Discussion Paper

Conformance framework options within Aotearoa New Zealand open banking

28 August 2026

paymentsnz®

Contents

1. Introduction

Aotearoa New Zealand's open banking ecosystem is built on a common set of technical, operational, security, and customer standards that enable organisations to exchange data and initiate payments in a consistent and secure way. While standards define the expected outcomes and behaviours, delivering those outcomes in practice depends on how those standards are implemented.

Conformance is the process of assessing whether implementations align with agreed standards. A conformance framework provides a structured way to identify implementation differences, support consistent outcomes across the ecosystem, and improve visibility of where standards or implementations may require further clarification or refinement. It is an important mechanism for supporting interoperability, reducing integration complexity, and promoting continuous improvement.

This discussion document proposes a potential approach to conformance for the open banking ecosystem of Aotearoa. It outlines:

- why a conformance framework may be valuable;
- the key components of a conformance programme;
- potential operating and remediation models;
- implementation options and international precedents; and
- recommendations intended to support industry discussion.

This document has been developed within the context of the API Centre's standards framework and current open banking standards. However, the concepts, principles, and approaches described are intended to help inform broader discussions about how conformance could operate within our country's evolving open banking and consumer data right landscape.

The purpose of this document is not to establish regulatory obligations or predetermined policy outcomes. Rather, it is intended to support discussion among industry participants, regulators, and other stakeholders by identifying practical options for improving implementation consistency, interoperability, and ecosystem outcomes over time.

2. Background and context

2.1 What conformance is and why it matters

For open banking to succeed at scale, participants need confidence that standards are being implemented consistently, securely and predictably. Conformance helps grow the trust, interoperability and confidence required for a healthy and sustainable open banking ecosystem.

Conformance is the process of assessing how implementations align with agreed standards. In the context of our country's open banking, it provides a structured way to evaluate implementation of the technical specifications, operational standards, and business rules that underpin the ecosystem.

Investing in conformance and generating consistent implementation provides measurable value across the ecosystem by enabling predictable outcomes, reducing integration complexity, and enabling a more consistent customer experience across the ecosystem.

Conformance also provides visibility of implementation differences. These differences may arise from varying interpretations, design choices, operational constraints, or ambiguity within the standards themselves. By identifying and understanding these differences, the ecosystem can determine whether implementation changes, further clarification, or future standards development is needed.

In this way, conformance acts as a continuous improvement feedback loop, helping to improve interoperability over time while recognising that some implementation variation may be appropriate. Ultimately, conformance supports trust in the ecosystem. It helps ensure that participants, regulators and customers can have confidence that open banking services will operate consistently and securely regardless of provider.

High levels of conformance benefit all ecosystem participants:

- **Accredited Requestors** benefit from more consistent integrations and reduced need for provider-specific handling.
- **Data Holders** benefit from clearer expectations, reduced ambiguity, and greater visibility of ecosystem-wide implementation differences.
- **Customers** benefit from more predictable and consistent experiences regardless of the providers they use.

2.2 Conformance vs compliance

Conformance is a subset of compliance. While compliance covers all regulatory and contractual obligations, conformance focuses specifically on alignment with the technical, functional, security, data, and customer standards.

Non-conformance with published standards is ultimately a compliance matter, since Standards Users have obligations to implement them. A conformance framework provides a collaborative pathway to identify and resolve issues before they need to escalate to the breach process.

2.3 Current state problem

The current ecosystem does not provide common tooling, test suites, or a structured process to validate implementations against the standards. As a result, a standards governance body in Aotearoa has no direct visibility of ecosystem-wide conformance. Conformance gaps can therefore exist without being surfaced or addressed through a common process. Commercial conformance tooling is used by some data holders however it does not provide an ecosystem-level view and reflects each organisation's own interpretation and implementation choices.

Where Accredited Requestors do encounter conformance differences, currently they raise them directly with the relevant Data Holder rather than through any central channel. There is no structured way to surface, track, or resolve issues across the ecosystem; problems get worked around bilaterally rather than fixed at the source.

The breach process is the only formal mechanism available. It serves as a blunt tool for handling routine conformance issues. This heavy compliance measure is intended for serious failures, not the everyday variations that comprise most conformance work. Relying solely on this pathway discourages collaborative reporting of variances and erodes trust.

