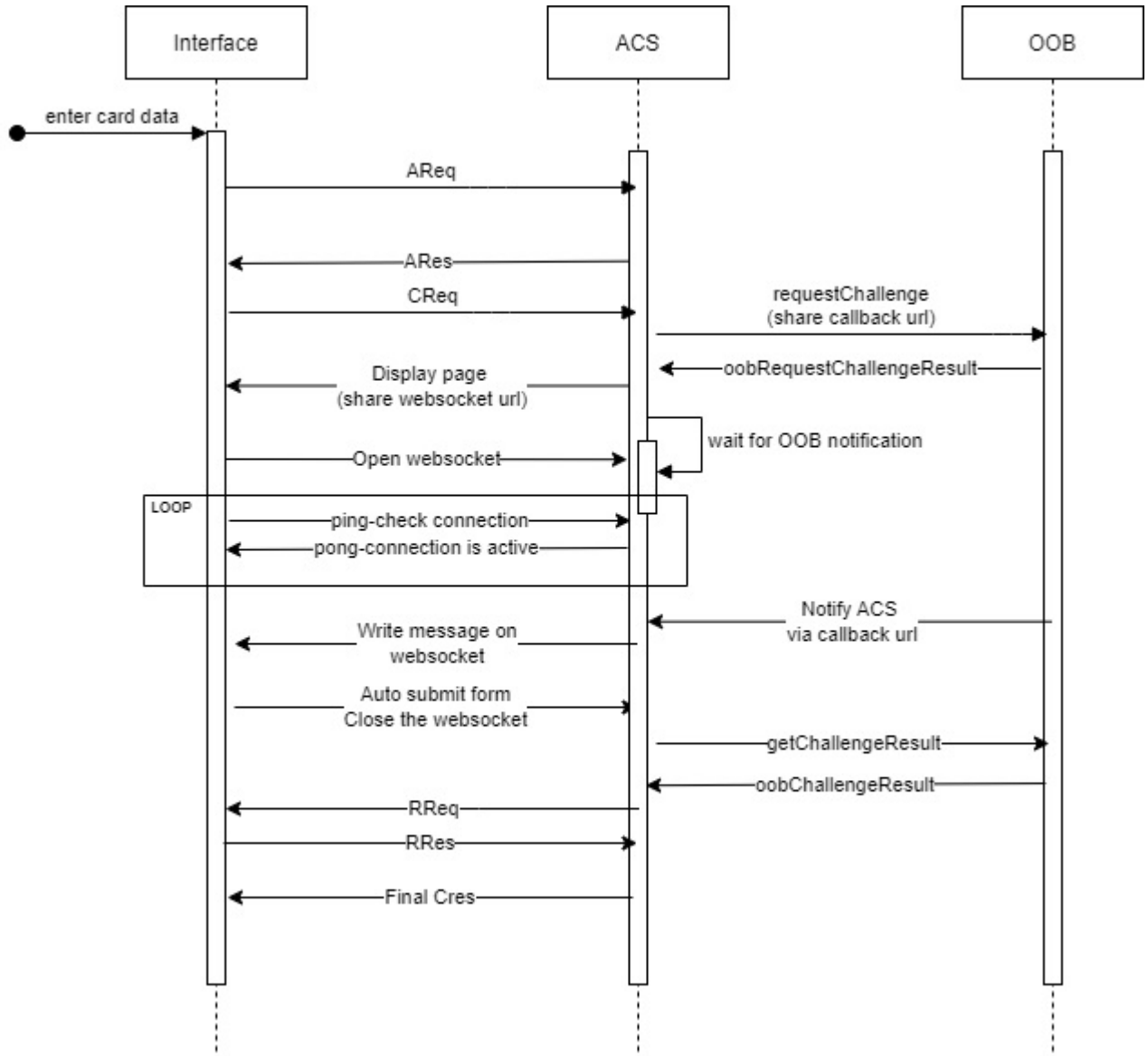
The key distinction between them lies in when the Result Request (RReq) and final Challenge Response (CRes) messages are generated:

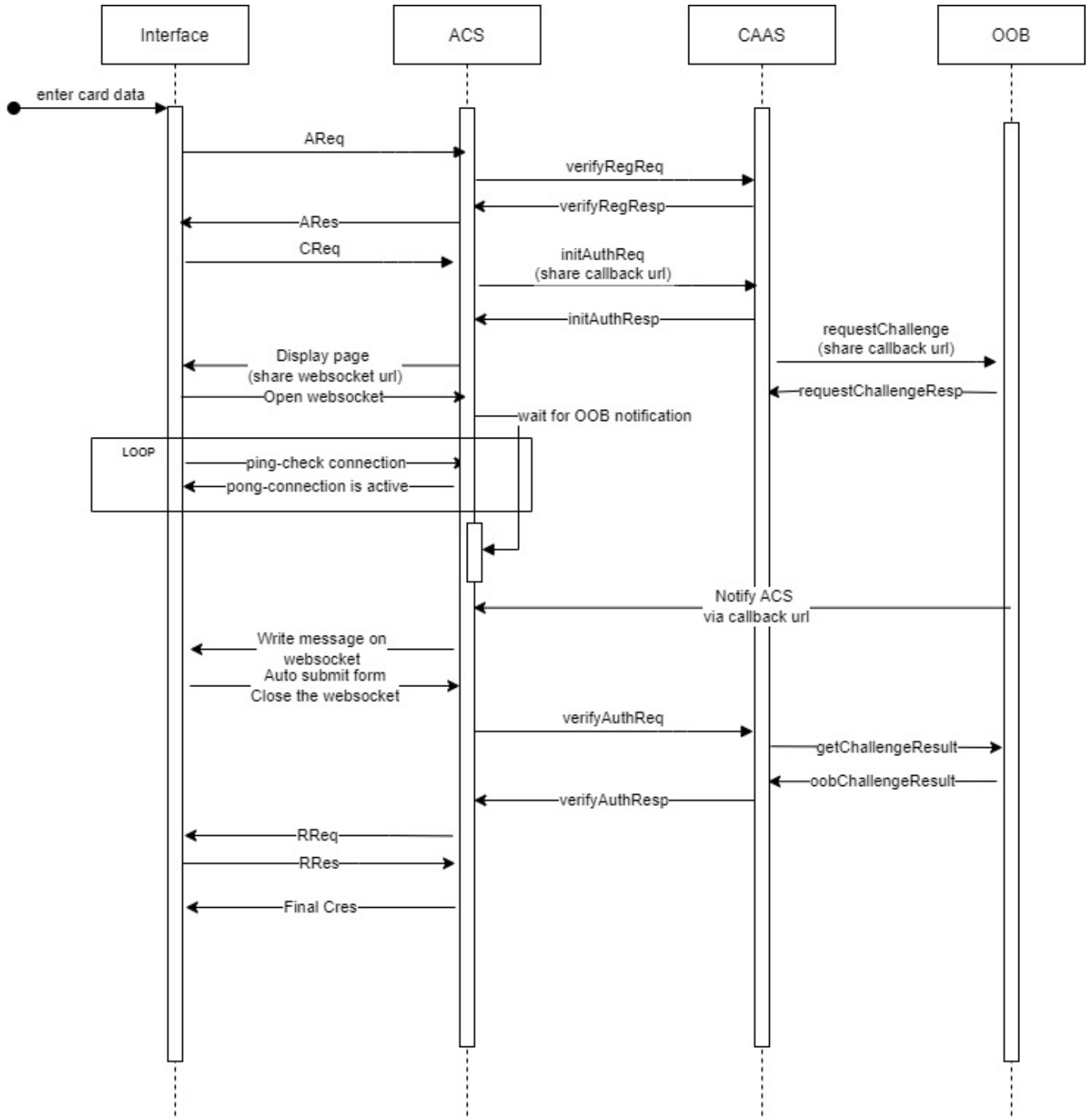
In the Standard OOB flow, these messages are triggered after the cardholder returns to the browser and submits the challenge page.

