FINANCIAL™
DATA EXCHANGE

Foundational Certification Model for Data Providers

Version 1.0
May 2021

Legal Notice

Financial Data Exchange, LLC (FDX) is a standards body and adopts this Foundational Certification Model for Data Providers for general use among industry stakeholders. Many of the terms, however, are subject to additional interpretations under prevailing laws, industry norms, and/or governmental regulations. While referencing certain laws that may be applicable, readers, users, members, or any other parties should seek legal advice of counsel relating to their particular practices and applicable laws in the jurisdictions where they do business. See FDX's complete Legal Disclaimer located at http://www.financialdataexchange.org for other applicable disclaimers.

Revision History

Document Version	Notes	Date
1.0	Initial Document Release This document was created as a result of FDX RFC 0116 and incorporates the full contents of the RFC for public release.	May 2021

Contents

1.0 Introduction

This document describes the model for the FDX Certification process, specifically the testing and methodology of the process. It includes the specific forms to use when applying for Certification as well as a description of performance monitoring and reporting.

Note that the requirements themselves are described in a separate document, Foundational Requirements for Data Providers.

The Certification process is separated into two categories, *Foundational Certification* and *Use Case Certification*. Foundational Certification applies to general function, performance, and security of the API implementation. Use Case Certification refers to functionality and performance of specific business use cases.

The Certification framework drives the following benefits for the open banking ecosystem:

- Reduces implementation time and costs
- Fosters widespread adoption
- Foundational API security requirements promote higher security
- Data quality, availability, and consistent terms and patterns improve user experiences
- Promotes Use Case compliance for interoperability and data minimization
- Reduces integration complexity via commonly understood integration practices

Both FDX members and non-members can apply for FDX Certification. The former may enjoy benefits such as reduced fees.

1.1 Scope

The FDX Certification qualifies an applicant against functional and performance requirements for one or more business Use Cases including a base set of requirements for function, performance, and security.

1.1.1 Foundational Verification

These are a base set of requirements that must be met to ensure the FDX API implementation is functional, secure, and operational. These are described in section 2.1 of the Foundational Requirements for Data Providers document, requirement numbers FR1 - FR4. These requirements are **minimally viable** rather than **optimal**, in that they provide minimum call and data compliance against a basic set of end points and data elements.

1.1.2 Use Case Certification

The following are the minimum requirements that an applicant must meet for a functional implementation against the defined business use case. The following use cases will be part of the test suite, once defined.

- PFM Use Case
- Credit Management and Servicing Use Case
- Money Movement Use Cases

Each use case defines the end points and data requirements that must be implemented and tested to qualify against that use case. Applicants may apply for certification of one or more use case.

1.2 Not in Scope

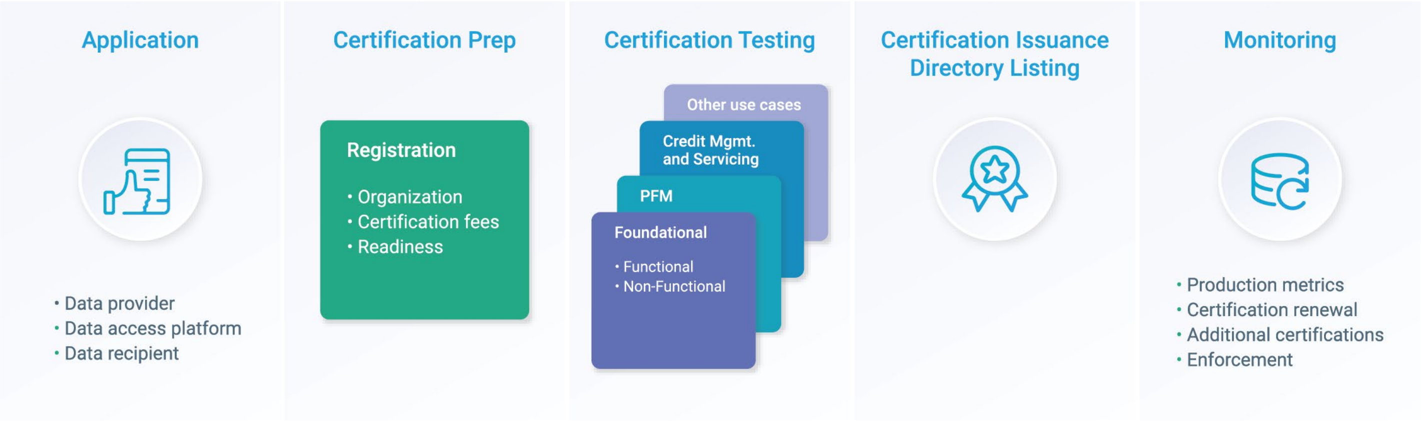
The FDX Certification program's current focus is ONLY on the technological certification.

