Workgroup:	Open Banking Brasil GT Security
Internet-Draft:	open-banking-brasil-financial-api-1_ID2
Published:	2 September 2021
Intended Status:	Standards Track
Authors:	R. Bragg GT. Security
	Raidiam *OBBIS*

Open Banking Brasil Financial-grade API Security Profile 1.0 Implementers Draft 2

Foreword

Este documento também está disponível em português

The Open Banking Brasil Initial Structure is responsible for creating standards and specifications necessary to meet the requirements and obligations of the Brasil Open Banking Legislation as originally outlined by the Brasil Central Bank. There is a possibility that some of the elements of this document may be the subject to patent rights. OBBIS shall not be held responsible for identifying any or all such patent rights.

Open Banking Brasil Financial-grade API Security Profile 1.0 consists of the following parts:

- Open Banking Brasil Financial-grade API Security Profile 1.0
- Open Banking Brasil Dynamic Client Registration Profile 1.0

These parts are intended to be used with RFC6749, RFC6750, RFC7636, OIDC, FAPI-1-Baseline and FAPI-1-Advanced

Introduction

The Open Banking Brasil Financial-grade API is a highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability which can be applied to APIs in the Brasil Open Banking area that require a higher level of privacy than provided by standard Financial-grade API Security Profile 1.0 - Part 2: Advanced. Among other enhancements, this specification addresses privacy considerations identified in FAPI-1-Advanced that are relevent in the Open Banking Brasil specifications but have not, so far, been required by other jurisdictions.

Although it is possible to code an OpenID Provider and Relying Party from first principles using this specification, the main audience for this specification is parties who already have a certified implementation of Financial-grade API Security Profile 1.0 - Part 2: Advanced and want to achieve certification for the Brasil Open Banking programme.

Notational Conventions

The key words "shall", "shall not", "should", "should not", "may", and "can" in this document are to be interpreted as described in ISO Directive Part 2. These key words are not used as dictionary terms such that any occurrence of them shall be interpreted as key words and are not to be interpreted with their natural language meanings.

Table of Contents

1. Scope

This document specifies the method of

- applications to obtain the OAuth tokens in an appropriately secure manner for higher risk access to data in a manner that meets the requirements of Open Banking Brasil;
- applications to use OpenID Connect to identify the customer; and
- applications to use OpenID Connect to assert identity of the customer;

This document is applicable to all participants engaging in Open Banking in Brasil.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applied. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISODIR2 - ISO/IEC Directives Part 2

RFC6749 - The OAuth 2.0 Authorization Framework

RFC6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage

RFC7636 - Proof Key for Code Exchange by OAuth Public Clients

RFC6819 - OAuth 2.0 Threat Model and Security Considerations

RFC7515 - JSON Web Signature (JWS)

RFC7519 - JSON Web Token (JWT)

RFC7591 - OAuth 2.0 Dynamic Client Registration Protocol

RFC7592 - OAuth 2.0 Dynamic Client Registration Management Protocol

BCP195 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

OIDC - OpenID Connect Core 1.0 incorporating errata set 1

FAPI-CIBA - Financial-grade API: Client Initiated Backchannel Authentication Profile

OIDD - OpenID Connect Discovery 1.0 incorporating errata set 1

OIDR - OpenID Connect Registration 1.0 incorporating errata set 1

RFC8705 - OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens

JARM - Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

PAR - OAuth 2.0 Pushed Authorization Requests

JAR - OAuth 2.0 JWT Secured Authorization Request

FAPI-1-Baseline - Financial-grade API Security Profile 1.0 - Part 1: Baseline

FAPI-1-Advanced - Financial-grade API Security Profile 1.0 - Part 2: Advanced

FAPI-2-Baseline - Financial-grade API Security Profile 2.0 - Part 1: Baseline

FAPI-2-Advanced - Financial-grade API Security Profile 2.0 - Part 2: Advanced

LIWP - OIDF FAPI WG Lodging Intent Working Paper

OBB-FAPI-DCR - Open Banking Brasil Financial-grade API Dynamic Client Registration Profile 1.0

RFC4648 - The Base16, Base32, and Base64 Data Encodings

3. Terms and definitions

For the purpose of this document, the terms defined in RFC6749, RFC6750, RFC7636, OpenID Connect Core and ISO29100 apply.