Differences in how standards are implemented can create practical challenges for Accredited Requestors.

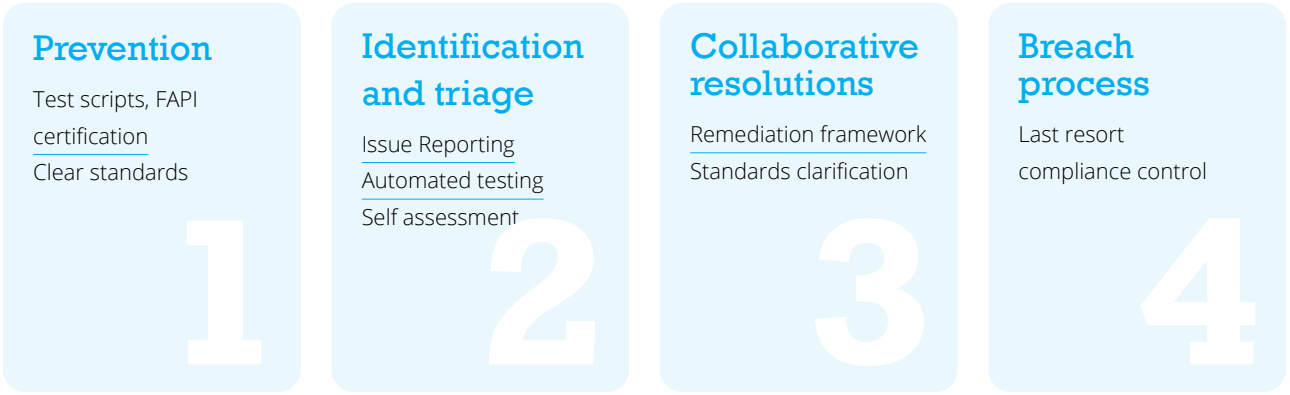
Where implementation approaches diverge from expected standard behaviour, Accredited Requestors may need to accommodate different outcomes through provider-specific integration logic, undermining the interoperability that standards are intended to deliver.

In summary:

- No ecosystem-wide tooling exists
- No central visibility into conformance state
- No structured channel for raising and resolving conformance issues; issues get worked through bilaterally
- The breach process is the only formal mechanism, which is disproportionate for most issues.

2.4 Conformance lifecycle

Conformance has a natural lifecycle, with four stages where issues can be prevented, caught, or resolved.



1. **Prevention** - clear standards, conformance test scripts, and FAPI certification. The goal is for issues to be designed out before they reach production.
2. **Identification and triage** - issue reporting workflow, automated testing, and self-assessment. Surface issues quickly when they do arise.
3. **Collaborative resolutions** - remediation framework, dispute resolution, and a standards clarification pathway. Resolve issues without needing to escalate.
4. **Breach process** - the existing API Centre breach process, used only when collaborative resolution has failed or where the issue warrants it on its own merits.

The intent of a conformance framework is for the bulk of activity to sit on the left of this flow. Each stage is about reducing the volume of issues that need to reach the next.

2.5 Why now

Conformance was considered a high priority in the API Centre work programme because:

1. **Ecosystem maturity** - when the ecosystem was small, investing in conformance infrastructure was a cost that felt unnecessary. With more implementations, integrations, and use cases, implementation inconsistencies now create real friction. The ecosystem has reached a scale where shared tooling and a structured channel make sense.
2. **A natural follow-on from existing work** - the Introduction to Conformance Assurance paper was presented to working groups in late 2025, socialising the concept and exploring what conformance means in the context of Aotearoa. There was broad acceptance that conformance would add value through better interoperability and reduced integration friction, and that it should apply to both Data Holders and Accredited Requestors. Three themes from those discussions are reflected in the positions taken later in this document: a focus on functional behaviour, recognition of test data challenges, and the need to size appropriately for the ecosystem of Aotearoa.
3. **Established continuous delivery within the eco-system** - standards development and implementation processes now enable a continuous feedback loop whereby conformance outcomes can flow back into prioritisation and delivery cycles within the standards body and Data Holder environments.

2.6 International precedent

Other open banking jurisdictions have already worked through similar conformance decisions. Appendix A summarises how the UK, Australia, and Brazil have approached this, and the recommendations later in this document draw on those precedents directly. The clearest examples are FAPI certification (Section 4.2), the choice of deployment model (Section 6.4), and the adoption of the UK Open Banking Implementation Entity (OBIE) conformance suite as a tooling foundation (Section 6.5).

2.7 Desired future state

The ultimate goal of conformance is not testing for its own sake, but improving the reliability, consistency and trustworthiness of open banking services for customers. A conformance programme addresses each of the gaps described above. The desired future state is one where:

Accredited Requestors can build once and integrate consistently.

- Unnecessary variation in how standards are implemented is reduced over time so that Accredited Requestors can rely on standard behaviours rather than coding for provider-specific differences. The ecosystem delivers on the interoperability promise that standards are intended to provide.
- **Conformance gaps are surfaced early and resolved before they become breaches.** Standards Users have a structured channel for raising and working through issues, so breach is a genuine last resort rather than the only available mechanism.

Standards Users can assess their own conformance.

- Standards Users have access to tooling, test suites, or structured guidance that supports validation of implementations against the standards. Conformance is something participants can proactively manage, not something that only surfaces when things go wrong.
- **Conformance is continuous, not a point-in-time exercise.** It becomes part of the implementation cycle, with automated tooling catching regressions early and reducing manual effort for both the API Centre and Standards Users.
- **The standards improve through feedback.** Conformance assessment reveals areas where the standards themselves are ambiguous, incomplete, or impractical. This feedback loop drives standards clarification and feature requests, improving the quality of the standards for everyone.
- **Customers benefit from a healthy ecosystem.** Conformance is work between Standards Users, but the end result is an open banking ecosystem customers can trust with their data and that delivers the new services and choices open banking promises to enable.

3. Proposed programme design

This section outlines what any programme to establish a conformance framework would need to cover and the principles that should guide it. A logical phased approach to how a conformance framework should be established is detailed in Section 4.

3.1 Scope

The work is proposed to assess conformance with the published open banking standards of Aotearoa. While elements of the proposal may be applicable agnostic of sector, the scope of this document is limited to open banking.

In scope

The programme assesses conformance across five categories. Each addresses a different aspect of implementation correctness.

Technical conformance validates that API implementations structurally align with published specifications.

- API request and response payloads match published OpenAPI specifications
- Data types, formats, and field constraints are correctly implemented
- Required fields are present; optional fields follow specification rules
- Error responses conform to the standard error format
- HTTP methods, status codes, and headers are correctly implemented.

Functional conformance validates that implementations behave correctly according to specified business rules and behaviours.

- Business logic is implemented as specified (for example, Consent state transitions)
- Features are complete and behave as documented
- Edge cases and error conditions are handled as specified
- Interactions between API resources follow documented patterns
- Requirements from the Customer Standard that govern the customer experience.

Data completeness validates that implementations support all required data types and value ranges.

- All required account types are supported
- Required data fields are populated (not just present, but containing meaningful data)
- Minimum date ranges for transaction history are met
- Enumerated values include all required options.

Security conformance validates that implementations meet authentication, authorisation, and encryption standards.

- Correct and complete implementation of the NZ Open Banking Security Profile
- Financial-grade API (FAPI) compliance
- Token handling (Access Tokens, Refresh Tokens) follows specification
- Certificate handling and mutual TLS implementation
- Consent authorisation flows function correctly.

Customer Standard conformance validates implementation of customer-facing requirements that sit outside the APIs themselves.

The programme applies to all Standards Users, however the ecosystem impact of implementation differences may vary depending on where those differences occur. For example a Accredited Requestor's non-conformance is usually rejected at the Data Holder boundary and stays contained. However an Data Holders implementation may have broader impact.

Conformance assessment covers alignment with:

- NZ Open Banking API Specifications (Account Information, Payment Initiation)
- NZ Open Banking Security Profile
- NZ Open Banking Customer Standard.

The scope above describes what can be raised as a conformance issue. The practical scope for testing (automated or not) will always be a subset.

Out of scope

- **Non-functional requirements** - response times, availability, and other performance metrics are covered by the existing Performance Standard
- **Contractual obligations** outside of the conformance standard itself, including the broader API Centre terms and conditions
- **Broader regulatory compliance** - obligations beyond the technical and functional standards.

3.2 Guiding principles

1. **Collaborative, not punitive** - The programme aims to help Standards Users achieve conformance, not to penalise them
2. **Sustainable focus** - Build a long-term programme that evolves with the ecosystem and feeds into existing change prioritisation and delivery frameworks
3. **Lightweight and proportionate** - avoid over-engineering; focus effort where it provides most value to the ecosystem rather than building infrastructure for its own sake
4. **Transparent** - Share learnings and improvements across the ecosystem
5. **Iterative** - Learn from manual processes before automating.

4. Implementation phases

Any programme to establish a conformance framework can be structured into phases. Each phase is intended to be valuable to the ecosystem on its own: if only the first one or two phases were completed, the ecosystem would still benefit from what was delivered.

4.1 Phase One: Develop the standard

Develop the conformance standard and operational processes. This phase is largely documentation and agreement.

The goal of this phase is to have a standard in place that can resolve conformance issues outside of any compliance obligations and breach processes.

- Develop conformance standard through the standards development process
- Design issue reporting workflow
- Agree remediation framework and timeframes with working groups
- Finalising the conformance standard and any applicable approval processes to approve the conformance standard
- Update any arrangements to distinguish and separate conformance issues from compliance breach processes.

Resourcing

- Standards development resources and working groups
- Legal counsel
- Governance consultation approval processes.

Phase One is complete when: the conformance standard is approved and published, the issue reporting process is live, and there is an agreed framework for handling reported variations.

4.2 Phase Two: Conformance test scripts and FAPI certification

This phase has two parallel tracks that can progress independently.

Track A: Conformance test scripts

Develop conformance test scripts alongside standards development. Written test scenarios that describe expected inputs, outputs, and functional behaviours.

The goal here is to bring value to the ecosystem early: Implementations can be tested against clear, agreed scenarios. The scripts also serve as the foundation for automated test cases in later phases. Because these would be an output of an approved and published standard, they can be generated at the end of the development cycle (post-publishing) as implementation support artefacts. They should support ecosystem users in the development of new standards implementations preventing conformance variations downstream.

While this focuses on new standards being developed, conformance issues that come forward from previous standard versions could also have tests retrofitted for them once expected behaviour is clarified and agreed amongst the ecosystem participants. Though the intention is not to retrofit everything right away.

Resourcing

- Standards development resources and working groups.

Track B: FAPI certification

Require FAPI certification for Data Holders through the OpenID Foundation. The FAPI certification tools already exist and this should be straightforward for the API Centre to implement.

The goal here is to increase trust in the security of the ecosystem. External certification of the security framework provides independent assurance that implementations meet an internationally recognised standard.

International precedent: UK Open Banking (OBIE), Australia (Consumer Data Right), and Brazil Open Finance have all certified against FAPI through profile adjustments where their local security profiles diverged from the base FAPI specification.

The NZ Open Banking Security Profile does not fully align with FAPI 1.0, and there is an ecosystem goal to move to FAPI 2.0. Until that alignment work is complete, certification against the standard FAPI profiles may not be possible without an adjustment.

So a two stage approach would be appropriate:

1. **Certification adjustment** - Get a certification profile or adjustment so that the current NZ Open Banking FAPI implementation can be certified without change. If possible, this is a relatively short path. There is precedent for this with existing international Open Banking implementations. But no research yet into what that would involve for Aotearoa.
2. **Security profile realignment** - For the next standards update (version 5.0) update the security profile to align with FAPI 2.0. Following this, OpenID certification will be able to run against the standard FAPI 2 profile.

Resourcing

- Standards development resources and working groups
- Data Holder technical staff for executing the conformance
- Engagement with OpenID Foundation for certification.

Phase Two is complete when: a published library of conformance test scripts exists and Data Holders have certification from OpenID for their FAPI implementations.

4.3 Phase Three: Functional testing - priority scenarios

Apply standardised automated conformance testing across the ecosystem, targeting the highest-priority functional scenarios first.

- Focus on key flows: Payments, Enduring Payments, and Account Information
- Include top conformance issues surfaced through Phases One and Two
- Potentially use scenarios developed in phase 2, but the key flows that already exist would be top priority.
- Select and implement testing infrastructure (with expandability as a core requirement)
- Agree representative test data standards
- Confirm deployment model.

The goal of this phase is to deliver automated testing for the highest-priority flows and resolve the remaining technical constraints (test account access, deployment model, and how automated findings feed into the operational framework from Phase One).

This approach does not call out schema validation as its own phase. Schema validation is implicit in functional testing (a response needs to match the spec to pass behavioural tests) but is not a goal in itself. The value is in testing whether implementations behave correctly, not just whether responses have the right shape.

Resourcing

- Standards development resources and working groups
- External testing expertise; likely requires a dedicated implementation partner for tooling and deployment
- Data Holder technical staff for executing the conformance tests.

Phase Three is complete when: Automated functional tests for the priority flows (Payments, Enduring Payments, Account Information) are running in production and the results are integrated with the Phase One issue reporting process.

4.4 Phase Four: Operationalise / Business as Usual (BAU)

Move conformance testing from project delivery into ongoing operations. The goal of this phase is the ongoing running of the conformance programme, with continuous improvement informed by what the ecosystem encounters in real implementations.

- Run a continuous conformance testing backlog for prioritisation, implementation, and continuous improvement
- Broaden test coverage to additional functional areas, informed by which areas generated the most conformance issues
- Expand edge case and cross-resource interaction testing
- Refine and improve existing test scenarios based on Phase Three experience.

Resourcing

- Standards development resources and working groups
- Ongoing operational resource.

This phase represents the BAU state of the conformance programme. Scope expands based on what the ecosystem needs, rather than a predetermined list. The priority is keeping conformance coverage and operational processes responsive to real issues and ecosystem feedback.

Phase Four is the ongoing operating state. A healthy BAU is one where conformance issues are routinely identified, prioritised through the continuous backlog, and resolved without being its own project.

From here the document splits into background material to explain our positions, offering up considerations as well as our initial recommendations.

5. Phase One detail

This section lists the considerations that the conformance standard and supporting processes will need to address in Phase One. The answers would need to be developed through the standards process and captured in the conformance standard itself.

5.1 Operating model

The conformance standard would fall under the category of operational standards. The items below describe the proposed operating model that the conformance standard would best exist under.

The operating model will address:

- **Operating principles** - the values that guide how the programme runs day to day (industry-led, consistent, adaptive, accountable)
- **Roles and responsibilities** - Standards governance body, Working Group, Working Groups, Data Holders, and Accredited Requestors; what each does and where the boundaries sit
- **Decision-making split** - which decisions the Standards governance body makes operationally, which require working group input, and which need formal approval
- **Dispute resolution** - how disputed findings are escalated and determined, and which working group handles which type of dispute
- **Programme evolution and change process** - how the programme changes over time, the change types, the approval path for each, and the review cycle
- **Reporting** - what reports the Standards governance body publishes, their frequency, and how confidentiality is preserved when aggregating

- **Records and documentation** - what is kept, for how long, and who has access
- **Relationship to other standards** - how the programme interacts with standards development, the existing compliance framework, and the Performance Standard.

5.2 Issue reporting process

The standard needs to define an issue reporting process that covers:

- **Reporting principles** - constructive intent, evidence-based, confidential handling, good faith engagement
- **Who can report** - Accredited Requestors, Data Holders, and the Standards governance body itself, and the contexts each typically reports from
- **What can (and cannot) be reported** - the conformance categories in scope, with clear redirects for issues that belong elsewhere (Performance Standard, security vulnerability disclosure, commercial disputes, feature requests)
- **Required and optional information** - what a report must contain to be assessable, and what supporting context helps
- **Reporting mechanism** - the system used (and how reports are submitted
- **Report lifecycle** - the workflow from submission through triage, validation, assignment, remediation, and closure
- **Severity classification** - the scheme used to prioritise and to inform remediation timeframes
- **Confidentiality** - reporter identity protection, issue detail handling, and aggregate reporting rules.

5.3 Remediation framework

The standard needs to define a remediation framework that covers:

- **Remediation principles** - reasonable timeframes, proportionate response, transparency, good faith, escalation as last resort
- **Remediation timeframes** - acknowledgement, target, and maximum extension by severity, agreed with the working groups
- **Remediation process** - the steps from issue assignment through investigation, fix, verification, and closure
- **Interim measures** - what can be agreed for critical or high-severity issues while a proper fix is developed
- **Extensions** - how Standards Users request more time, what they need to provide, and the limits on further extensions
- **Disputes and standards clarification pathway** - grounds for dispute, the determination process, and how the remediation clock is managed when a dispute is in progress
- **Escalation to compliance** - the indicators of failed collaborative resolution and the steps that move a matter into the formal breach process
- **Handling existing issues at programme launch** - how the backlog of pre-programme conformance issues is brought into the new framework without overwhelming Standards Users.

5.4 Required changes

A set of supporting changes will need to be made for Phase One to land:

- **Compliance governance arrangements** - update the compliance aspect of any governance framework that currently forces conformance issues into a breach process
- **Compliance standard / guidance** - update to reference the new conformance standard and clarify the boundary between conformance and breach
- **Issue reporting tooling** - configure tooling for the conformance issue type and lifecycle
- **Programme documentation and templates** - report templates, remediation correspondence templates, and internal triage / decision logs.

6. Testing approaches and recommendations

This section discusses the key decisions and recommendations for how conformance testing should work in the ecosystem of Aotearoa. In collaboration with the standard users, it provides the API Centre's recommended direction on each decision, intended as baseline discussion points for the industry to refine with MBIE, the governing standards body.

6.1 Functional testing

Conformance testing can target two different things: the structure of API responses (does the response match the published OpenAPI spec) or the behaviour of the implementation (does it handle a Consent state transition correctly). Both have a place, but they assure very different things. The first decision for the programme is which to lead with.

Schema validation is mechanical - it catches structural issues: missing fields, wrong types, malformed responses. It is necessary but not sufficient. An implementation can pass schema validation while still being non-conformant in ways that matter to the ecosystem: a Consent state that progresses incorrectly, an Enduring Payment that authorises outside its agreed parameters, an Account Information call that returns the right shape but the wrong data.

Functional testing validates the behaviours: state transitions, business rules, edge cases, cross-resource interactions. These are where ecosystem friction concentrates, because the response looks valid but the behaviour is wrong, and they are the conformance issues that actually surface in production and create work for Accredited Requestors.

This is why Phase Two Track A focuses on conformance test scripts rather than going straight to automated schema validation:

- Written scripts capture functional intent in a form that can be reviewed, agreed, and used directly by Data Holders, without waiting for tooling investment
- The act of writing a test script forces the standard to be specific. Ambiguities surface when someone tries to write the test, not when an issue is found in production
- Scripts written in Phase Two become the specification for automated tests in Phase Three. The behavioural intent does not need to be re-derived from the standards each time.

Schema validation is implicit in functional testing rather than a separate goal: a response that does not match the schema cannot pass a behavioural test that depends on it.

API centre recommended approach: Lead with functional testing via written conformance test scripts (Phase Two Track A). Schema validation is implicit in functional testing rather than pursued as a separate goal.

6.2 Security testing

Security testing has a different goal from functional or technical testing. Functional testing assures that an implementation does what it should do; security testing assures that an implementation cannot be made to do what it should not. A functional bug creates friction; a security bug breaks the trust the ecosystem depends on.

Our nation's open banking already depends on FAPI as its security foundation. The Security Profile (token handling, certificate management, authorisation flows, mutual TLS) is built on FAPI. This was chosen as FAPI is the international specification for financial-grade APIs, and adopting it gives Aotearoa a security model maintained by a much larger community than the ecosystem could resource alone. But that foundation only holds if implementations actually meet the specification.

FAPI certification is run by the OpenID Foundation, the body that defines the specification. Independence is what makes the certification meaningful. A body that doesn't operate the ecosystem it certifies sets a higher bar than internal testing could. UK Open Banking (OBIE), Australia (Consumer Data Right), and Brazil Open Finance all certify through this route, each using profile adjustments where their security profiles diverge from base FAPI. The tooling is mature and used in production at ecosystem scale.