Operational and organizational certification elements receive only as much consideration as necessary for cross referencing to other Certifications. They are also used to provide the relevant metadata, such as ensuring the applicant is a valid and a legal entity or to provide centralized references to industry accepted Certifications in a **central registry**.

The *Certification WG Charter Elaboration* document defines the following three items that comprise end-to-end Certification:

- Technological: Technologies, processes and systems for data (or feature) access
- Operational: Processes, policies and systems for data management within a firm including any secondary distribution of primary or derived data into that firm's own ecosystem
- Organizational: Legal and financial status of a firm

1.3 Process Summary



- Certification starts with an Application Form that collects the Certification Provider Applicant information, desired Certification level, relevant Use Cases, and applicable fees.
- The Certifier will review the Application information, setup the applicant on the Conformance Directory and schedule a Certification if the prerequisites are fulfilled.
- The Certifier performs all necessary Certification Test Cases for the requested Certifications and issues a pass/fail status. A fail status may be associated with a suggested remedy.
- “Certification Badges” of qualification are then issued and noted against the applicant in the registry. The Applicant is then deemed a Certified entity for the passed qualification criteria.
- The Certifier monitors the Certified Provider for ongoing obligations; production metrics, valid third party Certifications, implementation or spec updates, and member complaints to enforce the Certification requirements.

This is described in detail in the Certification process section below.

References

- Foundational Requirements for Data Providers
- Certification WG Charter Elaboration
- FDX Taxonomy of Permissioned Data Sharing

2.0 Certification Registry

A centralized registry with Certification status will be maintained for applicants that have applied for Certification.

2.1 Certification Registry Display

FDX Members will have the ability to view company details including FDX Certification status. In the main company details page, the Certification status will be displayed at a high level by Use Case, for example:

Use Case	Status	Link to Details
PFM	Show Badge	More Details >
Credit Lending	In Process	More Details >
Business Accounting	Show Badge	More Details >

Certification Status Definition

- **Supported** - The applicant supports the specified use case for all the applicable account types and products. The applicant also supports the use case for all required data elements. The certification badge is only granted for supported use cases. Some exceptions that may be permitted via the Conformance and Issue Review procedure.
- **Provisional Certification** - The applicant supports the specified use case. To maintain the provisional status, applicant must self report production monitoring data within specified timeframe. The terms provisional and full certification are to be used in the context of this document. These may be replaced by a better nomenclature for the sake of publishing the status externally.
- **Full Certification** - The certified entity has passed all criteria for provisional certification, and is now monitored by certifier. The terms provisional and full certification are to be used in the context of this document. These may be replaced by a better nomenclature for the sake of publishing the status externally.
- **In Process** - Certification is either underway or is pending fixes to achieve support
- **Incomplete** - Certification is complete but the functional requirements are incomplete. Common examples for an incomplete status include:
    - Missing account types or products with significant use case volume
    - Use Case Required fields with missing data

    - Availability of transaction history to support the use case
- **Not Supported** - The use case currently not supported by the company (may be in the future roadmap)
- **Not Applicable** - The use case is not applicable for the Provider, Data Access Platform or Recipient

Note that Foundational Verification must be complete for any use case to pass.

Exceptions/Considerations: The aim of certification is to incentivize a migration towards secure data sharing via tokenized APIs. To avoid dilution of the objective, the **supported** status is assigned only when the applicant meets the use cases for all applicable products and account types. However, an applicant may request an exception via the **Conformance and Issue Review Procedure** to be granted certification and a badge even when all relevant account types and products are not supported. The following are examples of situations in which an exception may be considered:

- *Multiple sites scenario*: Many providers have multiple end user secured login sites that separate products, account types and customer segments. A provider may choose to be FDX certified by one site at a time on the premise that other means of data access are not impact. Examples include:
    - Product portfolio is a white-labeled solution from a third party. These typically have a branded experience connected via SSO.
    - Within a data provider, there may be several customer facing sites as a result of acquisitions or platform consolidations.
    - Product and account types that target a distinctly different segment, for example commercial cards for enterprises that may be on a different site.
- *Digital service provider scenario*: Several data providers may be hosted on the same platform. The certification rules and exceptions apply for each data provider separately. The process may be facilitated by the digital service provider.
- *Low volume products:* Such product and account types do not form a significant share of the overall volume. For example, they are experimental, new to market, or are < 1% of the volume and allow a practical migration to the API.
- *End of life products*: Products that are in the process of being sunset and hence may not be part of the API.