4. Symbols and Abbreviated terms

API - Application Programming Interface

OBBIS - Open Banking Brasil Initial Structure

CSRF - Cross Site Request Forgery

DCR - Dynamic Client Registration

FAPI - Financial-grade API

HTTP - Hyper Text Transfer Protocol

OIDF - OpenID Foundation

REST - Representational State Transfer

TLS - Transport Layer Security

MFA - Multi-Factor Authentication

5. Brasil Open Banking Security Profile

5.1. Introduction

The Brasil Open Banking Security profile specifies additional security and identity requirements for high risk API resources protected by the OAuth 2.0 Authorization Framework that consists of RFC6749, RFC6750, RFC7636, FAPI-1-Baseline, FAPI-1-Advanced and other specifications.

This profile describes security and features provisions for a server and client that are necessary for the Brasil Open Banking Programme by defining the measures to mitigate or address:

- attacks that address privacy considerations identified in clause 9.1 of [FAPI1 Advanced]

- the requirement to support fine-grained access to resources for data minimisation purposes
- the requirement to convey the Authentication Context Request that was performed by an OpenID Provider to a Client to enable a appropriate client management of customer conduct risk.
- the requirement for clients to assert a pre-existing customer relationship by asserting a customer identity claim as part of the authorization flow.

5.2. Open Banking Brasil security provisions

5.2.1. Introduction

Open Banking Brasil has a requirement to address privacy considerations that were identified but not addressed in the FAPI-1-Advanced final specification without imposing additional requirements on Authorisation Servers being proposed in FAPI-2-Baseline. Participants in this ecosystem have a need for clients to request an openid provider to confirm values of identity claims as part of an authorization request using the mechanism defined in clause 5.5.1 of OIDC. The use of the claims parameter to request explicit claims values requires clients to ensure that they encrypt the request object to avoid information leakage. This risk is identified in clause 7.4.1 of FAPI-1-Baseline. In addition this profile describes the specific scope, acr and client management requirements necessary to support the wider Open Banking Brasil ecosystem.

As a profile of the OAuth 2.0 Authorization Framework, this document mandates the following for the Brasil Open Banking Security profile.

5.2.2. Authorization server

The Authorization Server shall support the provisions specified in clause 5.2.2 of Financial-grade API Security Profile 1.0 - Part 2: Advanced

In addition, the Authorization Server

1. shall support a signed and encrypted JWE request object passed by value or shall require pushed authorization requests PAR;
2. shall distribute discovery metadata (such as the authorization endpoint) via the metadata document as specified in OIDD and [RFC8414]
3. shall support the claims parameter as defined in clause 5.5 OpenID Connect Core
4. shall support the oidc standard claim "cpf" as defined in clause 5.2.2.2 of this document
5. shall support the oidc standard claim "cnpj" as defined in clause 5.2.2.3 of this document if providing access to resources where the resource owner is not a `natural person`
6. shall support the acr "urn:brasil:openbanking:loa2" as defined in clause 5.2.2.4 of this document
7. should support the acr "urn:brasil:openbanking:loa3" as defined in clause 5.2.2.4 of this document
8. shall implement the userinfo endpoint as defined in clause 5.3 OpenID Connect Core
9. shall support parameterized OAuth 2.0 resource scope *consent* as defined in clause 6.3.1 OIDF FAPI WG Lodging Intent Pattern
10. may support Financial-grade API: Client Initiated Backchannel Authentication Profile

11. shall support Financial-grade API: Client Initiated Backchannel Authentication Profile if supporting scope *payments*
12. shall support refresh tokens
13. shall issue access tokens with an expiry no greater than 900 seconds and no less than 300 seconds

5.2.2.1. ID Token as detached signature

The Authorization Server shall support the provisions specified in clause 5.2.2.1 of Financial-grade API Security Profile 1.0 - Part 2: Advanced

In addition, if the `response_type` value `code id_token` is used, the Authorization Server

1. should not return sensitive PII in the ID Token in the authorization response, but if it needs to, then it shall encrypt the ID Token.

5.2.2.2. Requesting the "cpf" Claim

This profile defines "cpf" as a new standard claim as per clause 5.1 OIDC

The **CPF** number (Cadastro de Pessoas Físicas, [sepeˈɛfi]; Portuguese for "Natural Persons Register") is the **Brazilian** individual taxpayer registry identification. This number is attributed by the **Brazilian** Federal Revenue to Brazilians and resident aliens who, directly or indirectly, pay taxes in **Brazil**. In the Brasil Open Banking identity model, the cpf is a string consisting of numbers that is 11 characters long and may start with a 0. If the cpf Claim is requested as an Essential Claim for the ID Token or UserInfo response with a values parameter requesting a specific cpf value, the Authorization Server MUST return a cpf Claim Value that matches the requested value. If this is an Essential Claim and the requirement cannot be met, then the Authorization Server MUST treat that outcome as a failed authentication attempt.