The implementation path for Aotearoa is the two-stage approach set out in Section 4.2 Track B: a certification profile adjustment to certify the current NZ Open Banking Security Profile, then realignment to FAPI 2.0 with the v5.0 standards update.

API Centre recommended approach: Adopt FAPI certification through the OpenID Foundation as the security testing mechanism. Run it as a parallel track to the conformance test scripts in Phase Two, rather than building any specific security testing for Aotearoa.

6.4 Deployment model

Open banking APIs can't be tested the way a standalone public API would be. Open banking APIs operate within a trust framework: accessing account information requires a real or representative bank account, initiating a payment requires a valid funding source, and authorisation flows involve Customer interaction. Conformance testing cannot simply call endpoints from the outside and inspect responses.

In practice, this means testing depends on the right accounts being in place, populated with representative data (multiple account types, transaction histories with the required date ranges, consent scenarios at different lifecycle stages), and configured on the provider side.

The deployment model i.e. who runs the tests, where they run, and how the test data and infrastructure are managed, is the first decision shaped by this constraint.

Two broad deployment models exist:

Provider-hosted testing - the Standards governance body publishes the tooling and test scripts, and Data Holders run them within their own environments. The UK follows this pattern. The provider is responsible for executing tests and submitting results to the Standards governance body.

Centralised testing - the Standards governance body operates a central platform that tests Data Holders externally over the public APIs. Australia follows this pattern. The Standards governance body is responsible for executing tests; the Data Holder being tested grants test account access.

Provider-hosted gives up some central visibility, but the practical case for it is stronger:

- **Test data is set up by the people who know it.** The provider is best placed to maintain the representative data the tests need. A centralised tester would need ongoing access agreements and refresh processes to keep test accounts useful.
- **Configuration issues are easier to diagnose.** When a test fails, the cause is usually environment- or configuration-specific. The provider running the test against their own implementation can debug with full access to logs, internal state, and configuration. A centralised tester sees only the external response and has to coordinate with the provider to investigate.
- **It fits our country's scale and the Standards governance body's operating model.** Centralised testing requires the Standards governance body, or a delegated party, to operate ongoing technical infrastructure that runs against every Data Holder. The ecosystem of Aotearoa is too small for centralised scale to pay back the investment, and run a continuously-operating technical platform. Provider-hosted spreads the work: each provider runs the tests they need against their own environment, on their own schedule.

API Centre recommended approach: Provider-hosted as the default for functional and technical conformance testing. The Standards governance body publishes the tooling and scripts; Data Holders run them and submit results. Security certification via FAPI is also provider-initiated, executed through the OpenID Foundation's external service.

The trade-off (less direct Standards governance body visibility into how tests are run) is mitigated by the issue reporting process and the operational reporting in Phase One. Where centralised testing has clear value later for specific cross-provider scenarios, it can be added without re-doing the foundational work.

6.5 Build vs adopt

The Standards governance body does not need to build conformance tooling from scratch. The decision should be guided by:

- **Adopt where mature tooling exists.** Build only what is genuinely specific for Aotearoa. Bespoke tooling for problems that are already solved is not a good use of ecosystem effort.
- **Licensing must support modification and provider-hosted execution.** The tooling needs to be runnable by Data Holders in their own environments and modifiable by the Standards governance body, with no commercial restrictions that would limit how it is used or extended.
- **Keep the test corpus separable from the infrastructure.** The test runner is one thing; the scripts that encode our country's specific behaviour are another. Separating them keeps the corpus extensible without touching the underlying platform (see Tooling selection criteria).

For security conformance, the FAPI certification suite from the OpenID Foundation is a clear adopt: externally maintained, internationally recognised, and the existing precedent across UK, Australia, and Brazil.
For functional and technical conformance, the UK OBIE conformance suite is a specific option that fits all three criteria. It is open source under the MIT license, has been used in production at ecosystem scale for several years, and is actively maintained. The MIT license places no restrictions on use, modification, or redistribution. The codebase also separates the test runner infrastructure from the test scenarios, which is the structure we'd want anyway.