2.2 More Details

A link to More Details > will be available for each of the use case that is included in the Certification Application. The Certification Use Case details page will include all the Account Categories (Deposits, LOC, Investments, etc.) and high level Certification areas. In cases where the Certification is "In Process", a high level summary will be available for members to view. The use case additional details page will match the outcome of the Certification Scorecard.

2.2.1 Example PFM More Details - Supported

Excerpt from FDX Certification Scorecard Spreadsheet

Account Category	PFM Requirement	Data Support	Normative	Notes
Deposit	CHECKING, SAVINGS	**Supported**		
	Required fields Covered	Supported	Yes	
	Transaction History (90+ days)	Supported	Yes	
		Supported	Yes	
LOC	CREDITCARD	**Supported**		
	Required fields Covered	Supported	Yes	
	Transaction History (90+ days)	Supported	Yes	
		Supported	Yes	
Loan	INSTALLMENT, MORTGAGE	**Supported**		
	Required fields Covered	Supported	Yes	
	Transaction History (90+ days)	Supported	Yes	
		Supported	Yes	
Investment		**Not Supported**		
Insurance		**Not Supported**		

2.2.2 Example PFM More Details - In Process

Excerpt from FDX Certification Scorecard Spreadsheet

Account Category	PFM Requirement	Data Support	Normative	Notes
Deposit		**In Process**		Foundational Verification Security requirement pending
	CHECKING, SAVINGS	Supported	Yes	
	Required fields Covered	Supported	Yes	
	Transaction History (90+ days)	Supported	Yes	
LOC		**In Process**		Foundational Verification Security requirement pending
	CREDITCARD*	Incomplete	Yes	*ABC Affinity Mastercard not supported
	Required fields Covered	In Process	Yes	All fields accept APR covered
	Transaction History (90+ days)	Supported	Yes	
Loan		**In Process**		Foundational Verification Security requirement pending
	All Account Type Supported	Supported	Yes	
	Required fields Covered	Supported	Yes	
	Transaction History (90+ days)	Supported	No	
Investment		**Not Supported**		
Insurance		**Not Supported**		

