

Third-Party Integration REST API Specification

Overview

This document specifies the REST API that third-party service vendors must implement to integrate with the Assessio Bloom Platform (ABP). It covers authentication, endpoints, flows, security, and response formats.

Basic Flow Summary

1. User starts the third-party service from ABP
2. ABP creates a session at the vendor (back-channel)
3. ABP starts the session and receives a one-time launch URL (back-channel)
4. User's browser is redirected to the launch URL (front-channel)
5. User completes the service in the vendor's UI
6. Vendor redirects user back to ABP with a signed return URL
7. ABP verifies completion back-channel and fetches results
8. User sees results in ABP

Configuration (One-Time per Vendor)

ABP stores the following per vendor integration:

Setting	Description	Example
'baseUrl'	Vendor's API base URL	'https://vendor.example.com'
'sharedSecret'	HMAC-SHA256 shared secret (256-bit minimum)	'a3f8c9...'
'callbackUrl'	ABP webhook endpoint (static per vendor)	'https://assessiobloom.online/applink/api/integrations/{vendorId}/webhook'
'returnUrl'	ABP return endpoint (static per vendor)	'https://assessiobloom.online/applink/api/integrations/{vendorId}/return'

Future API versions will be released, providing vendors with a designated transition period to update their integrations.

Authentication

All back-channel API calls are authenticated using HMAC-SHA256 request signing.

Request Signing

Every request from ABP includes:

Headers:

- X-Timestamp: 1716820000 (Unix epoch seconds)
- X-Signature: <HMAC-SHA256 signature>

Signature computation:

```
signature = HMAC-SHA256(  
  key: shared_secret,  
  message: "{METHOD}\n{PATH}\n{TIMESTAMP}\n{BODY}"  
)
```

- 'METHOD': HTTP method (uppercase: 'GET', 'POST')
- 'PATH': Request path including query string (e.g. '/api/sessions/abc123/results?language=en-UK')
- 'TIMESTAMP': Value of 'X-Timestamp' header
- 'BODY': Request body (empty string for GET requests)

Vendor must verify:

1. Signature matches
2. Timestamp is within 5 minutes of current server time

Return/Webhook Signing (Vendor → ABP)

Same HMAC approach. Vendor signs outbound requests/redirects so ABP can verify authenticity.

Endpoints: Third Party Implementation

All endpoints are relative to the vendor's baseUrl.

1. Create Session

Creates a new service session for a candidate.

POST /api/sessions

Request headers:

Content-Type: application/json

X-Timestamp: 1716820000

X-Signature: <signature>

Request body:

```
{  
  "userId": "uuid",  
  "firstName": "Jane",  
  "lastName": "Doe",  
  "email": jane.doe@example.com,  
  "language": "en-UK",  
  "customerId": "uuid",  
  "serviceId": 7897,  
  "normId": 2067  
}
```

All fields are required. email, firstName, lastName may be pseudonymized depending on ABP configuration.

Response (201 Created):

```
{  
  "sessionId": "uuid"  
}
```

2. Start Session

Activates the session and returns a one-time launch URL.

POST /api/sessions/{sessionId}/start

Request headers:

X-Timestamp: 1716820000

X-Signature: <signature>

Request body: empty

Response (200 OK):

```
{
  "url": "https://vendor.example.com/service/otp-xyz789"
}
```

URL requirements:

- Contains a one-time token (opaque, unguessable)
- Expires in 30 seconds
- Consumed (invalidated) on first use
- After consumption, vendor sets an HttpOnly session cookie and renders the service UI

Calling start multiple times (resume): Returns a new one-time URL each time. Vendor resumes the session where the user left off — no data loss.

3. Get Session Status

Returns the current status of a session.

GET /api/sessions/{sessionId}/status

Request headers:

X-Timestamp: 1716820000

X-Signature: <signature>

Response (200 OK):

```
{
  "sessionId": "uuid",
  "status": 2
}
```

Response headers must include: 'Cache-Control: no-store'

Status codes:

Value	Meaning
0	Created (not started)
1	In progress
2	Completed

4. Get Results

Returns structured scores for the completed session.