In the Alternative OOB flow, the ACS immediately finalises the transaction upon receiving the callback notification from the OOB application, without waiting for user interaction in the browser.

Both approaches maintain full EMV® 3DS compliance but offer flexibility in user experience — the Standard flow prioritises explicit user confirmation in the browser, while the Alternative flow provides a more seamless, fully asynchronous experience once the OOB authentication is complete.

The following diagrams provide an overview of the process for Standard Out-of-Band (OOB) Authentication:





When OOB is selected as the authentication method, the ACS generates a callback URL used to receive the finalisation notification of the OOB authentication from the OOB application. This URL is shared with the OOB adapter. In the case of remote authentication, it is the responsibility of the remote server (CAAS) to share this callback URL with the OOB component.

The ACS then serves the challenge page and establishes a WebSocket connection with the browser to enable real-time communication. To ensure the connection remains active, a ping–pong mechanism is implemented starting from ActiveAccess v9.4.0. Every 20 seconds, the

browser sends a ping message to the ACS, which responds with a pong message to keep the connection alive.

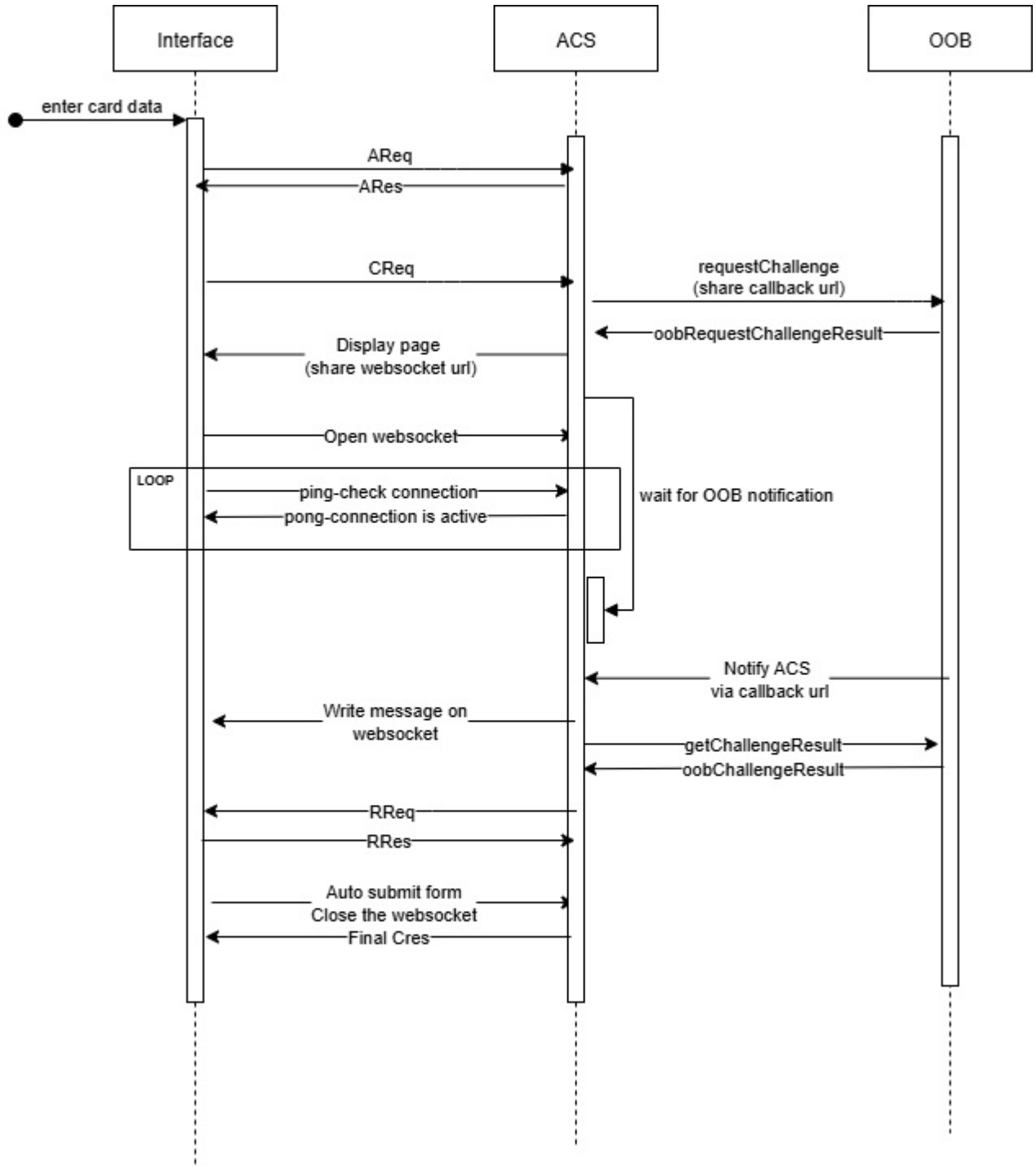
Once the OOB application completes the authentication, it sends a notification to the ACS through the callback URL. Upon receiving this notification, the ACS delivers a WebSocket message to the browser indicating that OOB authentication has been completed and that user action is now required to finalise the process.

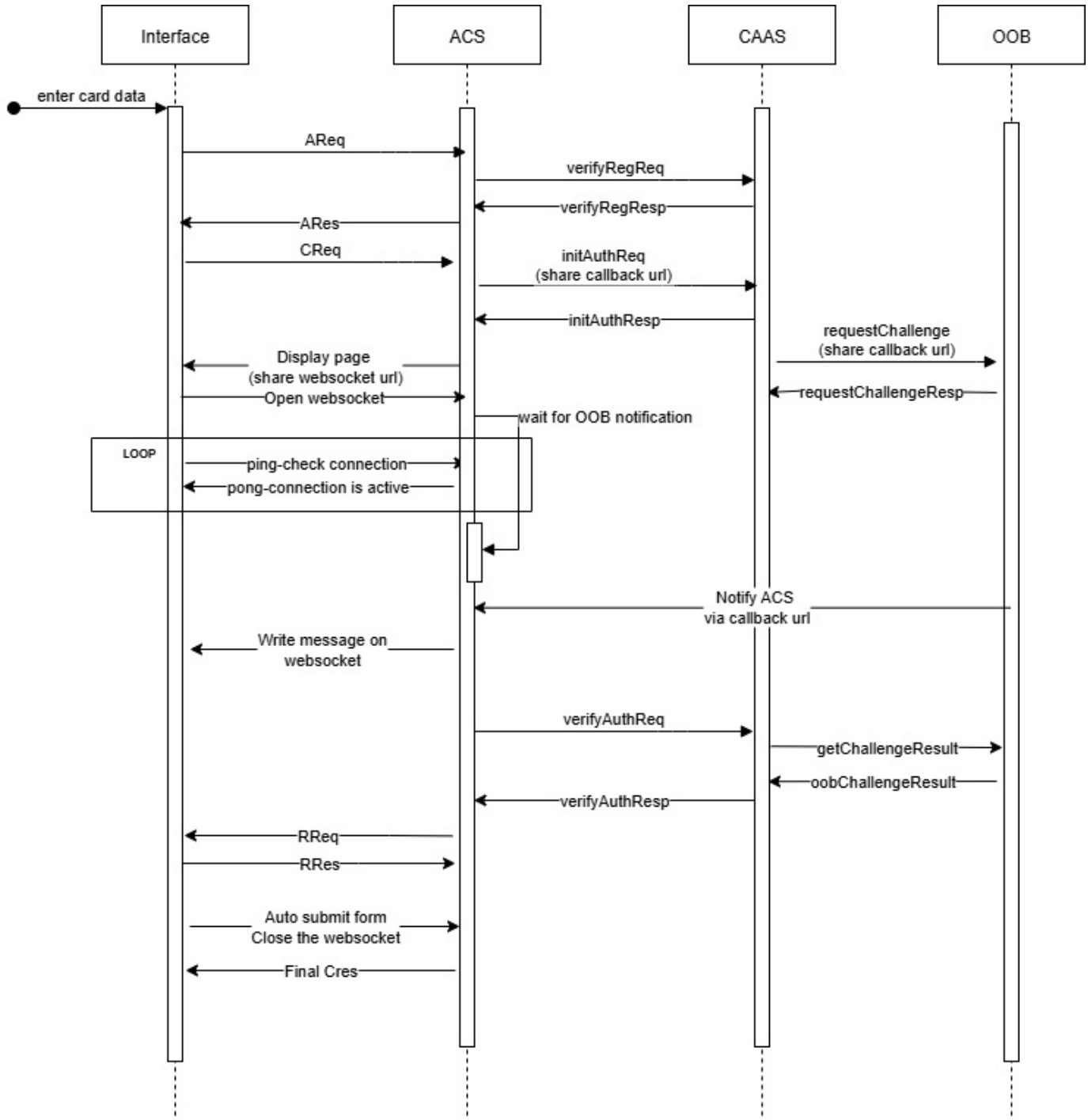
When the browser submits the challenge page, the ACS then prepares and sends the Result Request (RReq) message to the 3DS Server, followed by the final Challenge Response (CRes) message to complete the transaction.

