



DPC: 25/30512076 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 06 May 2025

Origin: International

Latest date for receipt of comments: 29 June 2025

Project No. 2025/01005

Responsible committee: ICT/1 Information systems co-ordination

Interested committees:

Title: BS ISO/IEC 25791-2 Draft Information technology — OpenID Connect FAPI Security Profile 1.0. Part 2: Advanced.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 29 June 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 25791-2

Information technology — OpenID Connect FAPI Security Profile 1.0 —

Part 2: Advanced

ICS: 35.030

ISO/IEC JTC 1

Secretariat: **ANSI**

Voting begins on:
2025-05-06

Voting terminates on:
2025-07-29

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 25791-2:2025(en)

Full document details: 25/30512076 DC

© ISO/IEC 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Foreword	3
Introduction	3
Notational Conventions	4
1. Scope	4
2. Normative references	4
3. Terms and definitions	5
4. Symbols and abbreviated terms	5
5. Baseline security profile	6
5.1 Introduction	6
5.2 Baseline security provisions	6
5.2.1 Introduction	6
5.2.2 Authorization server	6
5.2.3 Public client	8
5.2.4 Confidential client	8
6. Accessing Protected Resources	9
6.1 Introduction	9
6.2 Baseline access provisions	9
6.2.1 Protected resources provisions	9
6.2.2 Client provisions	10
7. Security considerations	10
7.1 TLS and DNSSEC considerations	10
7.2 Message source authentication failure	11
	2

7.3 Message integrity protection failure	11
7.4 Message containment failure	11
7.4.1 Authorization request and response	11
7.4.2 Token request and response	11
7.4.3 Resource request and response	11
7.5 Native Apps	12
7.6 Incomplete or incorrect implementations of the specifications	12
7.7 Discovery & Multiple Brands	12
8. Privacy considerations	13
8.1 Introduction	13
9. Acknowledgement	14
10. Bibliography	14
Appendix A. Copyright notice & license	15

Foreword

The OpenID Foundation (OIDF) promotes, protects and nurtures the OpenID community and technologies. As a non-profit international standardizing body, it is comprised by over 160 participating entities (workgroup participants). The work of preparing implementer drafts and final international standards is carried out through OIDF workgroups in accordance with the OpenID Process. Participants interested in a subject for which a workgroup has been established have the right to be represented in that workgroup. International organizations, governmental and non-governmental, in liaison with OIDF, also take part in the work. OIDF collaborates closely with other standardizing bodies in the related fields.

Final drafts adopted by the Workgroup through consensus are circulated publicly for the public review for 60 days and for the OIDF members for voting. Publication as an OIDF Standard requires approval by at least 50 % of the members casting a vote. There is a possibility that some of the elements of this document may be the subject to patent rights. OIDF shall not be held responsible for identifying any or all such patent rights.

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

- Financial-grade API Security Profile 1.0 - Part 1: Baseline
- [Financial-grade API Security Profile 1.0 - Part 2: Advanced](#)

These parts are intended to be used with [RFC6749](#), [RFC6750](#), [RFC7636](#), and [OIDC](#).

Introduction

The Financial-grade API is a highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability. The Financial-grade API security profile can be applied to APIs in any market area that requires a higher level of security than provided by standard [OAuth](#) or [OpenID Connect](#). Among other security enhancements, this specification provides a secure alternative to screen scraping. Screen scraping accesses user's data and functions by impersonating a user through password sharing. This brittle, inefficient, and insecure practice creates security vulnerabilities which require financial institutions to allow what appears to be an automated attack against their applications.

This document is Part 2 of FAPI Security Profile 1.0 that specifies an advanced security profile of OAuth that is suitable to be used for protecting APIs with high inherent risk. Examples include APIs that give access to highly sensitive data or that can be used to trigger financial transactions (e.g., payment initiation). This document specifies the controls against attacks such as: authorization request tampering, authorization response tampering including code injection, state injection, and token request phishing. Additional details are available in the security considerations section.

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 OpenID Connect and want to achieve a higher level of security. Implementers are encouraged to understand the security considerations contained in Section 8.7 before embarking on a 'from scratch' implementation.

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.

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

1. Scope

This part of the document specifies the method of

- applications to obtain the OAuth tokens in an appropriately secure manner for higher risk access to data;
- applications to use OpenID Connect to identify the customer; and
- using tokens to interact with the REST endpoints that provides protected data;

This document is applicable to higher risk use cases which includes commercial and investment banking and other similar industries.

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

[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

[OIDD](#) - OpenID Connect Discovery 1.0 incorporating errata set 1

[MTLS](#) - OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens