**PAS Explanatory Report for**

**FAPI 2.0**

**Suite of Specifications**

PAS Submitter: OpenID Foundation

2024-04-23

The OpenID Foundation declares that the organization acceptance criteria used for its recognition as a PAS Submitter have not changed since that recognition was granted.

JTC 1 offers its National Bodies, its Subcommittees (SCs), A-liaison organizations or PAS Mentors for counsel and advice to PAS Submitters during the generation of this Report and throughout the whole transposition process. JTC 1 encourages PAS Submitters to make use of this counsel.

# 

# **Template for PAS Explanatory Report**

References:

1. Consolidated JTC 1 Supplement clause F.2.1.1 – Requirement to submit an explanatory report with Fast Track submissions

2. Consolidated JTC 1 Supplement clause F.3 – *Preparation and Adoption of International Standards – JTC 1 PAS Transposition Process*

3. JTC 1 Standing Document 9 – *Guide to the Transposition of Publicly Available Specifications into International Standards*

Once a PAS Originator has been recognised, a PAS submission to the JTC 1 Secretariat may occur within the technical scope identified in the PAS Submitter application. This PAS submission must be accompanied by an Explanatory Report produced by the Submitter, and a statement that the conditions for recognition of the PAS Submitter have not changed, or an indication of the nature of changes that have occurred (see SD9 clause 6.2.2). The Explanatory Report must address the document-related criteria as shown below (section 7.4 from SD9).

The Submitter is further invited to comment on the following items in the Explanatory Report:

a) Clearly define the technical concepts used in the submission (see the definition of Explanatory Report in the Consolidated JTC 1 Supplement F.3.1 and SD 9 clause 5) and

b) Explicitly reference the JTC 1 common strategic characteristics (interoperability, portability, cultural and linguistic adaptability, and accessibility) (see SD 9 clause 4).

Similarly, JTC 1 requires that an Explanatory Report be submitted with every Fast Track submission, and it must follow the same model used for a PAS submission.

**Please be sure to address the following Document Related Criteria when making any PAS or Fast Track submission to JTC 1.** The paragraphs follow the clause numbering in SD9 section 7.4.

# **About the Specifications**

FAPI 2.0 is is an API security profile based on OpenID Connect 1.0 and the OAuth 2.0 Authorization Framework and related specifications suitable for protecting APIs in high-value scenarios. While the security profile was initially developed with a focus on financial applications, it is designed to be universally applicable for protecting APIs exposing high-value and sensitive (personal and other) data, for example, in e-health and e-government applications.

# **7.4.1** **Quality** *(per the corresponding section in SD9)*

Within its scope the specification shall completely describe the functionality (in terms of interfaces, protocols, formats, etc.) necessary for an implementation of the submission. If it is based on a product, it shall include all the functionality necessary to achieve the stated level of compatibility or interoperability in a product independent manner.

Response:

The FAPI 2.0 specifications have been demonstrated to sufficiently describe the functionality needed to create interoperable implementations. Some examples follow.

The FAPI 2.0 Attacker Model defines the core security threats that inform the decisions on security mechanisms employed by the FAPI security profiles to mitigate attacks: security attacks by dishonest or malicious actors are defined and formal security verification ([here](https://openid.net/wordpress-content/uploads/2022/12/Formal-Security-Analysis-of-FAPI-2.0_FINAL_2022-10.pdf) and [here](https://openid.net/security-analysis-fapi-2-0-completed/)) is then run against a formal mathematical model, the Web Infrastructure Model, to formally prove the security of the FAPI 2.0 security profile against attacks.

The FAPI 2.0 Security Profile defines the core security requirements for API ecosystems in a zero-trust environment: authentication is built on top of the OAuth 2.0 and OpenID Connect 1.0

specifications and the use of Claims to communicate information about the End-User. It also describes the security and privacy considerations for using oAuth and OpenID Connect to allow untrusted third-party Relying Parties to gain access to an End-User’s protected resources. In comparison to FAPI 1.0 it presents further standardisation for improved interoperability, enhanced security, and a simplified implementation to make it easier to deploy secure API-first zero-trust ecosystems.

The FAPI Client Initiated Backchannel Authentication (FAPI-CIBA) specification profiles the OpenID Connect CIBA specification. The FAPI-CIBA specification by defines a mechanism for an OpenID authentication flow to be ‘’decoupled’’ by seperating the authorization flow initiated by the Relying (the Consumption Device) from the device used to authenticate the End-User (the Authentication Device) in a way that addresses the security properties of the FAPI 2.0 Security Profile and the risks defined by the FAPI 2.0 Attacker Model.

In this submission, “FAPI 2.0 specifications” and “FAPI 2.0 profile” relate to the group of specifications submitted in this report. Namely:

* The FAPI 2.0 Security Profile,
* The FAPI 2.0 Attacker Model, and
* FAPI-CIBA

# **7.4.1.1** **Completeness (M)** *(per the corresponding section in SD9)*

a) How well are all interfaces specified?

Response:

The FAPI 2.0 specifications have been demonstrated to sufficiently describe the functionality needed to create interoperable implementations. A few examples of these interfaces follow.

The FAPI 2.0 Security Profile specification defines the interface between Relying Parties (which are OAuth 2.0 Clients) and OpenID Providers/Authorization Servers (identity providers which authorize access to the protected resources of the Resource Owner) facilitated by the End-User authenticating and authorizing access with the Authorization Server. This authorization is used to grant third-party access to the Relying Party to access the End-User’s protected resources.

The FAPI 2.0 Attacker Model specification defines the common attacks which the FAPI 2.0 Security Profile seeks to ameliorate. It defines a collection of scenarios where a malicious actor seeks to compromise the OpenID/oAuth server. The FAPI 2.0 Security Profile then defines the additional security controls to prevent such malicious access.

The FAPI-CIBA specification defines a decoupled OpenID Connect authentication interface used by Relying Parties to initiate the End-User’s authentication with their OpenID Provider using an Authentication Device which is independent of the Consumption Device the Relying Party has initiated authorization from.

All of these and more interfaces are tested by the FAPI 2.0 and FAPI-CIBA Certification test suites at <https://openid.net/certification/>, resulting in interoperable implementations.

b) How easily can implementation take place without need of additional descriptions?

Response:

There are seven certified implementations of the FAPI 2.0 Security Profile and thirteen implementations of FAPI-CIBA. Underpinning the FAPI 2.0 Security Profile, there are demonstrably hundreds of certified implementations and almost certainly thousands of interoperable implementations, of the underlying specifications including OpenID Connect. The page <https://openid.net/certification/> lists many such implementations.

c) What proof exists for successful implementations (e.g. availability of test results for media standards)?

Response:

Per the OpenID Certification results at <https://openid.net/certification/>, there are over 7 certified FAPI 2.0 OpenID Providers, 13 certified FAPI-CIBA OpenID Providers, and 1 certified FAPI 2.0 Relying Parties.

# **7.4.1.2** **Clarity** *(per the corresponding section in SD9)*

a) What means are used to provide definitive descriptions beyond straight text?

Response:

The Certification test provide a cross-check that implementers have followed the specifications correctly. These tests are publicly available to all for free and can be run at any time.

Because the FAPI 2.0 Security Profile is a limited profiling of the oAuth and OpenID Connect specifications, no additional diagrams are included beyond the text-based specification. FAPI-CIBA presents implementation examples at <https://openid.net/specs/openid-financial-api-ciba-ID1.html#appendix-a---examples>.

b) What tables, figures and reference materials are used to remove ambiguity?

Response:

The FAPI 2.0 Security Profile and FAPI-CIBA specifications are profiles on top of a series of OpenID Connect and oAuth specifications. This profiling includes security properties that constrain optionality such as limiting allowable ciper suites, or restricting the sort of oAuth clients that can communicate with the Authorization Server to just confidential clients using specific authentication mechanisms. As such, no additional diagrams are provided in the FAPI 2.0 Security Profile specification because they are contained in the composite normative specifications. FAPI-CIBA presents implementation examples at <https://openid.net/specs/openid-financial-api-ciba-ID1.html#appendix-a---examples>. The composite normative specifications include diagrams and tables to illustrate protocol flows and relationships between components, such as the diagram at <https://openid.net/specs/openid-connect-core-1_0-34.html#Overview> and the tables at <https://openid.net/specs/openid-connect-core-1_0-34.html#Authentication>.

c) What contextual material is provided to educate the reader?

Response:

The OpenID Foundation Web site contains contextual information - especially the <https://openid.net/wg/fapi/> page providing papers and presentations.

# **7.4.1.3** **Testability (M)** *(per the corresponding section in SD9)*

The extent, use and availability of conformance/interoperability tests or means of implementation verification (e.g. availability of reference material for magnetic media) shall be described, as well as the provisions the specification has for testability.

Response:

Testing can be performed at the OpenID Certification site <https://openid.net/certification/>. The tests can also be run locally in a Docker container. Instructions on how to test and certify implementations are at <https://openid.net/how-to-certify-your-implementation/>. For instance, the instructions for running tests on FAPI 2.0 OpenID Providers are at <https://openid.net/how-to-certify-your-implementation/> and FAPI-CIBA Providers are at <https://openid.net/certification/fapi_ciba_op_testing/>. Instructions for running tests on Relying Parties are at <https://openid.net/certification/fapi_rp_testing/>. These tests exercise normative testable statements in the specifications and include “negative” tests to detect security flaws in implementations, such as failing to check signatures.

The specification has had sufficient review over an extended time period to characterise it as being stable. Further, formal security analysis of the FAPI 2.0 Security Profile has been conducated to verify the security properties in accordance with a formal mathematical model, which is available at <https://openid.net/fapi-2-0-announcement/>.

Response:

The primary [FAPI 1.0 Security Profile](https://openid.net/wg/fapi/specifications/) specifications became Implementer’s Drafts in 2022. They have been stable ever since. The FAPI 2.0 profile is an evolution of the FAPI 1.0 profile which has been final since 2022 and, like FAPI 2.0 is itself a highly secured OAuth profile that aims to provide specific implementation guidelines for security and interoperability and is built on top of stable specifications such as oAuth and OpenID Connect. OpenID Connect has been Final since 2014. We have applied errata corrections based on feedback from developers and deployers over the years but these do not change the meaning of the specifications. Final Versions of the FAPI 2.0 Security Profile specifications are expected to be made Final before December 2024. Those will be the basis for the PAS submissions.

# **7.4.1.4** **Stability (M)** *(per the corresponding section in SD9)*

a) How long has the specification existed, unchanged, since some form of verification (e.g. prototype testing, paper analysis, full interoperability tests) has been achieved?

Response:

FAPI 2.0 Security Profile is currently in a stable first-Implementer’s Draft. Certification testing began in 2023 and has continued ever since.

FAPI-CIBA is currently in a stable first-Implementer’s Draft since 2019. Certification testing began in 2019 and has continued ever since.

b) To what extent and for how long have products been implemented using the specification?

Response:

Products have been deployed in production for over a decade. Authlete, Cloudentity, Curity, PayPal, Surius Technologies, and Zerobank Design Factor all support the FAPI 2.0 Security Profile. In addition, Authlete, Cloudentity, Curity, Finansystech, ForgeRock, Glue, IBM, Ping Identity, Radiam, Red Hat, Surius Technologies, and WSO2 support the FAPI-CIBA specification. This is by no means an exhaustive list.

c) What mechanisms are in place to track versions, fixes and addenda?

Response:

The OpenID Foundation specification process includes tracking proposed errata issues and applying resulting errata corrections, after obtaining working group and Foundation-wide consensus. The working group uses an issue tracker to file, triage, and fix issues.

Both the FAPI 2.0 Security Profile and FAPI-CIBA specifications are at first-Implementer’s Draft. Final versions of both specifications are in final stages of completion and will be the basis of the PAS submission.

# **7.4.1.5** **Availability (M)** *(per the corresponding section in SD9)*

a) Where is the specification available (e.g. one source, multinational locations, what types of distributors)?

Response:

The specifications being proposed as the basis for the PAS submission are freely available at these locations:

* <https://openid.net/specs/fapi-2_0-security-profile-ID2.html>
* <https://openid.net/specs/fapi-2_0-attacker-model.html>
* <https://openid.net/specs/openid-financial-api-ciba.html>

Note that these are all currently draft specifications that are currently undergoing OpenID Foundation-wide review for approval. Once approved in 2024, these final versions will be the basis of the PAS submissions for those specifications. Those marked “-final” will not change.

b) How long has the specification been available?

Response:

The FAPI 2.0 Security Profile specification have been available since 2022 and FAPI-CIBA since 2019.

c) Has the distribution been widespread or restricted? (describe the situation)

Response:

OpenID Specifications are always publicly available for free to all at all times.

d) What are the costs associated with specification availability?

Response:

They can be downloaded by all at no cost at any time.

# **7.4.2** **Consensus (M)** *(per the corresponding section in SD9)*

The accompanying report shall describe the extent of (inter)national consensus that the document has already achieved.

Response:

The FAPI 2.0 Security Profile is used worldwide by at least hundreds of Identity Providers and at least thousands of Relying Parties. A number of national open data ecosystems use it, including Brazil and Australia’s ConnectID.

# **7.4.2.1** **Development Consensus** *(per the corresponding section in SD9)*

a) Describe the process by which the specification was developed.

Response:

The FAPI 2.0 specifications were developed in an OpenID Foundation working group. OpenID working groups are open to all who sign the IPR Contribution agreement, free of charge. A wide range of perspectives and use cases were represented in the working group discussions.

The process by which the specification was developed is documented in the [OpenID Process Document](http://openid.net/wordpress-content/uploads/2010/01/OpenID_Process_Document_December_2009_Final_Approved.pdf) and follows the terms of [“Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards” of WTO TBT Agreement](http://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm#annexIII).

b) Describe the process by which the specification was approved.

Response:

The specification approval process is described in Section 5 of the [OpenID Process Document](http://openid.net/wordpress-content/uploads/2010/01/OpenID_Process_Document_December_2009_Final_Approved.pdf).

There are three stages of an OpenID Specification, of which the FAPI 2.0 specifications follow – draft, Implementer’s Draft, and Final Specification. An OpenID Specification begins as a “draft” and retains this status until approved as an Implementer’s Draft. An Implementer’s Draft may be further revised, and any revised Implementer’s Draft is deemed a “draft” until it is approved as a new Implementer’s Draft. The most recent Implementer’s Draft may be approved as a Final Specification. There is no specific timeframe under which a draft must become an Implementer’s Draft or an Implementer’s Draft must become a Final Specification, although the WG should make reasonable efforts to conform to any posted schedule of deliverables on its Webpage. Only after it is ratified to be a Final Specification, the specification may use the title “OpenID”.

The process by which the specification was approved is documented in the [OpenID Process Document](http://openid.net/wordpress-content/uploads/2010/01/OpenID_Process_Document_December_2009_Final_Approved.pdf) and follows the terms of [“Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards” of WTO TBT Agreement](http://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm#annexIII).

c) What “levels” of approval have been obtained?

Response:

First, the working group and then the OpenID Foundation members approved Implementer’s Drafts of these specifications. These are versions providing IPR protections to implementers that are used for early deployments and interop testing. Then they were approved by the working group and Foundation as Final specifications. In some cases, errata corrections have been applied, which also require working group and Foundation-wide approvals.

# **7.4.2.2** **Response to User Requirements** *(per the corresponding section in SD9)*

a) How and when were user requirements considered and utilized?

Response:

Numerous OpenID Foundation workshops were held in conjunction with the specification development, which had broad participation from different constituencies. Usability and user requirements were among the workshop topics. The specification developers also applied user privacy feedback resulting from various national government data privacy and legal frameworks such as PSD2, GDPR, Australian CDR, Brazilian Open Finance.

b) To what extent have users demonstrated satisfaction?

Response:

FAPI 2.0 is largely considered “scaffolding” and not a consumer-facing brand or product. End-Users use it many times a day without knowing it. It underpins many national data sharing and action intiiation reforms such as Open Banking and Open Finance and it is the preferred security rails by many countries around the world. End-User services are built on top of these security rails that provide solutions to everday needs such as personal banking and finance. There is not a body of user complaints about it.

# **7.4.2.3** **Market Acceptance** *(per the corresponding section in SD9)*

a) How widespread is the market acceptance today? Anticipated?

Response:

Again, the list of adopters in 7.4.1.4 is only a small subset demonstrating FAPI 2.0’s broad market adoption. FAPI 2.0 being a successor to FAPI 1.0 relies on a migration option from existing FAPI 1.0 ecysostems which have deomonstrated significant market acceptance. The FAPI profile of standards are a demonstrated preferred choice for many countries when implementing Opend Data ecosystems with success in the UK, Australia, and Brazil amongst many other countries.

b) What evidence is there of market acceptance in the literature?

Response:

The FAPI Certification Program <https://openid.net/certification/> has certified hundreds of implementations. Searching the Web for “FAPI OIDF Guide” and “FAPI OIDF Tutorial” generates hundreds of millions of search results.

# **7.4.2.4** **Credibility** *(per the corresponding section in SD9)*

a) What is the extent and use of conformance tests or means of implementation verification?

Response:

The OpenID Foundation has developed a suite of open source conformance tests that can be freely run by anyone at <https://openid.net/certification/> by which developers that implement the FAPI profile of Specifications can test their deployment of its various profiles.

Developers who successfully complete the applicable conformance tests then qualify for self-certification of their compliance – a formal public declaration filed by an entity with the OpenID Foundation certifying that its specific identified deployment of the specification in a product or service meets the requirements of specified conformance profiles of the FAPI standard, as demonstrated by passing a set of self-administered conformance tests for those profiles. With self-certification, the organization implementing an FAPI deployment tests its own deployment via the OpenID FAPI Test Suite™ software and verifies that it conforms to one or more defined OpenID Connect profiles. Once the tests for a profile are successfully completed, the organization signs and submits to the OpenID Foundation a Certification of Conformance attesting that it successfully completed the software tests and asserting that its deployment conforms to the designated FAPI profile. Following submission of the required materials, the self-certifications are published.

The OpenID Foundation enables deployments of [FAPI](https://openid.net/wg/fapi/) to be certified to specific conformance profiles to promote interoperability among implementations. The OpenID Foundation’s certification process utilizes self-certification and conformance test suites developed by the Foundation.

Self-certifications are registered by the OpenID Foundation at<https://openid.net/certification/>.

Additional information about the OpenID Certification program include:

* The [certification instructions](https://openid.net/certification/instructions/) describe how to certify your deployments.
* [OpenID Certification Frequently Asked Questions (FAQ)](https://openid.net/certification/faq/)
* Certified OpenID Connect implementations are featured for developers at <https://openid.net/developers/certified/> and <https://openid.net/certification/>.

In addition, many national Open Data ecosystems that rely on FAPI for their security profile have their own certification programmes—such as the Australian Consumer and Cometition Commission’s Conformance Test Suite available at [https://www.cdr.gov.au/participant-conformance-approach](https://www.cdr.gov.au/participant-conformance-approach—leverage)—leverage, require, or integrate FAPI certification testing. Another example is Brazil’s Open Insurance regulator required FAPI Certficiation, evidence of which is available at <https://openid.net/certification/#FAPI-RP-BROFv2>.

b) What provisions does the specification have for testability?

Response:

The specifications are replete with normative requirements that conforming implementations must comply with and that are testable, both through interop testing and through conformance testing.

# **7.4.3** **Alignment** *(per the corresponding section in SD9)*

The specification should be aligned with existing JTC 1 standards or ongoing work and thus complement existing standards, architectures and style guides. Any conflicts with existing standards, architectures and style guides should be made clear and justified.

Response:

FAPI 2.0 uses these ISO standards:

* ISO/IEC Directives Part 2 – Pricniples and rules for the structure and drafting of ISO and IEC documents
* ISO/IEC 29100 Information technology - Security techniques – Privacy framework
* ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment

In addition many of the normative specifications that the FAPI 2.0 Security Profile and FAPI-CIBA specifications rely upon, such as OpenID Connect make further use of ISO standards.

The OpenID Foundation is not aware of any conflicts with existing JTC 1 standards or ongoing work.

# **7.4.3.1** **Relationship to Existing Standards** *(per the corresponding section in SD9)*

a) What International Standards are closely related to the specification and how?

Response:

The specification, via it’s normative references, uses many data structures and formats developed by International Standards bodies. It makes heavy use of JavaScript Object Notation (JSON), which is both an IETF and an ECMA standard. It uses HTTP, which is a widely-deployed IETF standard.

It uses these ITU-T standards:

* ITU-T Recommendation X.509 -- Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
* ITU-T Recommendation X.1252 -- Cyberspace security -- Identity management -- Baseline identity management terms and definitions

It uses these ISO standards:

* ISO/IEC 29115 -- Information technology - Security techniques - Entity authentication assurance framework
* ISO 3166-1. Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes
* ISO 639-1. Codes for the representation of names of languages -- Part 1: Alpha-2 code
* ISO 8601. Data elements and interchange formats - Information interchange - Representation of dates and times

b) To what International Standards is the proposed specification a natural extension?

Response:

It is an application of:

* OpenID Connect, which is undergoing PAS Submission to JTC 1
* ISO/IEC 29100 Information technology - Security techniques – Privacy framework
* ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment

It complements:

* ISO/IEC 29115 -- Information technology - Security techniques - Entity authentication assurance framework
* ISO/IEC 29184 Information technology — Online privacy notices and consent
* ISO/IEC 27556 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework
* ISO/IEC TS 27560 Privacy technologies — Consent record information structure
* ISO/IEC 24760-1 -- IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts
* ISO/IEC TS 29003 -- Information technology - Security techniques - Identity proofing

c) How the specification is related to emerging and ongoing JTC 1 projects?

Response:

FAPI can be used with:

* ISO/IEC 29100 Information technology - Security techniques – Privacy framework
* ISO/IEC 29134 Information technology – Security techniques – Guidelines for privacy impact assessment
* ISO/IEC WD 24760-4 IT Security and Privacy — A framework for identity management — Part 4: Authenticators, Credentials and Authentication
* ISO/IEC WD 27566-1 Information security, cybersecurity and privacy protection — Age assurance systems — Part1: Framework
* ISO/IEC WD 27566-3 Information security, cybersecurity and privacy protection — Age assurance systems —Part 3: Part 3: Interoperability, technical architecture and guidelines for use
* FIDO2 Authentication, which is believed to be undergoing PAS Submission to JTC 1.
* OpenID Connect, which is undergoing PAS Submission to JTC 1.

# **7.4.3.2** **Adaptability and Migration** *(per the corresponding section in SD9)*

a) What adaptations (migrations) of either the specification or International Standards would improve the relationship between the specification and International Standards?

Response:

No adaptations are called for.

b) How much flexibility do the proponents of the specification have?

Response:

FAPI 2.0 is designed to be extensible, which has proven to be a practical benefit of its architecture. By providing the baseline security properties for a secure API-based ecosystem, implementers make the choice of what additional usability properties are applied on top of it. Further, implementations have flexibility to determine how there requirements are defined, such as the business and application layers.

c) What are the longer-range plans for new/evolving specifications?

Response:

The OpenID Foundation has recently evolved FAPI 1.0 to the FAPI 2.0 profile. This is a result of feedback from many successful implementations of FAPI 1.0 globally with an effort to imrpove security, simplify usability whilst providing a higher degree of interioperability between Relying Parties and OpenID Providers. It is anticipated that FAPI 2.0 Security Profile will prove a sufficiently security profile more many years to come. That said, as described above, extensions can and are used to increase its reach to additional use cases via the exensible nature of its framework.

# **7.4.3.3** **Substitution and Replacement** *(per the corresponding section in SD9)*

a) What needs exist, if any, to replace an existing International Standard? Rationale?

Response:

No replacement is needed.

b) What is the need and feasibility of using only a portion of the specification as an International Standard?

Response:

No subsetting is needed.

c) What portions, if any, of the specification do not belong in an International Standard (e.g. too implementation-specific)?

Response:

No portions are too implementation-specific.

# **7.4.3.4** **Document Format and Style** *(per the corresponding section in SD9)*

a) What plans, if any, exist to conform to JTC 1 document styles?

Response:

The OpenID Foundation hopes to retain the existing document formatting and conventions. Given the thousands of implementations already based on the existing specifications, we believe that risks of inadvertent changes introduced during reformatting outweigh the potential benefits.

# **7.4.4** **Maintenance (M)** *(per the corresponding section in SD9)*

a) Have changes occurred on the subject of maintenance since the PAS Submitter application or renewal or, for a Fast Track, since the most recent submission of the standard? (This is the place to mention any particular agreement reached with a JTC 1 subgroup).

Response:

As described in 7.4.1.5, the FAPI 2.0 profile of specificiations are in first-Implementer’s Draft with a pathway to becoming Final before the end of 2024. Those corrected versions will be the ones submitted for PAS status.