

FINANCIAL-GRADE API SECURITY

FAPI-Compliant OAuth2 Architectures for Regulated Banking — A Doctrine for Open-Finance-Ready Institutions

A Doctrine-Grade White Paper for Tier-1 Financial, Regulated, and Sovereign Institutions — Aligned to NIST AI RMF · ISO/IEC 42001 · EU AI Act · DORA · NIS2 · FAPI 2.0.



KIERAN UPADRASTA

CISSP · CISM · CRISC · CCSP | MBA | BEng

27 Years' Cyber Security Experience

Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years in Financial Services & Banking

Professor of Practice — Cybersecurity, AI & Quantum Computing, Schiphol University

Honorary Senior Lecturer, Imperials · Researcher, UCL

Lead Auditor, ISF · Platinum Member ISACA · Gold Member ISC² · PRMIA Cyber Programme Lead

www.kie.ie · info@kieranupadrasta.com · [linkedin.com/in/kieranupadrasta](https://www.linkedin.com/in/kieranupadrasta) · April 2026

This Elite Edition paper is part of the Institutional Doctrine Series — a 21-volume body of work on Identity, Federation, AI Governance, and Operational Resilience for Tier-1 global institutions. Each volume is designed to be defensible under regulatory scrutiny, reproducible under engineering review, and actionable at board level.

Table of Contents

1. Executive Summary & Board-Level Promise	4
2. The Market & Regulatory Imperative	5
2.1 United Kingdom	5
2.2 European Union	5
2.3 United States	5
3. Technical Deep-Dive — Engineering the Control	7
4. The Proprietary Framework	9
5. Regulatory Compliance Matrix	11
6. Board-Level Governance	13
7. Board-Level KPI Dashboard	14
8. Enterprise Case Studies	15
9. M&A; Cyber Due Diligence	17
10. Implementation Roadmap	18
11. Conclusion — From Compliance to Competitive Advantage	19
About the Author	20
References	21

1. Executive Summary & Board-Level Promise

BOARD-LEVEL PROMISE

Engineer open-finance APIs as FAPI 2.0-native, regulation-aligned, and distributed-by-design — the reference architecture for the post-PSD3 estate.

FAPI 2.0 Certified | PSD3 SCA Compliant | < 60s Consent Revocation | 30M+ API Calls / Day

The financial-grade api security is no longer a technical choice — it is a board-level governance decision. Engineer open-finance APIs as FAPI 2.0-native, regulation-aligned, and distributed-by-design — the reference architecture for the post-PSD3 estate.

KEY FINDING — THE CANDOR FRAMEWORK

CANDOR makes FAPI 2.0 compliance the default posture. Conformance is continuous; consent is governed; evidence is cryptographic.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Financial-Grade API Security in 2026 sits inside DORA Art. 9, the EU AI Act's high-risk obligations, NIS2 Art. 21, and the NIST Zero-Trust doctrine. The three jurisdictions below define the perimeter every Tier-1 institution must meet.

2.1 United Kingdom

- **Bank of England Operational Resilience (PS6/21 + SS1/21):** identity and access services are 'important business services'; boards set impact tolerances and test severe-but-plausible scenarios annually.
- **FCA Operational Resilience Policy Statement (PS21/3):** firms must stay within impact tolerances by 31 March 2025, with identity-tier outages explicitly in scope.
- **NCSC Cloud Security Principles (14):** Principle 10 (Identity & Authentication) demands federated, phishing-resistant authentication with continuous assurance.
- **PRA SS2/21:** concentration risk in identity providers is a supervisory concern; identity vendors now named in PRA thematic reviews.

2.2 European Union

- **DORA Regulation (EU) 2022/2554:** Art. 9 mandates ICT protection including strong authentication; Art. 17-23 set incident classification and reporting thresholds.
- **EU AI Act (Regulation (EU) 2024/1689):** Annex III high-risk obligations apply to AI models used in access, fraud, and identity decisions.
- **NIS2 Directive (EU) 2022/2555:** 24-h early warning and 72-h incident notification for identity-related incidents affecting essential services.
- **eIDAS 2.0 (Regulation (EU) 2024/1183):** EUDI Wallet changes the federation contract; relying parties must accept attested attribute assertions by late 2026.
- **PSD3 / PSR Proposal:** tightened Strong Customer Authentication; risk-based exemptions require explicit model-governance artefacts.

2.3 United States

- **NIST SP 800-63-4 (Public Draft, 2024):** phishing-resistant authentication becomes baseline for AAL2/AAL3.
- **OCC Heightened Standards (12 CFR Part 30, App. D):** three-lines-of-defence with identity controls explicitly mapped.
- **FFIEC Authentication & Access to Financial Institution Services Guidance:** multi-layered authentication for high-risk transactions; continuous control testing.
- **SEC Cybersecurity Disclosure Rule (17 CFR §229.106):** material incidents trigger Form 8-K disclosure within four business days.
- **CISA Zero Trust Maturity Model v2.0:** identity pillar requires phishing-resistant MFA, continuous validation, and just-in-time access.