GET /api/sessions/{sessionId}/results?language=en-UK&normId=2067

Request headers:

X-Timestamp: 1716820000

X-Signature: <signature>

Parameters:

Param	Type	Required	Description
language	string	Yes	BCP 47 language tag (e.g. 'en-UK', 'sv-SE', 'nl-NL')
normId	long	Yes	Norm type identifier

Response (200 OK):

```
{
  "sessionId": "uuid",
  "language": "en-UK",
  "normId": 2067,
  "normName": "NL-between 25-35",
  "values": [
    {
      "id": 1,                      // representing the id of the rawScore attribute
      "value": 7.2
    },
    {
      "id": 5,                      // representing decileBorders
      "value": [1.2, 2.4, 3.6, 4.8, 5.5, 6.1, 6.8, 7.5, 8.2]
    },
    {
      "id": 11,                     // representing scale name
      "value": "Openness to Experience"
    },
    ...
  ]
}
```

Response headers must include: 'Cache-Control: no-store'

ScoreDescription model — all fields optional except 'id':

Field	Type	Required	Description
id	long	Yes	Unique internal attribute identifier, from ABP
value	Object	Yes	The actual value of the attribute from Vendor

Attributes Types

Type	Value type	Required	Description	Indexable
rawScore	double	Yes	Raw score value	No
rawScoreMin	double	Yes	Minimum possible raw score	No
rawScoreMax	double	Yes	Maximum possible raw score	No
zScore	double	Yes	Standardized z-score	No
zScoreMin	double	Yes	Minimum z-score	No
zScoreMax	double	Yes	Maximum z-score	No
tScore	double	No	T-score (mean=50, sd=10)	No
decile	integer	No	Decile (1-10)	No
decileBorders	double[]	No	Decile borders based on raw scores	No
stanine	integer	No	Stanine (1-9)	No
stanineBorders	double[]	No	Stanine borders values if different than [-1.75,-1.25,-0.75,-0.25,0.25,0.75,1.25,1.75]	No
stens	integer	No	Sten score (1-10)	No
stensBorders	double[]	No	Sten borders values if different than [-2,-1.5,-1,-0.5,0,0.5,1,1.5,-2]	No
category	integer	Yes	Category number	No
categoryBorders	double[]	Yes	Category borders based on z-scores	No
percentile	integer	No	Percentile rank (0-100)	No
percentileBorders	double[]	No	Percentile border values	No
cScore	double	No	Computed c-score	No
cScoreCategory	integer	No	C-score category (0-10)	No
name	string	Yes	Localized score/scale name	No
description	string	Yes	Localized score description	No
categoryName	string	Yes	Localized category name	Yes
categoryDescription	string	Yes	Localized category description	Yes
cScoreCategoryName	string	No	Localized c-score category name	Yes
cScoreCategoryDescription	string	No	Localized c-score category description	Yes

The attributes definitions are stored in ABP. Each of them has a type and a group (ref scale). The attributes of type "text / string" should be returned in the required language. The returned values that depend on the norm should use the norm from the params.

For the attribute types that are indexable, there can be multiple attribute ids with the same type and group, but with different index : If a scale has 3 categories [1,2,3] we will have 3 attributes with for categoryName :

- categoryName1 with type=categoryName, valueType = string, group = extraversion, index=1
- categoryName2 with type=categoryName, valueType = string, group = extraversion, index=2
- categoryName3 with type=categoryName, valueType = string, group = extraversion, index=3 with the values: ["Low", "Medium", "High"].

5. Get Report (PDF)

Returns a PDF report as base64-encoded string.

GET /api/sessions/{sessionId}/report?reportId=42&language=en-UK&normId=2067

Request headers:

X-Timestamp: 1716820000

X-Signature: <signature>

Parameters:

Param	Type	Required	Description
reportId	long	Yes	Report type identifier
language	string	Yes	BCP 47 language tag
normId	long	Yes	Norm type identifier

Response (200 OK):

```
{
  "sessionId": "session-uuid-abc",
  "reportId": 42,
  "language": "en-UK",
  "normId": 2067,
  "normName": "NL-between 25-35",
  "pdf": "JVBERi0xLjQKMSAwIG9iago8P..."
}
```

Response headers must include: 'Cache-Control: no-store'

Endpoints: ABP Implements

These are called by the vendor.

6. Return URL (Browser Redirect)

User's browser is redirected here after completing the service.

GET

https://assessio**bloom**.online/applink/api/integrations/{vendorId}/return?session_id=SESSION_ID&status=2×tamp=1716820000&sig=SIGNATURE

Parameters:

Param	Type	Description
session_id	string	The session ID
status	integer	Session status code (see status table)
timestamp	long	Unix epoch seconds
sig	string	HMAC-SHA256(session_id\nStatus\nTimestamp, shared_secret) — pipe-delimited concatenation

ABP behavior:

1. Verifies 'sig' matches expected
2. Verifies 'timestamp' is within 5 minutes
3. Calls vendor 'GET /api/sessions/{sessionId}/status' to confirm (back-channel)

4. Shows results page to user

7. Webhook (Async Notification)

Vendor calls this when a session status changes. Vendor must retry with exponential backoff until receiving HTTP 200.