3.0 Certification Process

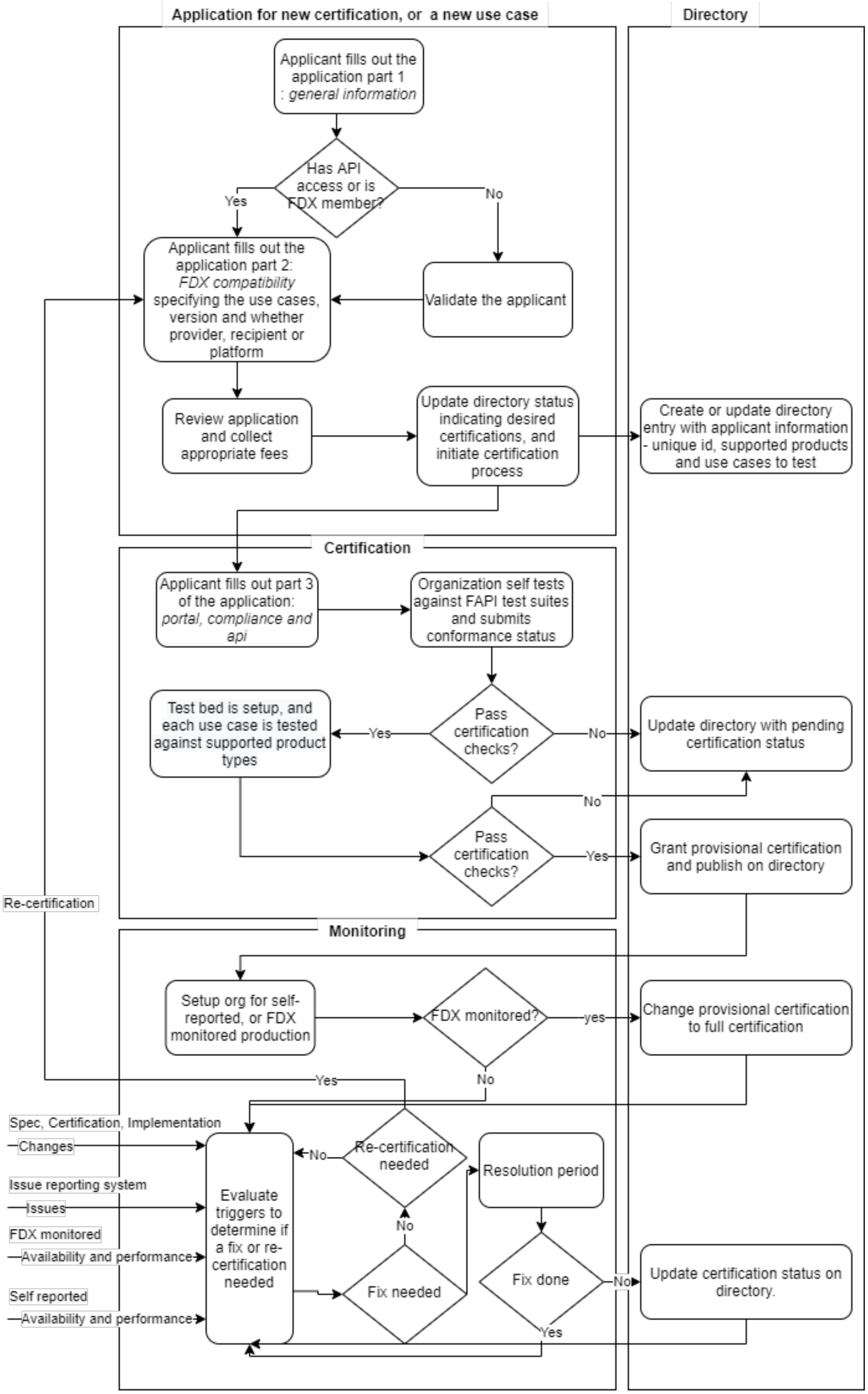

Application for new certification, or a new use case
Directory
Applicant fills out the application part 1 : general information
Has API access or is FDX member?
Yes
No
Applicant fills out the application part 2: FDX compatibility specifying the use cases, version and whether provider, recipient or platform
Validate the applicant
Review application and collect appropriate fees
Update directory status indicating desired certifications, and initiate certification process
Create or update directory entry with applicant information - unique id, supported products and use cases to test
Certification
Applicant fills out part 3 of the application: portal, compliance and api
Organization self tests against FAPI test suites and submits conformance status
Test bed is setup, and each use case is tested against supported product types
Yes
Pass certification checks?
No
Update directory with pending certification status
No
Pass certification checks?
Yes
Grant provisional certification and publish on directory
Re-certification
Monitoring
Setup org for self-reported, or FDX monitored production
FDX monitored?
yes
Change provisional certification to full certification
Yes
No
Spec, Certification, Implementation
Changes
Issue reporting system
Issues
FDX monitored
Availability and performance
Self reported
Availability and performance
Evaluate triggers to determine if a fix or re-certification needed
No
Re-certification needed
No
Fix needed
Resolution period
Fix done
No
Yes
Update certification status on directory.

Diagram 3.1: Certification Process Flow

Account Category	PFM Requirement	Data Support
3.1.1 Certification Request	The Organization "Applicant", submits a Certification request to the Certifier with the information in application form part 1 "Applicant General Information".	**Artifacts**: • Application form part 1 "Applicant General Information". **Outcomes:** • Entry is made in the conformance directory, noting the provided details and setting the 'Certification status' to 'Requested'. • Applicant gains access to pre-test automation package. The certification toolkit will be available to applicants so they can test their solution as much as possible before they enter the application process and incur the financial costs. Applicant is instructed to pay the fees, and fill out application form part 2 to proceed further in certification process, including gaining access to support.