> **Note**
>
> In this standard OOB flow, the RReq and final CRes processing are triggered by the browser submission. In contrast, in the Alternative OOB flow, these messages are generated immediately upon receiving the OOB callback notification, without waiting for the user to return to the browser or submit the page.

> **Note**
>
> The issuer can enable or disable WebSocket functionality on pages through the configuration option provided in the XSL file. WebSockets can also be optionally disabled for mobile browsers.

The following diagrams provide an overview of the process for Alternative Out-of-Band (OOB) Authentication:





When Out-of-Band (OOB) is selected as the authentication method, the Access Control Server (ACS) generates a callback URL used to receive the finalisation notification of the OOB authentication from the OOB application.This URL is shared with the OOB adapter. In the case of remote authentication, it is the responsibility of the remote server (CAAS) to share this callback URL with the OOB component.

After that, the ACS serves the challenge page and establishes a WebSocket connection with the browser to enable real-time communication. To ensure the connection remains active, the ping–

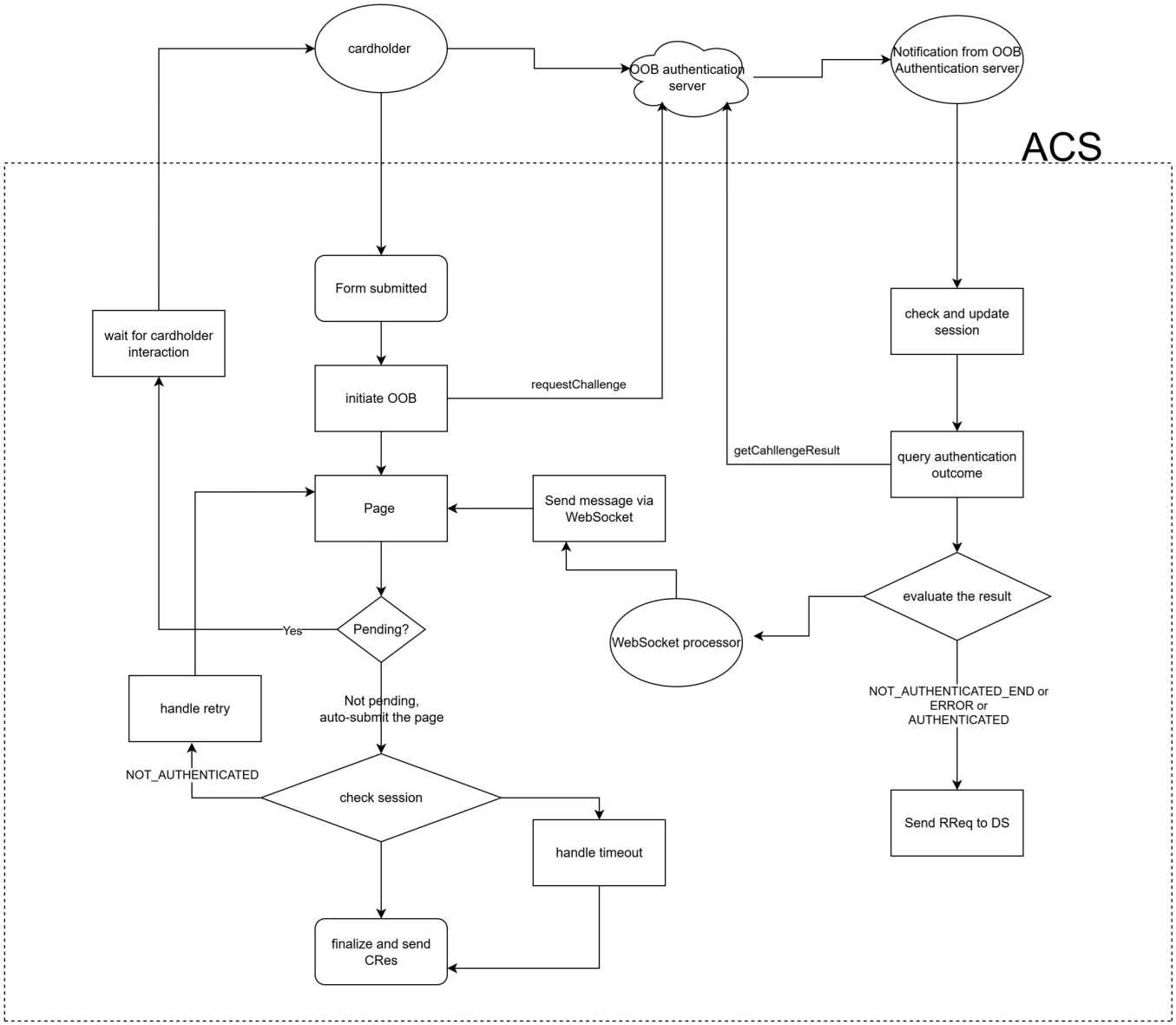
pong mechanism is used. Every 20 seconds, the browser sends a ping message to the ACS, which responds with a pong message to keep the connection alive.

Once the OOB application completes the authentication, it sends a notification to the ACS through the callback URL. Upon receiving this notification, the ACS retrieves the final OOB authentication result by querying the OOB server to confirm the outcome of the authentication process.

After confirming the result, the ACS: - Prepares and sends the Result Request (RReq) message to the 3DS Server, and - Simultaneously delivers a WebSocket notification to the browser to indicate that authentication has completed.

When the challenge page receives this WebSocket message, it automatically triggers the submission of page, thereby finalising the transaction by sending the final Challenge Response (CRes) message and closing the WebSocket connection.

The following diagram shows how cardholders interact with the system and how the ACS handles different authentication results:

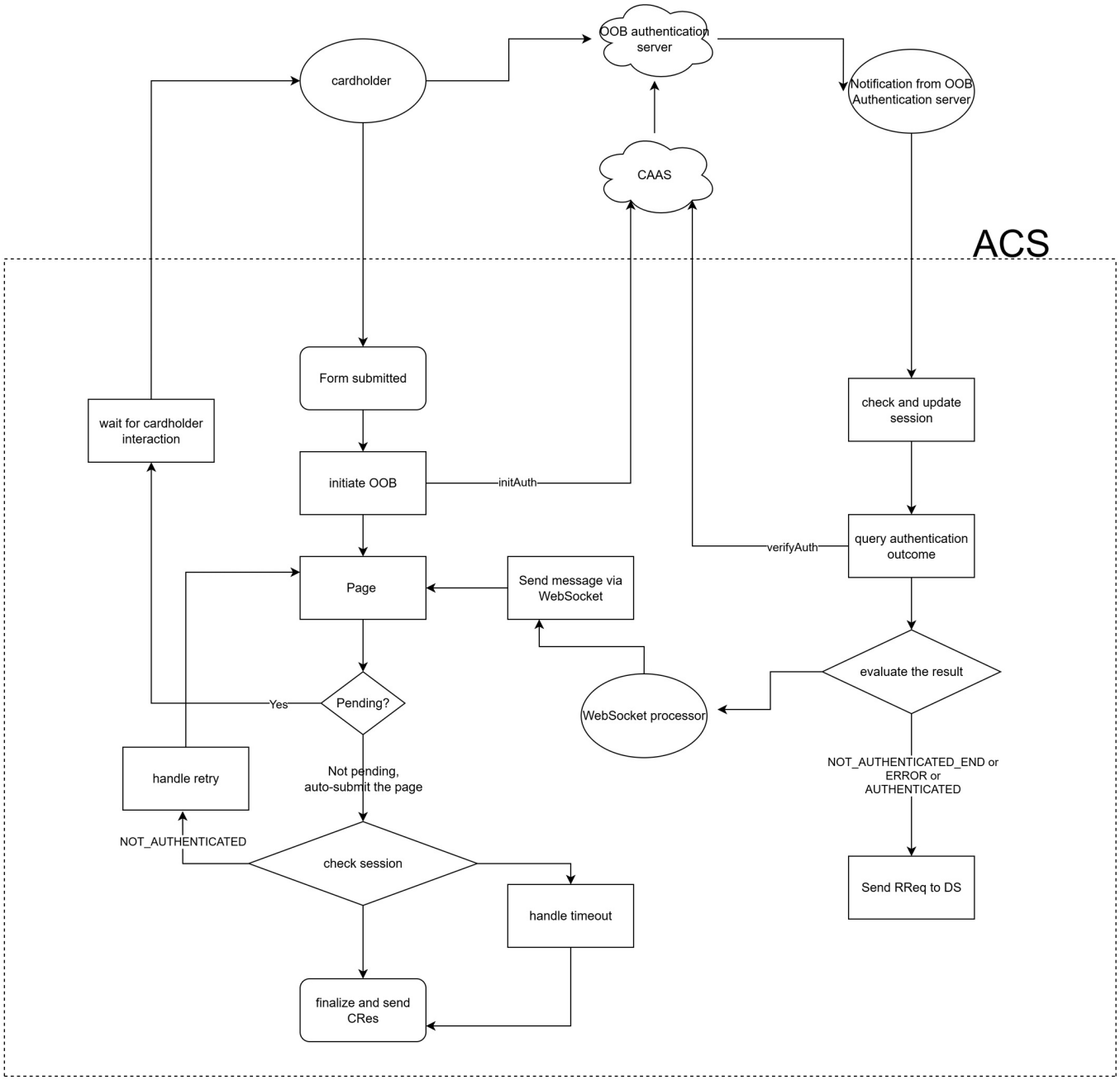


1. The cardholder initiates a transaction and is presented with the OOB authentication page.
2. The Access Control Server (ACS) connects to the issuer's OOB system to initiate authentication.
3. The cardholder completes authentication using the issuer's OOB application (e.g., mobile app or push notification).
4. After completion, the OOB system sends the result notification to the ACS.
5. The ACS processes the result as follows:
    - **AUTHENTICATED:** Updates session, sends RReq to the Directory Server (DS), auto-submits the challenge page via WebSocket, and sends the final CRes.

- **NOT_AUTHENTICATED:** Updates session, auto-submits via WebSocket, and displays a refreshed page with a clear message and guidance to retry authentication using the OOB application..
- **NOT_AUTHENTICATED_END:** Updates session, auto-submits via WebSocket, and sends final CRes to close the transaction.
- **ERROR:** Updates session, auto-submits via WebSocket, and sends final CRes for graceful termination.
- **PENDING:** Updates session, closes the WebSocket, and displays a “Continue” button. The ACS waits for user action before repeating the decision process and re-evaluating the result.

This flow enables secure, efficient authentication with minimal user disruption. Automated submission and structured retry handling ensure consistent user experience and data integrity.

For **Remote Authentication Issuers**, the following diagram illustrates the OOB authentication flow:



The ACS communicates with the OOB system via CAAS using asynchronous messaging. This flow highlights session updates, decision logic, and asynchronous result handling that maintain secure, efficient processing without requiring cardholder interaction on the ACS page.

Native API version of OOB Adapter

The Native API version of OOB Adapter is known as `oob.adapter` in this specification. The Native Adapters are provided in the form of `JAR` files, by GPayments or ActiveAccess clients. Only Java is supported for the Native API version of OOB Adapter.

Native OOB Adapter developers provide the adapters in one or more JAR files. The `oob.adapter` implementation in the adapter must implement the Java interface `Adapter` in the `com.gpayments.oob.api.v1` package.

Implementation Steps

The steps for implementing OOB Adapter are:

1. OOB Adapter developers create a Java project and obtain the corresponding Adapter API library from the ActiveAccess package. This library contains the interface definition for `oob.adapter` (Native OOB Adapter).
2. The Native API Adapter should be implemented as a Service based on the OOB interface `Adapter`. This specific implementation of the service known as *service provider*. `ACS` loads this class in startup and uses it in OOB Authentication. The requirement enforced by `ACS` is that *provider class* must have a public zero-argument constructor so that it can be instantiated during loading.
3. A service provider is identified by placing a *provider-configuration file* in the resource directory `META-INF/services`. The file's name is the fully-qualified binary name of the service's type, e.g. `com.gpayments.oob.api.v1.Adapter`. The file contains a list of fully-qualified binary names of concrete provider classes, one per line. Space and tab characters surrounding each name, as well as blank lines, are ignored. The comment character is '`#`' ('\u0023', NUMBER SIGN); on each line all characters following the first comment character are ignored. The file must be encoded in `UTF-8`.

Adapter Interface Methods

The `Adapter` interface has four methods as follows:

- **Method Name:** *`getAdapterInfo`*
  - **Description:** Returns information about `oob.adapter`
  - **Input:** This method takes no arguments
  - **Output:** An instance of `AdapterInfo` class that contains information about `oob.adapter` should be returned. The `AdapterInfo` is explained in detail in the AdapterInfo Data Elements section.
- **Method Name:** *`ping`*
  - **Description:** Checks whether OOB-Authenticator Server is accessible or not

- **Input:** This method takes no arguments
- **Output:** The result of *OOB Server* pinging should be returned in a *boolean* value. If the server responds to *ping* successfully, `true` should be returned, otherwise `false` should be returned.

- **Method Name:** *`requestChallenge`*
  - **Description:** To call when OOB authentication is necessary and returns whether authentication method for the card is available or not.
  - **Input:** This method takes the following parameters:
    - **Field Name:** `acsTransactionId`
      - **Description:** Universally Unique identifier assigned by the `ACS` to identify a single transaction
      - **Length:** 36 characters
      - **Format:** String
      - **Accepted Value:** Canonical format as defined in IETF RFC 4122
      - **Message Inclusion:** Required
    - **Field Name:** `transactionInfo`
      - **Description:** Information about the transaction, which is required for the OOB authentication
      - **Length:**
      - **Format:** An instance of type `TransactionInfo`. `TransactionInfo` is explained in detail in the TransactionInfo Data Elements section.
      - **Accepted Value:**
      - **Message Inclusion:** Required
  - **Output:** Adapter `requestChallenge` method has a `OobRequestChallengeResult` return type
    - **Field Name:** `oobRequestChallengeResult`
      - **Description:**
      - **Length:**
      - **Format:** An instance of type `OobRequestChallengeResult`. `OobRequestChallengeResult` is explained in details in the OobRequestChallengeResult Data Elements section.