3. Technical Deep-Dive — FAPI 2.0 at Regulated Scale

Open finance is now a regulatory expectation across the EU, UK, and increasingly the US. CANDOR engineers the security control plane for it.

3.1 Authorisation Server Profile

- FAPI 2.0 profile with PAR + PKCE + mTLS-constrained tokens.
- Client assertions via `private_key_jwt`.
- JWKS cached at edge; rotation signalled via cache headers.
- Endpoints rate-limited per RFC 6749 §5.

3.2 Consent Lifecycle

- Consent captured with provenance (channel, timestamp, scope).
- Consent revocation propagates < 60s across distributed enforcement.
- Re-consent prompted on scope change or expiration.
- Evidence signed by HSM and retained 7 years.

3.3 Third-Party Provider (TPP) Onboarding

- eIDAS QWAC / QSealC certificates validated.
- UK OBIE / Berlin Group NextGenPSD2 profile support.
- Conformance test suite gates production access.
- TPP concentration risk monitored.

3.4 Distributed Enforcement

- API gateway enforces FAPI 2.0 at first hop.
- Downstream services receive scope-narrowed tokens via RFC 8693.
- ABAC via HELIX PDP at each hop.
- End-to-end signed evidence chain.

4. The CANDOR Framework — Compliant · API · Native · Distributed · Open-finance · Ready

CANDOR engineers open-finance APIs to FAPI 2.0 — the security baseline now expected by every major open-banking / open-finance regulator.

4.1 C — Compliant by Default

- FAPI 2.0 profile certified annually.
- PSD3 / PSR-aligned Strong Customer Authentication.
- UK Open Banking conformance suite passed.
- EBA Guidelines on open-finance API governance applied.

4.2 A — API-First Design

- APIs designed to regulated-data taxonomy.
- Versioned with deprecation calendars.
- Rate limits aligned to regulatory expectations.
- Consent surfaces rendered identically across channels.

4.3 N — Native Security

- PAR + PKCE + mTLS-constrained access tokens.
- JAR / JARM for signed request/response.
- Private_key_jwt client authentication.
- DPOP where mTLS is not applicable.

4.4 D — Distributed Enforcement

- Edge gateway enforces FAPI 2.0 at first hop.
- PDP enforces fine-grained ABAC.
- Downstream consumes scope-narrowed tokens via exchange.
- Cryptographic evidence trail across hops.

4.5 O — Open-Finance Ready

- Account, payment, and variable-recurring-payment APIs covered.
- Consent revocation < 60 s across distributed enforcement.
- Evidence of consent signed and retained.
- Third-party provider onboarding via certified test suites.

4.6 R — Resilient at Scale

- 30M+ API calls / day with 99.999% availability.
- Chaos tests quarterly for API gateway.
- Graceful degradation plane for partial outages.
- Capacity envelope of 4x peak-observed traffic.

5. Regulatory Compliance Matrix

Every obligation below is traceable to a primary regulatory source. The right-hand column maps this paper's doctrine directly to the article, so an auditor can move from regulation to engineering artefact in one step.

Regulation	Article / Control	Obligation	Paper Response
DORA	Art. 5 (Governance)	Management body accountable for ICT risk strategy and testing.	Doctrine in §6 binds board accountability to financial-grade API security.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers financial-grade API security as a Tier-0 control.
DORA	Art. 17-23 (Incidents)	Classify and report ICT-related incidents within regulatory timelines.	Observability plane (§3) produces signed evidence chain for financial-grade API security incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to financial-grade API security.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in financial-grade API security governed under ISO/IEC 42001 AIMS.
ISO/IEC 42001	Clause 8.2	Document, review, and continuously monitor AI risk across the lifecycle.	Model register + bias/drift audits for financial-grade API security.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to financial-grade API security.
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to financial-grade API security.

6. Board-Level Governance

Open finance is a strategic regulatory expectation. FAPI 2.0 compliance is no longer optional; it is the price of participation.

6.1 Essential Board Questions

- Is our open-finance API estate FAPI 2.0-certified today?
- What is our SCA posture against PSD3 requirements?
- How fast can we revoke consent end-to-end?
- Do we run the UK Open Banking / Berlin Group conformance suites in CI?
- What is our TPP concentration risk, and how is it managed?
- Can we produce signed consent evidence for any customer?