Account Category	PFM Requirement	Data Support
3.1.2 Applicant Validation and Registration	• The applicant pays the applicable certification fees. • The applicant fills out application form part 2 “FDX Compatibility”. • Certifier validates the organization to ensure it is a real, legal entity. Certifier may request additional identification information to make an accurate assessment. • The following checks are performed: ○ Website check ○ OFAC check ○ Look up online and government records as necessary The registry record is updated with the requested certification information.	**Artifacts:** • Proof of payment. • Application form part 2 “FDX Compatibility” **Outcomes:** • Registry record now contains information on the requested certification details. • Certification status is set to “In review” when the process begins. If applicant fails validation, the Certification status is set to ‘rejected’ with the applicable reason.
3.1.3 Pre-Test	• The Applicant executes pre-test automation package. Results to be included in the Certification Application process.	**Artifact**: Pre-test Results.

Account Category	PFM Requirement	Data Support
3.1.4 Certification Scheduling	• Applicant provides application section 3 “Portal Information”, section 4 “API Interface”, and the pre-test results. • Certifier reviews the submitted information for completeness. Certifier updates the registry with the provided information, and puts the applicant on the certification schedule.	**Artifacts**: • Pre-test results. • Application part 3 and part 4. **Outcomes:** • Registry is updated with the provided information. • Certification status is set to “Scheduled”. If the certification is stopped for any reason, the status is set to “Pending”.
3.1.5 Certification Setup	• Certifier allocates the resources on the scheduled date. Certifier works with the Applicant to prepare the systems for the Certification.	**Outcomes:** The status is set to ‘In progress’.

Account Category	PFM Requirement	Data Support
3.1.6 Certification Testing	• Environment setup is verified and issues are addressed (commitment from Applicant required to expedite corrections to setup issues) • Certification Test Cases are executed • Results summarized into Completion Report If a non-passing result is reached, a prescribed period (*resolution period*) is allowed for corrections to be made by the Applicant. • A retest is executed once the issues are resolved. If a 2nd non-passing result is reached, findings are shared and the Certification process is stopped. Applicant can restart the Certification process after they have resolved all issues via returning to step 3.1.3 Scheduling. Additional fees may be required for restarting the tests. *Pausing of testing will return Applicant to step 3.1.3 to enable the Certification team to tear down the test environment and move onto the next Applicant in the queue. This will prevent a potentially long-running certification cycle.*	**Artifacts**: • Test environment, Test data. • Test cases. **Outcomes**: • Common open Issues list (e.g. JIRA). Completion report.

Account Category	PFM Requirement	Data Support
3.1.7 Certificate Issuance	A badge will be issued for each completed use case. There will also be 'FDX certified' badge issued if one or more use cases are supported. These will be displayed on the registry.	**Artifact:** • Test completion report **Outcomes:** • Certification details. • Certifications and badges, if granted. Certification is provisional on monitoring data.
3.1.8 Monitoring	Determination is made whether production monitoring data will be self reported, or measured by a third party e.g., FDX. If self-reported, the provisional status of the certification is maintained. If 3rd party monitored, FDX systems are set up collect the availability and performance data. After successful Initial Monitoring, the certification status changes to full certification. The production system will be monitored per the requirements in the monitoring section below.	**Artifact:** • Monitoring setup information. **Outcomes:** • Inclusion of monitored metrics in the registry. Removal of provisional badge if successful third party monitoring is implemented.

Account Category	PFM Requirement	Data Support
3.1.9 Re-Certification	Following events may trigger a re-certification request: • A new FDX version is available. • A new Provider Account Category or product is added for a certified use case. • Data Provider implementation has significant changes (Authorization or Data). • A new Use Case is applied for. • Organization fails to report the monitoring data. FDX will monitor impact of version updates, and notify the certified entities of the need of re-certification with the resolution timeframes. Addition of new products or account types, or implementation changes is community reported via the Service Desk. Ideally, the certified entity will inform FDX proactively of any such changes. Certified entity may apply for certification against a new use case. Appropriate resolution period is provided after which if the fix is not made, the issue is escalated per the process under Conformance and Performance Issue Review Procedure.	**Artifact:** • Service desk tickets. • FDX release. • Provider information submission (via Service desk) of changes in the implementation. • A certification request for a new use case. **Outcomes:** • Assessment report with a request for resolution. • Request for re-certification with a specified timetable. Escalation per Conformance and Performance Issue Review procedure.