Name: cpf, Type: String, Regex: $'d{11}$'

5.2.2.3. Requesting the "cnpj" Claim

This profile defines "cnpj" as a new standard claim as per clause 5.1OIDC

CNPJ, short for Cadastro Nacional de Pessoas Jurídicas, is an identification number of **Brazilian** companies issued by the **Brazilian** Ministry of Revenue, **in** Portuguese "Secretaria da Receita Federal" or "Ministério da Fazenda". In the Brasil Open Banking identity model, individuals can associated with 0 or more CNPJs. A CNPJ is a string consisting of numbers that is 14 digits long and may start with a 0, the first eight digits identify the company, the four digits after the slash identify the branch or subsidiary ("0001" defaults to the headquarters), and the last two are checksum digits. For this profile, the cnpj claim must be requested and supplied as the 14 digit number.

If the cnpj Claim is requested as an Essential Claim for the ID Token or UserInfo response with a values parameter requesting a specific cnpj value, the Authorization Server MUST return a cnpj Claim Value that contains a **set** of CNPJs one of which must match the requested value. If this is an Essential Claim and the requirement cannot be met, then the Authorization Server MUST treat that outcome as a failed authentication attempt.

Name: cnpj, Type: Array of Strings, Array Element Regex: $'d{14}$'

5.2.2.4. Requesting the "urn:brasil:openbanking:loa2" or "urn:brasil:openbanking:loa3" Authentication Context Request

This profile defines "urn:brasil:openbanking:loa2" and "urn:brasil:openbanking:loa3" as new Authentication Context Request classes.

- **LoA2:** Authentication performed using single factor;
- **LoA3:** Authentication performed using multi factor (MFA)

The following rules are applicable:

- * **Read-only APIs :** shall require resource owner authentication to at least LoA2, elevating the requirement to authenticate resource owners to LoA3 is at the discretion of the Authorization Server;
- **Read-and-Write APIs (Transactional):** shall require resource owner authentication to at least LoA3.

Authentication factors clarification

The authentication methods are:

- Something you know, such as password or phrase
- Something you have, such as token or smartcard;
- Something you are, such as biometric validation.

To performe a MFA authentication is necessary the end user to present at least two different methods as listed above. A unique method used more than once is not accepted as MFA.

5.2.3. Confidential client

A confidential client shall support the provisions specified in clause 5.2.3 of Financial-grade API Security Profile 1.0 - Part 2: Advanced,

In addition, the confidential client

1. shall support *encrypted* request objects
2. shall support Pushed Authorisation Requests PAR
3. shall use *encrypted* request objects if not using PAR
4. shall support parameterized OAuth 2.0 resource scope *consent* as defined in clause 6.3.1 OIDF FAPI WG Lodging Intent Pattern
5. shall support refresh tokens

6. Security considerations

Participants shall support all security considerations specified in clause 8 Financial-grade API Security Profile 1.0 - Part 1: Advanced and the Brazilian Central Bank Open Banking Security Manual. The Brazilian ICP issues RSA x509 certificates only therefor section removes for simplicity support for EC algorithms and requires that only IANA recommended encryption algorithms be used.

6.1. Message Content Signing Considerations (JWS)

1. JWS standad defined in RFC7515 shall be adopted to ensure integrity and non-repudiation of information processed in sensitive **API's (message sign requirement is indicated at API's documentation/swagger)**, which includes:
    - Header (*JSON Object Signing and Encryption - JOSE Header*), which defines the algorithm used and includes information about the public key or certificate that can be used to validate the signature;
    - Payload (*JWS Payload*): content itself as detailed in the API specification;
    - Digital signature (*JWS Signature*): digital signature, performed according to header parameters.
2. Each of elements above must be encoded using the Base64url pattern RFC4648 and the elements must be concatenated with "." (JWS Compact Serialization method as defined in RFC7515).
3. The payload of signed messages (request *JWT* and response *JWT*) shall include the following claims as defined at RFC7519:
    - **aud** (in the *JWT* request): the Resource Provider (eg the institution holding the account) must validate if the value of the **aud** field matches the endpoint being triggered;
    - **aud** (in *JWT* response): the API client (eg initiating institution) shall validate if the value of the **aud** field matches its own `organisationId` listed in the directory;
    - **iss** (in the *JWT* request and in the *JWT* response): the receiver of the message shall validate if the value of the **iss** field matches the `organisationId` of the sender;
    - **jti** (in the *JWT* request and in the *JWT* response): the value of the **jti** field shall be filled with the UUID defined by the institution according to [RFC4122] version 4;
    - **iat** (in the *JWT* request and in the *JWT* response): the **iat** field shall be filled with the message generation time and according to the standard established in RFC7519 to the *NumericDate* format.
4. The HTTP content-type of requests and responses with JWS messages shall be defined as: "application/jwt".
5. The JOSE header must contain the following attributes:
    - **alg** - shall be filled with the value `PS256`";
    - **kid** - shall be filled with the key identifier value used for the signature;
    - **typ** - shall be filled with the value `JWT`.
    - In case of error in signature validation by `Resource Provider` the API provider shall return HTTP error message with `status code` **400** and the `ResponseError` content shall include, in the `code` property, the content `BAD_SIGNATURE`.
    - Errors in validating the signed messages received by the client application (eg payment initiator) must be logged and the `Resource Provider` (eg account holding institution) must be notified.
6. The receiver shall validate the consistency of the JWS message's digital signature **exclusively based on the information obtained from the directory**, that is, based on the keys published in the institution's JWKS in the directory.