        - **Accepted Value:**
        - **Message Inclusion:** Required

- **Method Name:** `getChallengeResult`
    - **Description:** Checks if the card is authenticated successfully or not
    - **Input:** This method takes the following parameters:
        - **Field Name:** `acsTransactionId`
            - **Description:** Universally Unique identifier assigned by the `ACS` to identify a single transaction.
            - **Length:** 36 characters
            - **Format:** String
            - **Accepted Value:** Canonical format as defined in IETF RFC 4122
            - **Message Inclusion:** Required
        - **Field Name:** `oobTransId`
            - **Description:** Unique identifier assigned by the `OOB-Authenticator-System` to identify a single OOB Authentication Challenge
            - **Length:** Variable, maximum 36 characters.
            - **Format:** String
            - **Accepted Value:**
            - **Message Inclusion:** Optional
        - **Field Name:** `additionalInfo`
            - **Description:** Some additional Information for OOB authentication
            - **Length:**
            - **Format:** JSON object of `AdditionalInfo` type. `AdditionalInfo` is explained in the AdditionalInfo Data Elements section.
            - **Accepted Value:**
            - **Message Inclusion:** Optional
    - **Output:** Adapter `getChallengeResult` method has a `OobAuthenticationResult` return type.
        - **Field Name:** `oobAuthenticationResult`
            - **Description:**

- **Length:**
- **Format:** An instance of type `OobAuthenticationResult`. `OobAuthenticationResult` is explained in details in the OobAuthenticationResult Data Elements section.
- **Accepted Value:**
- **Message Inclusion:** Required

- **Method Name:** *`getSwitchResponse`*
  - **Description:** Checks if the switch to fallback mechanism is approved by OOB-Authenticator-System
  - **Input:** This method takes the following parameters:
    - **Field Name:** `acsTransactionId`
      - **Description:** Universally unique identifier assigned by the `ACS` to identify a single transaction.
      - **Length:** 36 characters
      - **Format:** String
      - **Accepted Value:** Canonical format as defined in IETF RFC 4122
      - **Message Inclusion:** Required
    - **Field Name:** `oobTransId`
      - **Description:** Unique identifier assigned by the `OOB-Authenticator-System` to identify a single OOB Authentication Challenge
      - **Length:** Variable, maximum 36 characters.
      - **Format:** String
      - **Accepted Value:**
      - **Message Inclusion:** Optional
    - **Field Name:** `additionalInfo`
      - **Description:** Some additional Information for OOB authentication
      - **Length:**
      - **Format:** JSON object of `AdditionalInfo` type. `AdditionalInfo` is explained in the AdditionalInfo Data Elements section.
      - **Accepted Value:**

- **Message Inclusion:** Optional
- **Output:** Adapter `getSwitchResponse` method has a `OobSwitchResponseResult` return type.

- **Field Name:** `OobSwitchResponseResult`
  - **Description:**
  - **Length:**
  - **Format:** An instance of type `OobSwitchResponseResult`. `OobSwitchResponseResult` is explained in details in the OobSwitchResponseResult Data Elements section.
  - **Accepted Value:**
  - **Message Inclusion:** Required

- **Method Name:** *`getChallengeCancel`*
  - **Description:** Notifies the OOB-Authenticator-System about a challenge cancellation when switch button is clicked then cancel button is clicked.
  - **Input:** This method takes the following parameters:
    - **Field Name:** `acsTransactionId`
      - **Description:** Universally unique identifier assigned by the `ACS` to identify a single transaction.
      - **Length:** 36 characters.
      - **Format:** String.
      - **Accepted Value:** Canonical format as defined in IETF RFC 4122.
      - **Message Inclusion:** Required.
    - **Field Name:** `oobTransId`
      - **Description:** Unique identifier assigned by the `OOB-Authenticator-System` to identify a single OOB authentication challenge.
      - **Length:** Variable, maximum 36 characters.
      - **Format:** String.
      - **Accepted Value:**
      - **Message Inclusion:** Optional.

- **Output:** The result of the *OOB Server* `getChallengeCancel` method should be returned as a *boolean* value. If the server responds to `getChallengeCancel` successfully (200 OK), `true` should be returned; otherwise, `false` should be returned.

- **Method Name:** *`getChallengeTimeout`*
  - **Description:** Notifies the OOB-Authenticator-System about a challenge timeout when switch button is clicked then transaction expired.
  - **Input:** This method takes the following parameters:
    - **Field Name:** `acsTransactionId`
      - **Description:** Universally unique identifier assigned by the `ACS` to identify a single transaction.
      - **Length:** 36 characters.
      - **Format:** String.
      - **Accepted Value:** Canonical format as defined in IETF RFC 4122.
      - **Message Inclusion:** Required.
    - **Field Name:** `oobTransId`
      - **Description:** Unique identifier assigned by the `OOB-Authenticator-System` to identify a single OOB authentication challenge.
      - **Length:** Variable, maximum 36 characters.
      - **Format:** String.
      - **Accepted Value:**
      - **Message Inclusion:** Optional.
  - **Output:** The result of the *OOB Server* `getChallengeTimeout` method should be returned as a *boolean* value. If the server responds to `getChallengeTimeout` successfully (200 OK), `true` should be returned; otherwise, `false` should be returned.

RESTful API version of OOB Adapter

For the Restful API version of the `oob.adapter`, a Restful API needs to be defined similar to the adapter interface. `ACS` implements the Restful client and the `OOB Adapter API Server` will be implemented by the client. In this case, no JARs or plugins need to be loaded by `ACS`. Clients

must provide a specific URL for `ACS`. Known as `Adapter-URL` in this document and the required REST API endpoints are defined based on this URL.

> **Note**
>
> We also provide a Swagger API for the sample REST OOB Adapter server that is included in release package. To use it, run OOB Server in the installation package and then open `https://localhost:8447/swagger-ui.html#/` in your browser.

Get OOB Adapter Information

The ACS sends an HTTP request to get `oob.adapter` information. The details of this request are:

- **URL:** `Adapter-URL` /adapter-info
- **Request Method:** GET
- **Request Parameters:** there are not any request parameters for this REST API
- **Response:**
  - **Name:** adapterInfo
  - **Format:** JSON object of `AdapterInfo`.
  - **Description:** For further details on `AdapterInfo`, refer to the AdapterInfo Data Elements section.
  - **Inclusion:** Required

Sample request

```
HTTP URL: http://localhost:8447/restful-adapter/oob/adapter-info
```

Sample response

```
{
  "id": "0b99b82f-62cf-4275-88b3-de039020f14e",
  "name": "restful-adapter",
  "version": "1.6.0",
  "signature": "SIGNATURE"
}
```

Check OOB Authenticator Server availability status

The ACS sends an HTTP request to check whether OOB Authenticator Server is accessible or not. The details of this request are:

- **URL:** `Adapter-URL` /ping
- **Request Method:** GET
- **Request Parameters:** there are not any request parameters for this REST API
- **Response:** If Adapter Server is accessible to perform the OOB challenge process, this API returns an HTTP entity with 200 (OK) HTTP status code. Any other status codes such as 404 and 500 are considered as OOB Server unavailable.

Request OOB Challenge

ACS calls an HTTP API when OOB authentication is necessary and returns whether authentication method for the card is available or not.

- **URL:** `Adapter-URL` /request-challenge/{acsTransactionId}
- **Request Method:** POST
- **Path variables:**
  - **Name:** acsTransactionId
  - **Format:** String
  - **Inclusion:** required
- **Request Body:**
  - **Name:** transactionInfo
  - **Format:** JSON object of TransactionInfo type. For further details on TransactionInfo, refer to the TransactionInfo Data Elements section.
  - **Inclusion:** required
- **Response:**
  - **Name:** oobRequestChallengeResult
  - **Format:** JSON object of OobRequestChallengeResult.
  - **Description:** `OobRequestChallengeResult` is explained in details in the OobRequestChallengeResult Data Elements section.

