TECHNICAL SPECIFICATION

ISO/TS 23029

First edition
2020-02

Web-service-based application programming interface (WAPI) in financial services

Reference number
ISO/TS 23029:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Design principles **3**
4.1 General 3
4.2 Standards compatibility 3
4.3 Extensibility 3
4.4 Non-repudiation 3
4.5 Web resource unique identifiers (ID fields) 3
4.6 Idempotency 3
4.7 States 3
5 Related technology **3**
5.1 General 3
5.2 Representational state transfer (REST) and simple object access protocol (SOAP) 3
5.2.1 General 3
5.2.2 REST 4
5.2.3 SOAP 4
5.3 WebSocket and Webhook 5
5.3.1 General 5
5.3.2 WebSocket 5
5.3.3 Webhook 5
5.4 HTTPS 6
5.5 JSON and XML 6
5.5.1 General 6
5.5.2 JSON 6
5.5.3 XML 6
5.6 Content negotiation 7
5.7 RESTful API description languages 7
6 Naming conventions **7**
7 Resource path **8**
7.1 General 8
7.2 Resource hops 8
7.3 Single resource versus collections of resources 9
8 WAPI styles **9**
8.1 General 9
8.2 REST 10
8.2.1 General 10
8.2.2 Uniform interface 11
8.2.3 Apply the standard HTTP methods 12
8.2.4 Stateless sessions 13
8.2.5 Idempotency 13
8.2.6 Composition of the URI 14
8.2.7 Handling associations between resources 14
8.2.8 Request parameter usage 14
8.2.9 Post usage 17
8.2.10 The response 18
8.3 Asynchronous messaging and server push 21
8.3.1 Bidirectional communication model 22
8.3.2 Message subscription 23

8.3.3 Message publish 24
9 Data payload syntax 24
9.1 JSON 24
9.1.1 General 24
9.1.2 Syntax and structure 24
9.1.3 Data types 26
9.2 XML 26
9.2.1 General 26
9.2.2 Syntax and structure 26
9.2.3 Data types 28
10 Security and authentication 30
10.1 General 30
10.2 TLS 30
10.2.1 Certificate issuance and verification 31
10.3 Application and access layer security 32
10.3.1 Introduction 32
10.3.2 Overview of the OAuth 2.0 protocol 33
10.4 Read-only security profile 33
10.5 Read and write security profile 33
10.6 Message level integrity, source authentication and non-repudiation 34
10.6.1 General 34
10.6.2 Signing HTTP requests and responses 34
10.6.3 Signing JSON Payload 34
10.6.4 HTTP signature 35
10.7 Message level encryption 35
10.8 Version control 35
11 Use cases 36
11.1 ISO 20022 Web services 36
11.1.1 Introduction 36
11.1.2 Modelling guidelines 36
11.2 Mapping rules 39
11.2.1 RepositoryConcept 39
11.2.2 MessageDefinition 39
11.2.3 MessageBuildingBlock 40
11.2.4 MessageComponent 40
11.2.5 ChoiceComponent 41
11.2.6 MessageElement 42
11.2.7 ISO 20022 DataType transformation to JSON Schema 43
Annex A (informative) **Approach to FX trading 49**
Bibliography 52

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 9, *Information exchange for financial services*.

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.

Introduction

0.1 Opening comments

The purpose of this document is to help implementers in the financial services industry define the framework, function and protocols for an application programming interface (API) ecosystem, enabling online synchronised interactions. It documents an international view of an API ecosystem in response to an urgent and significant world-wide demand for guidance and standardisation of APIs in financial services.

This has been driven by a number of emerging requirements – market-, corporate- and regulatory-driven – from different communities and jurisdictions for financial institutions to share data and enable functionality, such as between third parties acting on behalf of the customer, client or end user; between business to business processes; and within internal processes. It has been widely agreed that standardised APIs provide the most secure, developer-friendly, efficient, technically proven way of meeting many of these requirements. Moreover, it is understood that a standardised approach would unlock benefits conducive to promoting interoperability, enhancing security and supporting innovation. The sharing of data, and the subsequent use of APIs, is not limited to exchanges referenced in this document.

Despite these emerging requirements, there is currently no standardised approach at an international level. Moreover, there is no informative documentation covering the various considerations for developing APIs in financial services, especially given the maturity of some of its components (e.g. some are in draft). This document has been developed in response to meet these current and foreseen requirements that exist in the market. This document does not specify implementations of APIs, but instead takes an international view and references, as appropriate, specific implementation scenarios for illustrative purposes for guidance.

0.2 How to approach this document

This document should be approached as a best-practice framework for developing APIs in financial services. In this sense, some aspects of the document are more mature than others. The document is prescriptive where there is room to be. Where areas are less mature, commentary on best practice has been provided and the considerations set out.

Broadly speaking, this document adopts the following logic and order:

— Clause 3: terms and definitions used in the document;

— Clause 4: the initial considerations for the design of the API;

— Clause 5: overview and commentary on the different technology options;

— Clause 8: specific guidance on APIs under WAPI technical specification.

In Annex A, we set out an example of how to approach the document depending on a specific business area/desired API functionality.

Web-service-based application programming interface (WAPI) in financial services

1 Scope

This document defines the framework, function and protocols for an API ecosystem that will enable online synchronised interaction. Specifically, the document:

— defines a logical and technical layered approach for developing APIs, including transformational rules. Specific logical models (such as ISO 20022 models) are not included, but they will be referenced in the context of specific scenarios for guidance purposes;

— will primarily be thought about from a RESTful design point of view, but will consider alternative architectural styles (such as WebSocket and Webhook) where other blueprints or scenarios are offered;

— defines for the API ecosystem design principles of an API, rules of a Web-service-based API, the data payload and version control;

— sets out considerations relevant to security, identity and registration of an API ecosystem. Specific technical solutions will not be defined, but they will be referenced in the context of specific scenarios for guidance purposes;

— defines architectural usage beyond query/response asynchronous messaging towards publish/subscribe to support advanced and existing business models.

This document does not include:

— a specific technical specification of an API implementation in financial services;

— the development of JSON APIs based on the ISO 20022 specific message formats, such as PAIN, CAMT and PACS;

— a technical specification that is defined or determined by specific legal frameworks.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
application programming interface
API
set of well-defined methods, functions, protocols, routines or commands which application software uses with facilities of programming languages to invoke services

Note 1 to entry: An API is available for different types of software, including Web-based system/ecosystem.