Oberbank
3 Banken Gruppe

Description xs2a Fallback

A TPP can recognize that something went wrong with the xs2a-server or its essential external sources like DB or bank backend when it receives one of 5xx HTTP status codes back on its 5 consecutive requests for access to information for provision of payment initiation services or account information services within a total timeframe of 30 seconds.

Here is the list of 5xx HTTP status codes:

HTTP 500 Internal Server Error
HTTP 501 Not Implemented
HTTP 502 Bad Gateway
HTTP 503 Service Unavailable
HTTP 504 Gateway Timeout
HTTP 505 HTTP Version Not Supported
HTTP 506 Variant Also Negotiates
HTTP 507 Insufficient Storage
HTTP 508 Loop Detected
HTTP 510 Not Extended
HTTP 511 Network Authentication Required
HTTP 599 Network Connect Timeout Error

In this case a TPP may use the fallback mechanism which is in our case is the certificate-checker under the URL xs2a-fallback.banking-oberbank.at/certificate-checker/cc. A TPP must send a request using HTTP method = GET. A TPP must provide its valid production QWAC when calling this URL.

When QWAC validation has been completed successfully, a TPP will be redirected to the Oberbank Kundenportal and can access necessary information by using web-scraping.

When QWAC validation has failed, a TPP might receive one of the following errors in the response

Case 1. Call without certificate
HTTP 403 Forbidden
{ "timestamp": "2019-09-03T09:03:12.699+0000", "status": 403, "error": "Forbidden", "message": "Access Denied", "path": "/certificate-checker/cc" }

Case 2. certificate without PSD2 extention
HTTP 403 Forbidden
{ "errorMessage": "Certificate doesn't have qcExtensions section" }

Case 3. certificate status = revoked
HTTP 403 Forbidden
{ "certificateStatus": "REVOKED" }

Case 4. certificate status = unknown
HTTP 403 Forbidden { "certificateStatus": "UNKNOWN" }

Oberbank
3 Banken Gruppe

Beschreibung xs2a Fallback

Wenn es Probleme am xs2a-Server gibt oder die geforderten 5 Anfragen betreffend

- access to information for provision of payment initiation services
- account information services

innerhalb eines Zeitfensters von 30 Sekunden nicht beantwortet werden können, dann wird einer der folgenden 5xx Status codes geliefert:

HTTP 500 Internal Server Error
HTTP 501 Not Implemented
HTTP 502 Bad Gateway
HTTP 503 Service Unavailable
HTTP 504 Gateway Timeout
HTTP 505 HTTP Version Not Supported
HTTP 506 Variant Also Negotiates
HTTP 507 Insufficient Storage
HTTP 508 Loop Detected
HTTP 510 Not Extended
HTTP 511 Network Authentication Required
HTTP 599 Network Connect Timeout Error

Das berechtigt den TPP den Fallbackweg zu wählen:

- Der TPP muss eine HTTP-Anfrage mit der GET-Methode absetzen
- Der TPP muss eine gültige produktive QWAC mitsenden

Aufruf: xs2a-fallback.banking-oberbank.at/certificate-checker/cc

Wenn kein QWAC Zertifkat mitgegeben wird oder die QWAC-Prüfung fehlschlägt, gibt es folgende Fehlermeldungen

Call without certificate
HTTP 403 Forbidden { "timestamp": "2019-09-03T09:03:12.699+0000", "status": 403, "error": "Forbidden", "message": "Access Denied", "path": "/certificate-checker/cc" }

certificate without PSD2 extention
HTTP 403 Forbidden { "errorMessage": "Certificate doesn't have qcExtensions section" }

certificate status = revoked
HTTP 403 Forbidden { "certificateStatus": "REVOKED" }

certificate status = unknown
HTTP 403 Forbidden { "certificateStatus": "UNKNOWN" }

Wenn der Aufruf **erfolgreich** war, erfolgt ein Redirect auf die Login-Seite des Oberbank Kundenportals. Dabei werden die Informationen aus dem Zertifikat an die Login-Seite übergeben.