- **Inclusion:** required

Sample Request

```
HTTP URL: http://localhost:8447/restful-adapter/oob/request-challenge/da3cb8f9-90a2-489b-a7af-28ba33ce924a

Body:
{
"acctNumber": "4548812049400004",
"additionalInfo": {
    "callbackUrl": "http://localhost:8080/acs/oobnotify/02/da3cb8f9-90a2-489b-a7af-28ba33ce924a",
    "clientId": "123456789012345",
    "deviceId": "123e4567-e89b-12d3-a456-426655440000"
},
"cardHolderInfo": {
    "cardholderName": "cardholderName",
    "email": "abc@example.com",
    "homePhone": {
        "cc": "61",
        "subscriber": "234567890"
    },
    "mobilePhone": {
        "cc": "61",
        "subscriber": "234567890"
    },
    "shipAddrCity": "shipAddrCity",
    "shipAddrCountry": "040",
    "shipAddrLine1": "shipAddrLine1",
    "shipAddrLine2": "shipAddrLine2",
    "shipAddrLine3": "shipAddrLine3",
    "shipAddrPostCode": "shipAddrPostCode",
    "shipAddrState": "VIC",
    "workPhone": {
        "cc": "61",
        "subscriber": "234567890"
    }
},
"deviceChannel": "01",
"issuerName": "AnyBank",
"last4Digits": "0004",
"merchantName": "merchantName",
"messageCategory": "01",
"purchaseAmount": "12345",
"purchaseCurrency": "036",
"purchaseDate": "20181223122338",
"purchaseExponent": "2",
"threeDSRequestorAppURL": "https://appName.com?transID=b2385523a66c-4907-ac3c91848e8c0067",
"threeDSRequestorAuthenticationInd": "01",
"threeDSServerTransID": "a4edc97f-4b89-4e52-8590-6c328f0b9648"
}
```

Sample response


```
{
    "requestChallengeEnum": "OK",
    "oobTransId": "0679cb73-ea9a-41fb-8fda-dec78a46cd0b",
    "message": "message example",
    "authenticationMethod": "07",
    "instruction": "Verify your purchase in 2 steps\n\n1.Open YourBank app on your mobile to
verify.\n\n2.Return to merchant and tap complete.",
    "appURL":"https://oobapp.com/here"
}
```


Get OOB authentication result

`ACS` calls an HTTP API to check if the cardholder is authenticated successfully or not. The details of this REST API are:

- **URL:** `Adapter-URL` /challenge-result/{acsTransactionId}/{oobTransId} (or `Adapter-URL` / challenge-result/{acsTransactionId} if `oobTransId` is null.)
- **Request Method:** POST
- **Path variables:**
  - **Name:** acsTransactionId
  - **Format:** String
  - **Inclusion:** Required
  - **Name:** oobTransId
  - **Format:** String
  - **Inclusion:** Optional
- **Request Body:**
  - **Name:** additionalInfo
  - **Format:** JSON object of `AdditionalInfo` type. You can find details of `AdditionalInfo` in the AdditionalInfo Data Elements section.
- **Response:**
  - **Name:** oobAuthenticationResult
  - **Format:** JSON object of type `OobAuthenticationResult`

- **Description:** `OobAuthenticationResult` is explained in details in the OobAuthenticationResult Data Elements section.
- **Inclusion:** Required

Sample Request

```
    HTTP URL: http://localhost:8447/restful-adapter/oob/challenge-result/da3cb8f9-90a2-489b-a7af-28ba33ce924a

Body:
{
    "callbackUrl": "http://localhost:8080/acs/oobnotify/02/da3cb8f9-90a2-489b-a7af-28ba33ce924a",
    "clientId": "123456789012345",
    "deviceId": "123e4567-e89b-12d3-a456-426655440000"
}
```

Sample response

```
    {
     "authenticationMethod": "07",
    "authenticationResultEnum": "AUTHENTICATED",
    "instruction": "instruction example",
    "message": "message example"
    }
```

Get OOB switch result

The `ACS` calls an HTTP API to check if the cardholder is allowed to switch to fallback mechanism. The details of this REST API are:

- **URL:** `Adapter-URL` /switch-result/{acsTransactionId}/{oobTransId} (or `Adapter-URL` /switch-result/{acsTransactionId} if `oobTransId` is null.)
- **Request Method:** POST
- **Path variables:**
  - **Name:** acsTransactionId
  - **Format:** String
  - **Inclusion:** Required
  - **Name:** oobTransId

- **Format:** String
- **Inclusion:** Optional

- **Request Body:**
  - **Name:** additionalInfo
  - **Format:** JSON object of `AdditionalInfo` type. You can find details of `AdditionalInfo` in the AdditionalInfo Data Elements section.
- **Response:**
  - **Name:** OobSwitchResponseResult
  - **Format:** JSON object of type `OobSwitchResponseResult`
  - **Description:** `OobSwitchResponseResult` is explained in details in the OobSwitchResponseResult Data Elements section.
  - **Inclusion:** Required

Sample request

```
HTTP URL: http://localhost:8447/restful-adapter/oob/switch-result/da3cb8f9-90a2-489b-
a7af-28ba33ce924a

Body:
{
    "callbackUrl": "http://localhost:8080/acs/oobnotify/02/da3cb8f9-90a2-489b-
a7af-28ba33ce924a",
    "clientId": "123456789012345",
    "deviceId": "123e4567-e89b-12d3-a456-426655440000"
}
```

Sample response

```
Body:
{
    "switchResponseEnum": "SWITCH_APPROVED",
    "message": null,
    "oobTransId": null
}
```

Notify OOB Challenge Cancel

The ACS sends an HTTP request to notify the OOB Authenticator Server about a challenge cancellation. The details of this request are as follows:

- **URL:** `Adapter-URL` /challenge-cancel/{acsTransactionId}/{oobTransId} (or `Adapter-URL` / challenge-cancel/{acsTransactionId} if `oobTransId` is null.)
- **Request Method:** GET
- **Path Variables:**
  - **Name:** `acsTransactionId`
  - **Format:** String
  - **Inclusion:** Required
  - **Name:** `oobTransId`
  - **Format:** String
  - **Inclusion:** Optional
- **Request Parameters:** There are no request parameters for this REST API.
- **Response:** If the Adapter Server successfully processes the `getChallengeCancel` request, this API returns an HTTP entity with a `200 (OK)` status code.

Notify OOB Challenge Timeout

The ACS sends an HTTP request to notify the OOB Authenticator Server about a challenge timeout. The details of this request are as follows:

- **URL:** `Adapter-URL` /challenge-timeout/{acsTransactionId}/{oobTransId} (or `Adapter-URL` / challenge-timeout/{acsTransactionId} if `oobTransId` is null.)
- **Request Method:** GET
- **Path Variables:**
  - **Name:** `acsTransactionId`
  - **Format:** String
  - **Inclusion:** Required
  - **Name:** `oobTransId`

- **Format:** String
- **Inclusion:** Optional

- **Request Parameters:** There are no request parameters for this REST API.
- **Response:** If the Adapter Server successfully processes the `getChallengeTimeout` request, this API returns an HTTP entity with a `200 (OK)` status code.

Authentication mechanism for the RESTful API version

Certificate based mutual authentication is used as the authentication mechanism for the RESTful API version. The steps are:

- `ACS` publishes a CA for adapter communication, known as `Adapter CA`
- `ACS` also issues a server certificate for the adapter.
- `ACS` uses a generated client certificate that is issued by the same `Adapter CA`.
- The Adapter server implementation must be set up with the CA and mutual authentication provided.
- `ACS` will try to connect to the Adapter Server and if the connection can be established then `ACS` will continue with the adapter, otherwise it throws an error.

Adapter Data Elements

AdapterInfo Data Elements

- **Field Name:** `id`
  - **Description:** The `ACS` assigned *UUID* to the `OOB Adapter`
  - **Length:** 36 characters
  - **Format:** String
  - **Accepted Value:** Canonical format as defined in IETF RFC 4122
  - **Message Inclusion:** Required
- **Field Name:** `name`
  - **Description:** The `ACS` assigned *name* to the `OOB Adapter`
  - **Length:** Variable, maximum 100 characters

- **Format:** String
- **Accepted Value:**
- **Message Inclusion:** Required

- **Field Name:** `version`
  - **Description:** The number that sets the version of the used `OOB Adapter` API.
  - **Length:** Variable
  - **Format:** String
  - **Accepted Value:** Supported versions can be found in Current Supported Versions section.
  - **Message Inclusion:** Required
- **Field Name:** `signature`

> **Note**
>
> This field is not currently used and is reserved for for future versions.