4.0 Application Form - Certification Request

4.1 What it provides

The applicant provides information required for conformance directory, Certification, and registry:

- Certification request - The applicant provides information identifying the organization, providing the contact information, Certification fees and the desired Certification types.
- Application form - The applicant provides detailed information on their test setup, use cases, products, desired levels of Certification. Additional fees may be assessed at this stage depending upon the scope.
- Compliance information - The applicant provides information on their compliance with the relevant government and industry regulations. This information helps elevate their listing from conformance directory to being a part of the registry.

4.2 Contents

The application form is for organizations interested in becoming FDX Certified. The completion of the application form will initiate the certification process. The organization's ability to complete this application form will act as an indicator of an organization's capability of becoming FDX certified on some level. The application is used to establish the API Provider's legitimacy, technical capability, and regulatory obligations. The application form is in four sections, Applicant General Information, Portal Information, FDX Compatibility, and Compliance Information.

4.3 Application Form

Item	#	Applicant Information	Description	Public / Private
4.3.1. Applicant General Information	1.1	API Provider Name	Name of the organization that is providing the API	Public
	1.2	Other Known Names for API Provider	Other names the organization may be known by (Example: Truist, Suntrust)	Public
	1.3	API Provider Company Information	Brief description of the company.	Public
	1.4	API Provider Company Address	Address of headquarters	Public
	1.5	Legal ID	Company registration number	Private
	1.6	EIN(s)		Public
	1.7	URL	URL of main organization's website	Public
	1.8	Parent Company Name	Name of the parent company.	Public
	1.9	FDX Member Number	A unique identifier assigned to an FDX member	Private
	1.10	Application Point of Contact	The individual that will be the point of contact for the applicant company.	Private
	1.11	Contact info. for Point of Contact	The email and/or phone number of the individual that will be the point of contact for the applicant company. This field has the potential to contain PII.	Private
	1.12	Developer Portal URL	The URL for developer documentation.	Public

	1.13	API Recipient Reference	Name and contact method for reference. This will be used to add legitimacy to the company's existence. This is not to endorse APIs or API provider's performance.	Private
	1.14	Organization Type	Bank, Credit Union, Insurance company, Brokerage company	Public
	1.15	Logo	SVG logo	Public
		All required fields for registry v1 should be provided		
4.3.2. FDX Compatibility	2.1	FDX Version compatibility	Which version of FDX are you applying for/will be compatible with?	Public
	2.2	FDX Role	Choose one: Provider / Recipient / Access Platform	Public
	2.3	Certification Level	Accepted values are (only one): Use Case, Provider. Use cases below, this is dynamic. Based on choice, subsets of either Use Cases or Data Structures will display for further clarification. For instance, if Minimal is chosen, then Structures might display: Accounts, Transactions, Holdings. Choosing Use Case would display 3.4 below. Choosing Provider would display 3.4 below completely checked off.	Public

	2.4	Use Cases Supported ☐ PFM ☐ Move Money ☐ Tax ☐ Lending ☐ Accounting ☐ Fraud	Choose one or more: PFM, Move Money, Tax, Lending, Accounting, Fraud This is intended to be a dynamic field. When the use cases are selected, there will be additional fields generated based on the use requirements.	Public
	2.5	Account Categories available via API	Account Categories that the API data provider has data for via the API (Example: Account type coverage - Deposit, LOC, Investments, Insurance, etc. If a provider maintains multiple sites per Exceptions/ Considerations in section 2.1, this data must be provided per site. Please list account categories that are not supported and refer to section 2.1 for the acceptable Exceptions/Considerations.	Public

	2.6	Account Types	List of actual Account Types that are supported under each Account category. (e.g. Deposit - CHECKING and SAVINGS, Loans - MORTGAGE, LOC - CREDITCARD, Investments - 401k, IRA, 529, Roth, ESPP, etc.) as listed in the Conformance Directory. If a provider maintains multiple sites per Exceptions/ Consideration in section 2.1, this data must be provided per site. Please list account types that are not supported and refer to section 2.1 for the acceptable Exceptions/Considerations.	Public
	2.7	End User Secured Login Sites	A Provider may have several separate end user secured login sites. Examples include Retail, Private, Corporate and Commercial Banking. List the sites/URLs that are in scope (supported) as well as the sites that are out of scope (unsupported) for FDX Certification.	Public
4.3.3. Test Environment Information	3.1	Data Host (Resource Server)		Public
	3.2	Resource URI		Public
	3.3	Oauth Endpoint(s)	List of endpoint(s)	Public
	3.4	OIDC or OAuth2	A version of OAuth supported.	Public
	3.5	Authorize Information	Provide a link or a PDF copy of developer documentation.	Public

	3.6	Token information		Public
	3.7	Authorization Code expiry		Public
	3.8	Access Token Expiry		Public
	3.9	Refresh Token Expiry		Public
	3.10	Refresh/Authentication /Timing		Public
	3.11	Scopes/Data Clusters	Example: “readonly”, “accounts transactions”, etc. Data cluster coverage - Accounts, Transactions, Statements, Tax, etc.	Public
	3.12	TLS version supported	Must to be TLS v1.2 or higher	Public
	3.13	Portal availability	Need to establish if this is 24/7, only business hours (timezone?). This has huge implications for testing if not going through self-certification. The organization should ideally publish planned downtime/non-availability periods via API.	Public
	3.14	API Endpoints implemented		Public
	3.15	API Support Email	A generic contact for API recipients (Intended for API recipients)	Public
	3.16	API Support URL	A generic contact for API recipients (Intended for API recipients)	Public
	3.17	API Provider Company logo	200x200 Logo URL	Public

	3.18	Affiliated Brands Supported by API	Affiliated Brands the end-user would be familiar with or that is white-labeled that has data available in the API(Amazon Credit Card by ABC Bank).	Public
	3.19	Version swap outages	List of timeframes the Portal/QA region is inaccessible during a refresh (sometimes for days/weeks).	Public
	3.20	Auto/Manual dev setup	Online application & setup or manual form & email	Public
	3.21	MTLS requirements		Public
	3.22	IP White Listing requirements		Public
4.3.4. API Interface	4.1	Pagination	Yes or No	Public
		If Yes, what is the default and the page Limit (max number of transactions per response)		Public
	4.2	Days of look back Online	How many days worth of data is stored & accessible online?	Public
	4.3	Max Date Range	Widest data range for retrieving data in a single request (e.g., 30/60/90 days)	Public
	4.4	API field-level discrepancies	List known deviations from FDX standard.	Public

4.3.5. Compliance Information (Optional)	5.1	Name of regulating organization	What, if any, agencies the API provider reports to? (OCC, CPFM, FCA) The purpose of providing this information is to given assurance that the applicant has previously described their bona fides as a serious organization. Therefore the more information they can provide the better and for international organizations demonstrating that they have received certification from a non-US body is evidence that they are such a serious organization,	Public
	5.2	Nature of regulating organization	The applicant will select what kind of regulatory agency is presiding over them: 1. National governmental organization 2. International governmental organization 3. National industry organization 4. International industry organization	Public
	5.3	Name of any superior organization from which the regulating organization derives its legal or technical authority	For instance, in the UK, the Open Banking Implementation Entity derives its technical authority from the Financial Conduct Authority. But other industrial organizations may be self-perpetuating (that is derive their authority from their continuing activities).	Public

	5.4	Name of certification/compliance/conformance provided by regulating organization		Public
	5.5	Links to/copies of documents describing the certification/compliance/conformance provided by regulating organization		Public
	5.6	Links to/copies of documents providing the outputs from certification/compliance/conformance process		Public
	5.7	Date of certification/compliance/conformance process		Public
	5.8	Date of grant of certification/compliance/conformance if different		Public
	5.9	Date of expiry certification/compliance/conformance if different		Public

	5.10	Current status of certification/compliance/conformance	1. Fully compliant 2. Minor non-compliance 3. Major non-compliance 4. Other including information in the public domain on current or past disputes arising from non-compliance issues with regulating organization	Private

5.0 Conformance Monitoring and Issues Reporting

Certifiers will employ continuous active API monitoring to ensure that the certified entity is continually meeting the minimum certification requirements.

Further, the Certifier will monitor for items specified in re-certification requirements 3.1.9 to determine if a re-certification is necessary.

This section defines the methods and metrics for monitoring, as well as key reporting issues. Procedures for handling disputes and non-compliant events follow.

5.1 Summary

The following methods are to be employed after certification has been achieved:

- Production test accounts will be provided by all FDX certified members
- External, synthetic monitoring of endpoints will be used to ensure baseline performance of the key API scenarios
- Calls should be made using a suitable tool against a production endpoint with a test account
- FDX will convene a panel on an ad-hoc basis to review disputes and rule on remedial actions, if/when deemed necessary

Alternately, the certified entity may self-report the production monitoring data. Please see the sections below.

5.2 Production Monitoring

5.2.1 FDX Monitored

- Once the provider successfully completes certification in pre-production, they are granted provisional certification.
- After the software is deployed in production, FDX will validate that it is the same software. This may be done manually.
- Third party synthetic monitoring of performance and availability begins.
- After 30 days of reported metrics, the provisional condition is removed from the certification.

FDX will select a tool for monitoring key APIs and workflows. This tool will perform the following, at a minimum:

- Monitoring will be conducted against production APIs
    - Monitoring will occur regularly, such as every 5-15 minutes
    - Monitoring will occur over a core range of the functionality used by 3rd parties such as consent, authorization, and basic data interaction
    - Monitoring will involve calls made externally, in different parts of the country, and ideally involving different cloud data centers - care must be used when calculating the number of synthetic calls as a small percentage of real calls and appropriately spaced throughout the day
    - If in use, signing certificates will be stored securely and used to create JWT tokens where needed
- Metrics described in the FDX Foundational Certification Requirements Document
- The following metrics will be generated monthly:
    - Availability, based on the pass rate as defined in the Foundational Certification
    - Latency of calls based on the 95th percentile of calls, made from originating locations in different US regions/cloud data centers
    - Metrics will be compared to the agreed FDX standards
- Additional Metrics may be delivered to FDX for use in dispute resolution if needed
- Metrics will be available only to FDX staff for analysis.

5.2.2 Self Reported

- Once the provider successfully completes certification in pre-production, they are granted provisional certification.
- After the software is deployed in production, FDX will validate that it is the same software. This may be done manually.
- Data provider monitors their production instance for performance and availability to maintain the provisional certification. The metrics are reported to FDX with in six months of the successful use case certification.
- The provisional clause is removed when the data provider transitions to FDX monitored production environment, and metrics can be successfully collected for at least 30 days.

5.3 Reporting Requirements

FDX will provide a tool for 3rd party monitoring of key data points:

- Monitoring data will be gathered and processed centrally by FDX
    - Data will be reported for the membership using a tool selected and paid for by FDX
- FDX will manage a collection of production target accounts for use in the creation of synthetic API calls

The benefit of this approach is that real time availability metrics could be provided by FDX for members through the directory or similar.

Notes:

- FDX will use the data for internal purposes only and dispute resolution.
- Data on availability and performance could be made available to members of the FDX Conformance Directory
- If it is impossible for a provider to provide an account, FDX will provide a definition of the monitoring scope and provide a mechanism for reporting

5.3.1 Monitoring Standards

- A suitable tool will be configured to perform external synthetic queries against a defined set of endpoints to capture, at a minimum, the following:
    - Authentication/Consent Flows for the APIs
        - Exercising tokens and refresh tokens
    - Access to a set of defined API calls that should, at a minimum:
        - Get the user or account information/types available
        - Access data from an account such as a list of events/transactions or similar for a 24-hour period
- Frequency
    - A monitoring sequence to be conducted no more than every 15 minutes, ideally every 5 minutes, to ensure that availability metrics are accurate
- Production
    - Calls will be made to a live account on a production server
    - Data gathered is to be delivered to FDX on a monthly basis by the 5th of the month
        - Reporting method TBD (most likely via a portal to upload metrics)
    - Remediation will be based upon output or issues if any are determined
- Other items
    - Calls shall be made externally to production endpoints

    - Production security authorization shall be used and certificates used for signing purposes shall be stored appropriately

5.4 Conformance and Performance Issue Review Procedure

Should a dispute or issue occur between members concerning performance or conformance to FDX standards, a review committee will be convened comprising:

- A core of FDX employees and
- Non-involved members of the TRC, Certification, and Conformation committees (subject to agreement by parties)

The review committee will review the data delivered and rule on any actions to take. This may include the following:

- Determine the severity/importance of the event
- Confirm if an event has taken place and identify potential reason for the incident
- Provide data to parties to enable the development by them of a resolution plan
- Agree on a timetable for the next steps
- Review and verify conformance/performance has been *regained* or discuss resolution steps