API Centre recommended approach:

1. **Adopt the OBIE suite as the foundation** - take the existing test runner, configuration model, certificate handling, and results capture as-is
2. **Replace the test scripts with specific scenarios for Aotearoa** - the infrastructure carries across; the behavioural tests are written against the standards of Aotearoa
3. **Contribute back upstream where appropriate** - general-purpose fixes and extensions go back to OBIE so the tooling of Aotearoa stays close to the maintained codebase; specific scripts for Aotearoa stay in our own repository.

This gets Aotearoa a working conformance test runner without building infrastructure, keeps the country's test corpus in the governing standards body control, and aligns naturally with the provider-hosted deployment model (OBIE is designed to run in the provider's own environment).

6.6 Tooling selection criteria

Tooling decisions made in Phase Two and Phase Three must accommodate the full priority list, not just the first use case.

- **Tooling must be extendable across the testing priority list** - the scope of what gets tested expands over phases, from schema-level checks through to behavioural and cross-resource scenarios. Tooling chosen for the first use case must be capable of carrying the later ones. Schema-only tooling that cannot be extended to functional behaviour would create a false economy.
- **Test scripts must be extendable without per-change cost** - if external software is engaged to deliver the tooling, the test scripts themselves must be authorable and extendable by the Standards governance body (and other

ecosystem participants where appropriate) without the supplier needing to do and bill for every addition. The test corpus belongs to the ecosystem, not to a vendor.

- **Representative test data standards** - provider-hosted testing depends on providers maintaining representative data within their conformance environments. The programme needs an agreed baseline for what "representative" means (account types, transaction history depth, consent lifecycle states) so tests run against comparable conditions across the ecosystem.

6.7 Recap

The recommendations below summarise the API Centre's proposed starting point for industry discussion and further refinement.

- **Functional testing first.** Use written conformance test scripts to capture expected behaviours, with schema validation treated as part of functional testing.
- **Security via FAPI certification.** Use OpenID Foundation certification, starting with a profile adjustment and moving to FAPI 2.0 alignment in v5.0.
- **Provider-hosted testing by default.** Publish tooling and scripts for Data Holders to run in their own environments and submit results.
- **Adopt OBIE and tailor the test corpus.** Use the UK Open Banking suite as the tooling foundation and replace test scripts with specific scenarios for Aotearoa.
- **Select extendable tooling.** Ensure scripts can be maintained by the Standards governance body and supported by agreed representative test data.
- **Keep investment proportionate.** Scale automation to our country's ecosystem needs, rather than replicating larger jurisdictions.

Overall, the proposed direction is behaviour over schema, mature tooling where practical, testing where data is best managed, and investment sized to the ecosystem of Aotearoa.

Appendix A: international conformance approaches

Other open banking jurisdictions have implemented conformance programmes at varying levels of maturity. Their experience provides reference points for Aotearoa.

Jurisdiction	Approach	Automation	Key observation
UK	Open-source conformance tools run by providers, plus FAPI certification	High	Provider-hosted model; separation of functional, security, and CX testing
Australia	Centralised automated suite as a gateway to activation	High	Fast execution (~1 hour); mandatory pre-activation gate; scale closest to Aotearoa
Brazil	Sandbox testing, FAPI certification, and daily production monitoring	Very high	Sandbox alone is insufficient; production drift is a real problem

Several themes emerge:

- **FAPI certification is a common thread across mature jurisdictions.** Rather than building bespoke security testing, the UK, Australia, and Brazil all leverage the existing FAPI conformance suite.
- **Sandbox-only testing has limitations.** Brazil's experience shows that APIs passing sandbox testing can drift in production. Their response was daily automated production monitoring.
- **Australia's scale is closest to Aotearoa.** Their automated suite runs in approximately one hour and serves as a mandatory gateway. This demonstrates meaningful automation is achievable in a smaller ecosystem.
- **Deployment models vary.** The UK uses provider-hosted; Australia and Brazil use centralised platforms. The differences reflect trade-offs in visibility, access, and ecosystem scale.

paymentsnz.co.nz

Discussion paper on conformance framework options for open banking in Aotearoa New Zealand

paymentsnz®