  - **Description:** Signature to validate `OOB Adapter` integrity
  - **Length:** Variable
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional

TransactionInfo Data Elements

- **Field Name**: `threeDSServerTransID`
  - **Description:** Universally unique transaction identifier assigned by the 3DS Server to identify a single transaction.
  - **Length:** 36 characters
  - **Format:** String
  - **Accepted Value:** Canonical format as defined in IETF RFC 4122. May utilise any of the specified versions if the output meets specified requirements.

- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Required

- **Field Name:** `additionalInfo`
  - **Description:** Some additional Info for OOB authentication
  - **Length:**
  - **Format:** JSON object of `AdditionalInfo` type. `AdditionalInfo` is explained in the AdditionalInfo Data Elements section.
  - **Accepted Value:**
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Optional
- **Field Name**: `purchaseAmount`
  - **Description:** Purchase amount in minor units of currency with all punctuation removed. When used in conjunction with the Purchase Currency Exponent field, proper punctuation can be calculated.
  - **Length:** 48 characters
  - **Format:** String
  - **Accepted Value:** Example: If the purchase amount is USD 123.45, element will contain the value 12345.
  - **Device Channel:** 01-APP, 02-BRW
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** 01-PA: Required, 02-NPA: Conditional
  - **Conditional Inclusion:** Required for 02NPA if 3DS Requestor Authentication Indicator = 02 or 03.
- **Field Name**: `purchaseCurrency`
  - **Description:** Currency in which purchase amount is expressed.
  - **Length:** 3 characters
  - **Format:** String

- **Accepted Value:** ISO 4217 three-digit currency code; 955-964 and 999 values are excluded and not permitted.
- **Device Channel:** 01-APP, 02-BRW
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** 01-PA: Required, 02-NPA: Conditional
- **Conditional Inclusion:** Required for 02NPA if 3DS Requestor Authentication Indicator = 02 or 03.

- **Field Name**: `purchaseExponent`
  - **Description:** Minor units of currency as specified in the ISO 4217 currency exponent.
  - **Length:** 1 character
  - **Format:** String
  - **Accepted Value:** Number
  - **Device Channel:** 01-APP, 02-BRW
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** 01-PA: Required, 02-NPA: Conditional
  - **Conditional Inclusion:** Required for 02NPA if 3DS Requestor Authentication Indicator = 02 or 03.
- **Field Name**: `messageCategory`
  - **Description:** Identifies the category of the message for a specific use case
  - **Length:** 2 characters
  - **Format:** String
  - **Accepted Value:** 01-PA, 02-NPA
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Required
- **Field Name**: `purchaseDate`
  - **Description:** Date and time of the purchase, expressed in UTC timezone.
  - **Length:** 14 characters
  - **Format:** String (Date Format: YYYYMMDDHHMMSS)

- **Accepted Value:**
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** 1-PA: Required, 02-NPA: Conditional
- **Conditional Inclusion:** Conditional (Required if purchaseAmount is set)

• **Field Name**: `deviceChannel`

- **Description:** Indicates the type of channel interface being used to initiate the transaction.
- **Length:** 2 characters
- **Format:** String
- **Accepted Value:** 01 (APP); 02 (BRW); 03 (3RI)
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Required

• **Field Name**: `acctNumber`

- **Description:** Account number that will be used in the authorisation request for payment transactions. It will be represented by PAN, token. This field can be raw, hashed, encrypted, or empty.
- **Length:** 13-19 characters, or up to 72 characters when encryption for sensitive data is enabled
- **Format:** String
- **Accepted Value:** Format represented ISO 7812.
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Optional

• **Field Name**: `merchantName`

- **Description:** Merchant name assigned by the Acquirer or Payment System.
- **Length:** Variable, maximum 40 characters
- **Format:** String
- **Accepted Value:** Same name used in the authorisation message as defined in ISO 8583.

- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** 01-PA: Required, 02-NPA: Optional
- **Conditional Inclusion:** Optional but strongly recommended to include for 02NPA if the merchant is also the 3DS Requestor.

- **Field Name**: `cardHolderInfo`
  - **Description:** Information about the Cardholder, which is provided by the 3DS Requestor. For further details, refer to the CardHolderInfo Data Elements section
  - **Type:** CardHolderInfo
- **Field Name**: `issuerName`
  - **Description:** Name of the Issuer
  - **Length:** Variable, maximum 64 characters.
  - **Format:** String
  - **Accepted Value:** Any.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Required
- **Field Name**: `threeDSRequestorAppURL`
  - **Description:** 3DS Requestor App declaring their URL within the CReq message so that the Authentication app can call the 3DS Requestor App after OOB authentication has occurred. Each transaction would require a unique Transaction ID by using the SDK Transaction ID.
  - **Length:** Variable, maximum 256 characters
  - **Format:** String
  - **Accepted Value:** Fully qualified URL
  - **Message Inclusion:** Optional
- **Field Name**: `threeDSRequestorAuthenticationInd`
  - **Description:** Indicates the type of Authentication request. This data element provides additional information to the ACS to determine the best approach for handling an authentication request.

- **Length:** 2 characters
- **Format:** String
- **Accepted Value:** 01-Payment transaction, 02-Recurring transaction, 03-Instalment transaction, 04-Add card, 05-Maintain card, 06-Cardholder verification as part of EMV token ID & V
- **Message Inclusion:** Optional

- **Field Name**: `last4Digits`
  - **Description:** Last four digits of the account number that will be used in the authorisation request for payment transactions.
  - **Length:** 4 characters
  - **Format:** String
  - **Message Inclusion:** Required

AdditionalInfo Data Elements

- **Field Name:** `clientId`
  - **Description:** Client ID
  - **Length:** 15 characters
  - **Format:** String
  - **Accepted Value:** Decimal numbers
  - **Message Inclusion:** Optional (this field will be excluded from RESTful JSON message when it has no value)
- **Field Name:** `deviceId`
  - **Description:** Device ID
  - **Length:** Variable, maximum 36 characters
  - **Format:** String
  - **Accepted Value:** Any
  - **Message Inclusion:** Optional (this field will be excluded from RESTful JSON message when it has no value)

- **Field Name:** `callbackUrl`
  - **Description:** URL to be called by `OOB system` when OOB authentication result is prepared. ACS will call `getChallengeResult` after receiving this request.
  - **Length:** Variable, maximum 2048 characters
  - **Format:** String
  - **Accepted Value:** Fully qualified URL
  - **Message Inclusion:** Required
  - **URL:** `http(s)://{$acsDomain}/acs/oobnotify/`

CardHolderInfo Data Elements

- **Field Name**: `cardholderName`
  - **Description:** Cardholder name
  - **Length:** 2-45 characters or up to 104 characters when encryption for sensitive data is enabled
  - **Format:** String
  - **Accepted Value:** Alphanumeric special characters, listed in EMVBook 4, “Appendix B”.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Conditional
  - **Conditional Inclusion:** Required unless market or regional mandate restricts sending this information.
- **Field Name**: `email`
  - **Description:** The email address associated with the account that is either entered by the Cardholder, or is on file with the 3DS Requestor.
  - **Length:** 254 characters
  - **Format:** String
  - **Accepted Value:** Shall meet requirements of Section 3.4 of IETF RFC 5322.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Conditional

- **Conditional Inclusion:** Required unless market or regional mandate restricts sending this information.

- **Field Name**: `homePhone`
  - **Description:** The home phone number provided by the Cardholder. For further details, refer to the HomePhone Data Elements section
  - **Type:** HomePhone
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Conditional
  - **Conditional Inclusion:** Required unless market or regional mandate restricts sending this information.
- **Field Name**: `mobilePhone`
  - **Description:** The mobile phone number provided by the Cardholder. For further details, refer to the MobilePhone Data Elements section
  - **Type:** MobilePhone
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Conditional
  - **Conditional Inclusion:** Required unless market or regional mandate restricts sending this information.
- **Field Name**: `shipAddrCity`
  - **Description:** City portion of the shipping address requested by the Cardholder
  - **Length:** Variable, maximum 50 characters
  - **Format:** String
  - **Accepted Value:**
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Optional
- **Field Name**: `shipAddrCountry`
  - **Description:** Country of the shipping address requested by the Cardholder.

