International Standard

ISO/IEC 25791-1

First edition
2026-09

Information technology — OpenID Connect FAPI Security Profile 1.0 —

Part 1: Baseline

Technologies de l'information — Profil de sécurité 1.0 basé sur le protocole OpenID Connect conçu pour les API finanières, FAPI —

Partie 1: Niveau de référence

Reference number
ISO/IEC 25791-1:2026(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 ... iv
Introduction ... v
Notational conventions ... vi
1. Scope ... 1
2. Normative references ... 1
3. Terms and definitions ... 2
4. Symbols and abbreviated terms ... 2
5. Baseline security profile ... 2
5.1 Introduction ... 2
5.2 Baseline security provisions ... 3
5.2.1 Introduction ... 3
5.2.2 Authorization server ... 3
5.2.3 Public client ... 5
5.2.4 Confidential client ... 5
6. Accessing Protected Resources ... 6
6.1 Introduction ... 6
6.2 Baseline access provisions ... 6
6.2.1 Protected resources provisions ... 6
6.2.2 Client provisions ... 7
7. Security considerations ... 7
7.1 TLS and DNSSEC considerations ... 7
7.2 Message source authentication failure ... 7
7.3 Message integrity protection failure ... 8
7.4 Message containment failure ... 8
7.4.1 Authorization request and response ... 8
7.4.2 Token request and response ... 8
7.4.3 Resource request and response ... 8
7.5 Native Apps ... 8
7.6 Incomplete or incorrect implementations of the specifications ... 9
7.7 Discovery & Multiple Brands ... 9
8. Privacy considerations ... 9
Annex A (Informative) Acknowledgement ... 11
Notices ... 12
Bibliography ... 13

© 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 1: Baseline) 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 financial institutions to allow what appears to be an automated attack against their applications.

This document is Part 1 of FAPI Security Profile 1.0. It specifies a baseline security profile of OAuth that is suitable for protecting APIs with a moderate inherent risk. Importantly, this profile does not provide non-repudiation (signing of authorization requests and responses) and sender-constrained access tokens. If such features or a higher level of security is desired, the use of FAPI Security Profile 1.0 - Part 2: Advanced is recommended.

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 7.6 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 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.

© ISO/IEC 2026 – All rights reserved

Information technology — OpenID Connect FAPI Security Profile 1.0 —

Part 1:
Baseline

1. Scope

This document specifies the method for an application to:

- obtain OAuth tokens in a moderately secure manner for access to protected data;
- use OpenID Connect (OIDC) to identify the customer (user); and
- use tokens to access REST APIs in a moderately secure manner.

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.

RFC 4122 - A Universally Unique IDentifier (UUID) URN Namespace

RFC 6749 - The OAuth 2.0 Authorization Framework

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

RFC 6125 - Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)

BCP212 - OAuth 2.0 for Native Apps

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

IANA TLSP - Transport Layer Security (TLS) Parameters

OIDC - OpenID Connect Core 1.0 incorporating errata set 2

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

OIDD - OpenID Connect Discovery 1.0 incorporating errata set 2

RFC 7231 - Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content

© 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, OIDC apply.

4. Symbols and abbreviated terms

API - application programming interface

CAA - certificate authority authorization

CORS – cross-origin resource sharing

CSRF - cross site request forgery

DNSSEC - domain name system security extensions

FAPI - FAPI

HTTP - hypertext transfer protocol

IP - internet protocol

JARM - JWT secured authorization response mode

JSON - javaScript object notation

JWT - JSON web token

OIDF - OpenID foundation

RP - relying party

RSA - Rivest-Shamir-Adleman

REST - representational state transfer

TLS - transport layer security

URI - uniform resource identifier

UTF - unicode transformation format

UUID - universally unique identifier

5. Baseline security profile

5.1 Introduction

The OIDF FAPI security profile specifies security requirements for API resources protected by the OAuth 2.0 Authorization Framework that consists of RFC 6749, RFC 6750, RFC 7636, and other specifications.

© ISO/IEC 2026 – All rights reserved