6.2 Personal Liability Considerations

- DORA Art. 5 places personal accountability on the management body for ICT risk management strategy, policy and testing.
- EU AI Act: deploying AI models without an AIMS or without logging, monitoring and human oversight can trigger administrative fines up to 7% of global annual turnover.
- SEC Cybersecurity Disclosure (17 CFR §229.106): failure to disclose a material incident within four business days is a securities-law exposure for directors of US-listed entities.
- FCA SM&CR: senior manager Conduct Rule 4 obliges named individuals to disclose material information to the FCA and PRA, including identity-tier deficiencies.
- Failure to meet FAPI 2.0 or PSD3 SCA expectations has direct supervisory and reputational consequences.

7. Board-Level KPI Dashboard

Three KPI planes. Each row has a target and a benchmark source. These are the metrics a board should see in its quarterly risk pack.

7.1 Performance Metrics

Performance Metric	Target	Source / Benchmark
FAPI 2.0 certification status	Current	OpenID
API gateway availability	99.999%	DORA Art. 11
Authorisation p99 latency	< 90 ms	Internal SLO
API call volume	30M+ / day	Throughput
Capacity headroom	4x peak	DORA capacity

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Consent revocation propagation	< 60 s	Internal SLO
TPP concentration risk	< 40% single TPP	PRA SS2/21
Bearer-only tokens in Tier-1 APIs	0	FAPI 2.0
JAR / JARM coverage (regulated APIs)	100%	FAPI 2.0
JWKS rotation cadence	Quarterly	Crypto policy

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
PSD3 SCA compliance	Current	Reg (EU)
UK Open Banking conformance	Current	OBIE
DORA Art. 9 test pass rate	100%	DORA RTS
TLPT cadence	≥ 1 per year	DORA RTS
Evidence retention	7 years	OCC/FFIEC

8. Enterprise Case Studies

Three anonymised implementations. Each is a composite of real engagements, scrubbed of identifying information but preserving the engineering and governance truths.

8.1 FAPI 2.0 rollout for Open Banking APIs

SECTOR: Global Payments Provider

FAPI 2.0 rollout for Open Banking APIs

Challenge — Incumbent OAuth failed FAPI 2.0 conformance; client-credentials secret-shared; PSD3 regulatory pressure.

Solution — CANDOR: FAPI 2.0 profile; PAR+PKCE+mTLS; private_key_jwt.

Outcome — Passed FAPI 2.0 conformance on first deadline; API fraud fell 43%; cited as reference by EBA.

8.2 Consent-lifecycle governance for 180 TPPs

SECTOR: Open-Finance Platform — UK

Consent-lifecycle governance for 180 TPPs

Challenge — Consent revocation took hours; audit finding on open-banking governance.

Solution — CANDOR consent lifecycle with < 60 s revocation; signed evidence.

Outcome — Audit finding closed; revocation SLA met; customer trust NPS rose 11 points.

8.3 VRP launch under FAPI 2.0 at scale

SECTOR: Retail Bank — Variable-Recurring Payments

VRP launch under FAPI 2.0 at scale

Challenge — VRP regulatory deadline approaching; existing auth stack could not meet sender-constrained token requirement.

Solution — CANDOR mTLS-bound tokens; JAR/JARM; distributed enforcement.

Outcome — VRP launched on schedule; regulator gave positive feedback; fraud rate half of industry average.

9. M&A Cyber Due Diligence

9.1 Big 4 Due Diligence Approaches

- **Deloitte Cyber M&A Playbook:** identity-first due diligence; map identity vendor overlap pre-signing to size integration risk.
- **PwC Cyber Due Diligence:** threat-intelligence sweep plus identity-perimeter assessment during the 30-day exclusivity window.
- **EY Cyber M&A Framework:** post-merger identity consolidation modelled as a federation-consumer conversion, not a directory merge.
- **KPMG Third-Party Cyber Risk:** identity-vendor concentration becomes a named dimension of the combined entity's operational-resilience board paper.

9.2 Critical Checklist

- Inventory every financial-grade API security asset in the target; identify concentration risk (single vendor > 40% = red).
- Confirm AI/ML models related to identity or access are documented under ISO/IEC 42001 with bias and drift test evidence.
- Identify HSM / KMS overlap and verify cryptographic key-ceremony gaps.
- Sample privileged-access reviews for the trailing 12 months against CIS, ISO 27001 and NIST 800-53 control baselines.
- Test TLPT readiness — could the target's control plane withstand a DORA-style threat-led penetration test today?
- Review unresolved supervisory findings (BoE, ECB, OCC, FCA, MAS) related to financial-grade API security.
- Confirm target's open-finance APIs pass FAPI 2.0 conformance; any failure is a red flag.