- **Length:** 3 characters
- **Format:** String
- **Accepted Value:** ISO 3166-1 three-digit country code; 901-999 values are excluded and not permitted.
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Optional

• **Field Name**: `shipAddrLine1`

- **Description:** First line of the street address or equivalent local portion of the shipping address requested by the Cardholder.
- **Length:** Variable, maximum 50 characters
- **Format:** String
- **Accepted Value:**
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Optional

• **Field Name**: `shipAddrLine2`

- **Description:** Second line of the street address or equivalent local portion of the shipping address requested by the Cardholder.
- **Length:** Variable, maximum 50 characters
- **Format:** String
- **Accepted Value:**
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Optional

• **Field Name**: `shipAddrLine3`

- **Description:** Third line of the street address or equivalent local portion of the shipping address requested by the Cardholder.
- **Length:** Variable, maximum 50 characters
- **Format:** String

- **Accepted Value:**
- **Device Channel:** 01-APP, 02-BRW, 03-3RI
- **Message Category:** 01-PA, 02-NPA
- **Message Inclusion:** Optional

- **Field Name**: `shipAddrPostCode`
  - **Description:** The ZIP or other postal code of the shipping address requested by the Cardholder
  - **Length:** Variable, maximum 16 characters
  - **Format:** String
  - **Accepted Value:**
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Optional
- **Field Name**: `shipAddrState`
  - **Description:** The state or province of the shipping address associated with the card being used for this purchase.
  - **Length:** Variable, maximum 3 characters
  - **Format:** String
  - **Accepted Value:** Should be the country subdivision code defined in ISO 3166-2.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Optional
- **Field Name**: `workPhone`
  - **Description:** The work phone number provided by the Cardholder. For further details, refer to the WorkPhone Data Elements section
  - **Type:** WorkPhone
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
  - **Message Inclusion:** Conditional

- **Conditional Inclusion:** Required (if available) unless market or regional mandate restricts sending this information.

HomePhone Data Elements

- **Field Name**: `cc`
  - **Description:** Country Code of the number
  - **Length:** 1-3 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
- **Field Name**: `subscriber`
  - **Description:** Subscriber sections of the number
  - **Length:** Variable, maximum 15 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA

MobilePhone Data Elements

- **Field Name**: `cc`
  - **Description:** Country Code of the number
  - **Length:** 1-3 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA

- **Field Name**: `subscriber`
  - **Description:** Subscriber sections of the number
  - **Length:** Variable, maximum 15 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA

WorkPhone Data Elements

- **Field Name**: `cc`
  - **Description:** Country Code of the number
  - **Length:** 1-3 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA
- **Field Name**: `subscriber`
  - **Description:** Subscriber sections of the number
  - **Length:** Variable, maximum 15 characters
  - **Format:** String
  - **Accepted Value:** Refer to ITU-E.164 for additional information on format and length.
  - **Device Channel:** 01-APP, 02-BRW, 03-3RI
  - **Message Category:** 01-PA, 02-NPA

OobRequestChallengeResult Data Elements

- **Field Name**: `requestChallengeEnum`
  - **Description:** Result of requesting OOB authentication challenge to `OOB-Authenticator-System`, that determines whether OOB authentication method is available for this card or not.
  - **Length:**
  - **Format:**
  - **Accepted Value:** OK, ERROR
  - **Accepted Value:**
  - **Message Inclusion:** Required
- **Field Name:** `oobTransId`
  - **Description:** Unique identifier assigned by the `OOB-Authenticator-System` to identify a single OOB Authentication Challenge.
  - **Length:** Variable, maximum 36 characters
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional
- **Field Name**: `message`
  - **Description:** Any required message that should be returned to the `ACS`
  - **Length:** Variable, maximum 500 characters
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional
- **Field Name**: `instruction`
  - **Description:** Cardholder instructions on how to perform the OOB authentication
  - **Length:** Variable, maximum 350 characters
  - **Format:** String
  - **Accepted Value:** Any
  - **Message Inclusion:** Optional

- **Field Name**: `authenticationMethod`
  - **Description:** OOB authentication approach used to authenticate the cardholder.
  - **Length:** 2 characters.
  - **Format:** String
  - **Accepted Value:** 07-OOB Biometrics, 08-OOB Login, 09-OOB other, 11-Push confirmation
  - **Message Inclusion:** Optional

OobSwitchResponseResult Data Elements

- **Field Name**: `switchResponseEnum`
  - **Description:** Result of switch request
  - **Length:**
  - **Format:**
  - **Accepted Value:** SWITCH_APPROVED, SWITCH_REJECTED, DECLINE_TRANSACTION, ERROR
  - **Message Inclusion:** Required
- **Field Name**: `message`
  - **Description:** Any required message that should be returned to the `ACS`
  - **Length:** Variable, maximum 500 characters
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional
- **Field Name**: `oobTransId`
  - **Description:** Unique identifier assigned by the OOB-Authenticator-System to identify a single OOB Authentication Challenge.
  - **Length:** Variable, maximum 36 characters.
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional

- **Field Name**: `appUrl`
  - **Description:** Universal App Link to an Authentication App used in the OOB authentication. The OOB App URL will open the appropriate location within the OOB Authentication App.
  - **Length:** 256 characters.
  - **Format:** String
  - **Accepted Value:** Fully Qualified URL
  - **Message Inclusion:** Optional

OobAuthenticationResult Data Elements

- **Field Name**: `authenticationResultEnum`
  - **Description:** Result of OOB authentication challenge
  - **Length:**
  - **Format:**
  - **Accepted Value:** AUTHENTICATED, NOT_AUTHENTICATED, NOT_AUTHENTICATED_END, ERROR, PENDING
  - **Message Inclusion:** Required
- **Field Name**: `message`
  - **Description:** Any required message that should be returned to the `ACS`
  - **Length:** Variable, maximum 500 characters
  - **Format:** String
  - **Accepted Value:**
  - **Message Inclusion:** Optional
- **Field Name**: `instruction`
  - **Description:** Cardholder instructions on how to perform the OOB authentication
  - **Length:** Variable, maximum 350 characters
  - **Format:** String
  - **Accepted Value:** Any
  - **Message Inclusion:** Optional

- **Field Name**: `authenticationMethod`
  - **Description:** OOB authentication approach that is used to authenticate the cardholder.
  - **Length:** 2 characters.
  - **Format:** String
  - **Accepted Value:** 07-OOB Biometrics, 08-OOB Login, 09-OOB other, 11-Push confirmation
  - **Message Inclusion:** Optional

Current Supported Versions

OOB Adapter version	Minimum required version of ACS	Made changes
1	8.0.0	Initial version of OOB Adapter is released
1.1	8.1.0	Interactive API documentation is generated using Swagger Values of RequestChallengeResultEnum is converted to uppercase Values of AuthenticationResultEnum is converted to uppercase PENDING is added to the AuthenticationResultEnum values
1.2	8.2.0	additionalInfo field is added to the TransactionInfo additionalInfo is added to getChallengeResult method parameters
1.3	8.2.1	API documentation is updated
1.4.0	8.4.0	purchaseDate field is added to the TransactionInfo
1.5.0	8.5.0	NOT_AUTHENTICATED_END value is added to the AuthenticationResultEnum
1.6.0	9.0.0	threeDSRequestorAppURL field is added to the TransactionInfo callbackUrl field is added to the AdditionalInfo instruction field is added to the OobAuthenticationResult instruction field is added to the OobRequestChallengeResult

OOB Adapter version	Minimum required version of ACS	Made changes
1.7.0	9.1.0	authenticationMethod field is added to the OobAuthenticationResult authenticationMethod field is added to the OobRequestChallengeResult threeDSRequestorAuthenticationInd field is added to the TransactionInfo last4Digits field is added to the TransactionInfo