FINAL DRAFT
International Standard

ISO/IEC
FDIS
25791-2

Information technology — OpenID Connect FAPI Security Profile 1.0 —

Part 2: Advanced

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2026-07-09

Voting terminates on:
2026-09-03

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.

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.

Reference number
ISO/IEC FDIS 25791-2:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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 v

Introduction vi

Notational Conventions vii

1. Scope 1

2. Normative references 1

3. Terms and definitions 2

4. Symbols and abbreviated terms 2

5. Advanced security profile 3

5.1 Authorization response security 3
5.1.1 Introduction 3
5.1.2 ID Token as detached signature 3
5.1.3 JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) 4

5.2 Advanced security provisions 4
5.2.1 Introduction 4
5.2.2 Authorization server 4
5.2.3 Confidential client 6
5.2.4 (withdrawn) 7
5.2.5 (withdrawn) 7

6. Accessing protected resources (using tokens) 7

6.1 Introduction 7

6.2 Advanced access provisions 8
6.2.1 Protected resources provisions 8
6.2.2 Client provisions 8

7. (Withdrawn) 8

8. Security considerations 8

8.1 Introduction 8

8.2. Uncertainty of resource server handling of access tokens 8

8.3 Attacks using weak binding of authorization server endpoints 8
8.3.1 Introduction 8
8.3.2 Client credential and authorization code phishing at token endpoint 9
8.3.3 Identity provider (IdP) mix-up attack 9
8.3.4 Access token phishing 9

8.4. Attacks that modify authorization requests and responses 10
8.4.1 Introduction 10
8.4.2 Authorization request parameter injection attack 10
8.4.3 Authorization response parameter injection attack 10

8.5 TLS considerations 10

8.6 Algorithm considerations 11
8.6.1 Encryption algorithm considerations 11

8.7 Incomplete or incorrect implementations of the specifications 11

8.8 Session Fixation 11

© ISO/IEC 2026 – All rights reserved

8.9 JWKS URIs 11
8.10 Multiple clients sharing the same key 12
8.11 Duplicate Key Identifiers 12
9. Privacy considerations 12
10. IANA Considerations 14
10.1. Additions to JWT claims registry 14
10.1.1. Registry Contents 14
Annex A (Informative) Examples 15
A.0 JWK for examples 15
A.1 Example request object 15
A.2 Example signed id_token for authorization endpoint response 16
A.3 Example signed and encrypted id_token for authorization endpoint response 16
A.4 Example JARM response 17
A.5 Example private_key_jwt client assertion 18
Annex B (Informative) Acknowledgement 19
Notices 20
Bibliography 21

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by the OpenID Foundation (OIDF) (as FAPI Security Profile 1.0 - Part 2: Advanced) and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

A list of all parts in the ISO/IEC 25791 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

FAPI is a highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability. The FAPI 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 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.

© ISO/IEC 2026 – All rights reserved

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/IEC Directives, Part 2. These keywords are not used as dictionary terms such that any occurrence of them shall be interpreted as keywords and are not to be interpreted with their natural language meanings.

© ISO/IEC 2026 – All rights reserved

Information technology — OpenID Connect FAPI 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 documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Part 1 FAPI Security Profile 1.0 - Part 1: Baseline

ISO/IEC 29100 ISO/IEC 29100 information technology – Security techniques – Privacy framework

RFC 6749 The OAuth 2.0 Authorization Framework

RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage

RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients

OIDC - OpenID Connect Core 1.0 incorporating errata set 2

RFC 8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

JARM - JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)

RFC 9101 - OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)

RFC 9126 - OAuth 2.0 Pushed Authorization Requests (PAR)

© ISO/IEC 2026 – All rights reserved

3. Terms and definitions

For the purpose of this document, the terms defined in RFC 6749, RFC 6750, RFC 7636, OpenID Connect Core, and ISO 29100 apply.

4. Symbols and abbreviated terms

API – application programming interface

CSRF – cross site request forgery

DN – distinguished name

FAPI – FAPI

HTTP – hypertext transfer protocol

HTTPS – hypertext transfer protocol secure

JAR – JWT-secured authorization request

JARM – JWT-secured authorization response mode

JOSE – javascript object signing and encryption

JSON – javascript object notation

JWE – JSON web encryption

JWK – JSON web key

JWKS – JSON web key sets

JWS – JSON web signature

JWT – JSON web token

MTLS – mutual transport layer security

OIDF – OpenID foundation

PAR – pushed authorization request

PII – personally identifiable information

PKCE – proof key for code exchange

REST – representational state transfer

RP – relying party

TLS – transport layer security

URI – uniform resource identifier

URL – uniform resource locator

© ISO/IEC 2026 – All rights reserved