POST <https://assessiobloom.online/applink/api/integrations/{vendorId}/webhook>

Headers:

Content-Type: application/json

X-Timestamp: 1716820000

X-Signature: HMAC-SHA256("{METHOD}\n{PATH}\n{TIMESTAMP}\n{BODY}",
shared_secret)

Body:

```
{  
  "sessionId": "session-uuid-abc",  
  "status": 2,  
  "timestamp": 1716820000  
}
```

ABP response: '200 OK' (empty body)

Retry policy: Vendor retries with exponential backoff (1s, 2s, 4s, 8s, ...) up to 24 hours or until 200 received.

Complete Flow

1. CREATE SESSION (back-channel)

ABP → POST vendor/api/sessions
Headers: X-Timestamp, X-Signature
Body: { userId, firstName, lastName, email,
customerId, serviceId, normId, language}
← 201 { sessionId }



2. START SESSION (back-channel)

ABP → POST vendor/api/sessions/{sessionId}/start
Headers: X-Timestamp, X-Signature
← 200 { url: "https://vendor.com/service/otp-xyz789" }



3. LAUNCH USER (front-channel)

ABP → 302 redirect user's browser to url
Vendor: validates one-time token (single-use, 30s expiry)
→ sets HttpOnly session cookie
→ renders service UI
Token is now consumed and useless.



4. USER COMPLETES SERVICE

Vendor → 302 redirect user's browser to:
[https://assessio bloom.online/applink/api/integrations/{vendorId}/return?
session_id=X&status=2×tamp=T&sig=HMAC\(...\)](https://assessio bloom.online/applink/api/integrations/{vendorId}/return?session_id=X&status=2×tamp=T&sig=HMAC(...))
|
ABP: verifies sig → calls GET vendor/api/sessions/{id}/status
→ confirms completion → shows results page



5. WEBHOOK (async backup, parallel to step 4)

Vendor → POST https://assessio bloom.online/applink/api/integrations/{vendorId}/webhook
Headers: X-Timestamp, X-Signature
Body: { sessionId, status, timestamp }
← 200 OK
(Retries until 200)



6. FETCH RESULTS (back-channel)

ABP → GET vendor/api/sessions/{sessionId}/results?language=en-UK,normId=123
Headers: X-Timestamp, X-Signature
← 200 { values: [...] }

ABP → GET vendor/api/sessions/{sessionId}/report?reportId=42&...
Headers: X-Timestamp, X-Signature
← 200 { pdf: "base64..." }



7. RESUME (if user closed browser before finishing)

Repeat steps 2 + 3 with same sessionId.
New one-time URL issued. Vendor resumes where user left off.

Error Responses

All error responses follow a consistent format:

```
{
  "error": "ERROR_CODE",
  "message": "Human-readable description"
}
```

HTTP Status	Error Code	When
400	'INVALID_REQUEST'	Missing or invalid parameters
401	'UNAUTHORIZED'	Invalid signature or expired timestamp
404	'SESSION_NOT_FOUND'	Session ID does not exist
409	'SESSION_ALREADY_COMPLETED'	Attempting to start a completed session
410	'TOKEN_EXPIRED'	One-time launch URL has expired
410	'TOKEN_CONSUMED'	One-time launch URL already used
422	'RESULTS_NOT_READY'	Session not yet completed
429	'RATE_LIMITED'	Too many requests
500	'INTERNAL_ERROR'	Vendor internal failure

Security Summary

Concern	Solution
API call authenticity	HMAC-SHA256 signed requests (method + path + timestamp + body)
Replay attacks	Timestamp within 5-minute window
Launch URL interception	One-time token, 30s expiry, consumed on first use
Return URL forgery	HMAC signature + back-channel status verification
Webhook spoofing	HMAC-SHA256 signature on request
Caching sensitive data	'Cache-Control: no-store' required on all responses
MITM	HTTPS mandatory on all endpoints
Session hijacking	HttpOnly cookie after launch, token consumed

Requirements for Vendors

1. Implement 5 endpoints (create, start, status, results, report)
2. Verify HMAC-SHA256 signatures on all incoming requests
3. Sign return redirects and webhook calls
4. Issue one-time, short-lived launch URLs (30s expiry, single-use)
5. Set HttpOnly cookies for service UI sessions
6. Support session resume (idempotent start with same sessionId)
7. Retry webhooks with exponential backoff until 200
8. Serve all endpoints over HTTPS
9. Return 'Cache-Control: no-store' on all responses
10. Support BCP 47 language codes for localized content