7. Signatures must be performed using the digital signature certificate specified in the Open Banking Brazil Certificates Standard.

6.2. Algorithm considerations

For JWS, both clients and Authorization Servers

1. shall use PS256 algorithm;

6.2.1. Encryption algorithm considerations

For JWE, both clients and Authorization Servers

1. shall use RSA-OAEP with A256GCM

6.2.2. Secure Use of Transport Layer Security considerations

For TLS, Authorization Server endpoints and Resource Server endpoints used directly by the Client

1. shall support `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
2. shall support `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`

7. Data Sharing Considerations

7.1. Authorisation Mechanism

7.1.1. Introduction

Existing mechanisms for appropriately managing access to resources defined in RFC6749 are insufficient to meet the requirements for a modern data sharing ecosystem. Leveraging static scope strings does not provide consumers control of sufficient granularity to share with third parties. Open Banking Brasil have elected to implement a Consent API as a OAuth 2.0 protected resource that can be used to manage fine grain access to resources. The reference to the Consent Resource will be conveyed as part of an OAuth 2.0 dynamic resource scope.

7.1.2. Dynamic Consent Scope Definition

This profile defines OAuth 2.0 dynamic scope "consent" as follows:

- string 'consent'; and
- delimiter of a colon ":"; and
- Consent API REST Resource Id as returned by a successful creation of Open Banking Consent Resource;

In addition:

- the Consent Resource Id must include url safe characters only;
- the Consent Resource Id must be namespaced;
- the Consent Resource Id must have the properties of a nonce;

7.1.3. Dynamic Consent Scope Example

consent:urn:bancoex:C1DD33123

7.2. Authorisation Life Cycle

7.2.1. Introduction

The Consent Resource has a life cycle that is managed seperately and distinctly from the OAuth 2.0 Authorisation Framework. The state transitions and expected behaviours and error conditions expected of REST Resources protected with this profile are defined in the functional API specifications published by Open Banking Brasil.

7.2.2. Authorization server

In addition to the requirements outlined in Open Banking Brasil security provisions the Authorization Server

1. shall only issue tokens on presentation of a refresh token when the consent resource the refresh token is bound to is active and valid;
2. shall only share access to resources when presented with an access token linked to an active and valid consent;
3. shall revoke refresh tokens and where practicable access tokens when the linked Consent Resource is deleted;
4. shall ensure Access Tokens are issued with sufficient scope necessary for access to data specified in the Permissions element of a linked Consent Resource object;
5. shall not reject an authorisation request requesting more scope than is necessary to access data specified in the Permissions element of a linked Consent Resource object;
6. may reduce requested scope to a level sufficient to enable access to data resources specified in the Permissions element of a linked Consent Resource object;
7. shall retain a complete audit history of the consent resource in accordance with current Central Bank brazilian regulation;

7.2.3. Confidential Client

In addition to the requirements outlined in Open Banking Brasil security provisions the Confidential Client

1. shall revoke where possible and cease usage of refresh and access tokens that are bound to a Consent Resource that has been deleted;
2. shall delete Consent Resource that are expired;

8. Acknowledgements

With thanks to all who have set the foundations for secure and safe data sharing through the formation of the OpenID Foundation FAPI Working Group, the Open Banking Brasil GT Security and to the pioneers who will stand on their shoulders.

The following people contributed to this document:

- Ralph Bragg (Raidiam)
- Joseph Heenan (Authlete)

- Alexandre Siqueira (Mercado Pago)
- Marcos Rodrigues (Itaú)
- Mário Ginglass (BNDES)

Appendix A. Notices

Authors' Addresses

Ralph Bragg
Raidiam
Email: ralph.bragg@raidiam.com
URI: https://www.raidiam.com/

OBBIS GT Security
Open Banking Brasil Initial Structure
Email: gt-seguranca@openbankingbr.org
URI: https://openbankingbrasil.org.br/