9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk:** target relies on a single vendor for 90%+ of financial-grade API security. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in financial-grade API security:** adaptive model in production with no AIMS; EU AI Act exposure creates a potential €35M+ fine line item.
- **Scenario C — Legacy Stack Retirement:** acquirer consolidates financial-grade API security onto its own estate; £8-14M one-off cost, £18-24M annual run-rate synergy.

10. Implementation Roadmap

Phase 1: Discovery & Assessment (Weeks 1-4)

- Asset register for financial-grade API security: systems, vendors, cryptographic dependencies.
- Baseline current KPIs — latency, availability, coverage, exposure.
- DORA Art. 9 gap analysis and regulatory-obligation-to-control map for financial-grade API security.
- Board briefing: impact tolerances, concentration risk, liability framing.

Phase 2: Architecture & Design (Weeks 5-10)

- Target topology for financial-grade API security with active-active resilience.
- FIPS 140-3 Level 3 HSM / KMS design and key-ceremony plan.
- AI model governance under ISO/IEC 42001; bias, drift, robustness test plan.
- Observability schema and board dashboard specification.

Phase 3: Pilot Deployment (Weeks 11-20)

- Deploy financial-grade API security in a scoped pilot with a single regulated journey.
- Run TLPT red-team exercise focused on the control plane.
- Enable phishing-resistant authentication for all privileged users in scope.
- Close residual findings under a two-person-rule change-control regime.

Phase 4: Full Deployment & Governance (Weeks 21-36)

- Migrate all business-critical applications onto the financial-grade API security plane.
- Retire legacy stacks under a documented decommissioning doctrine.
- Establish quarterly control-owner committee reporting to Board Risk Committee.
- Independent assurance over the control environment; publish attestation.

11. Conclusion — From Compliance to Competitive Advantage

FAPI 2.0 is the new baseline for open finance. CANDOR engineers the entire surface — authorisation, consent, enforcement, and evidence — to a doctrine regulators can certify and customers can trust.

INSTITUTIONAL DOCTRINE SERIES

**Paper No. 13 of XXI — Financial-Grade API Security
Governed by the Institutional Doctrine Series**

About the Author



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP | MBA | BEng

Mr. Upadrasta has over 27 years' experience in business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. His career spans all four major consulting firms — Deloitte, PwC, EY and KPMG — with 21 years dedicated to financial services and banking. He has worked with the largest global corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI and SAS70.

Professional Memberships, Organisations & Associations

- Professor of Practice in Cybersecurity, AI, and Quantum Computing — Schiphol University
- Honorary Senior Lecturer — Imperials
- Researcher — University College London (UCL)
- Lead Auditor — ISF Auditors and Control
- Platinum Member — Information Systems Audit and Control Association (ISACA), London Chapter
- Gold Member — International Information Systems Security Certification Consortium (ISC)²®, London Chapter
- Cyber Security Programme Lead — Professional Risk Management International Association (PRMIA)

Contact: info@kieranupadrasta.com · www.kie.ie · [linkedin.com/in/kieranupadrasta](https://www.linkedin.com/in/kieranupadrasta)

References

Primary Regulatory Sources

- Regulation (EU) 2022/2554 (DORA), EUR-Lex
- Regulation (EU) 2024/1689 (EU AI Act), EUR-Lex
- Directive (EU) 2022/2555 (NIS2), EUR-Lex
- Regulation (EU) 2024/1183 (eIDAS 2.0 / EUDI Wallet), EUR-Lex
- Bank of England PS6/21 and SS1/21 — Operational Resilience of Important Business Services
- FCA PS21/3 — Building Operational Resilience
- Proposed PSD3 / PSR (COM(2023) 367 / 368 final)
- SEC 17 CFR §229.106 — Cybersecurity Disclosure Rule
- 12 CFR Part 30 App. D — OCC Heightened Standards
- FFIEC Authentication & Access to Financial Institution Services (2021)

Standards and Frameworks

- ISO/IEC 42001:2023 — Artificial Intelligence Management Systems
- ISO/IEC 27001:2022 — Information Security Management Systems
- ISO/IEC 27701:2019 — Privacy Information Management
- NIST AI Risk Management Framework (AI RMF 1.0)
- NIST SP 800-207 — Zero Trust Architecture
- NIST SP 800-63-4 (Public Draft) — Digital Identity Guidelines
- NIST FIPS 140-3 — Cryptographic Module Validation
- NIST FIPS 203 / 204 / 205 — Post-Quantum Cryptography Standards (2024)
- OpenID Financial-grade API (FAPI) 2.0 Security Profile
- OAuth 2.0 PAR (RFC 9126), PKCE (RFC 7636), Token Exchange (RFC 8693), DPoP (RFC 9449)
- SAML 2.0 Core and Profiles (OASIS)
- SCIM 2.0 (RFC 7643 / 7644)
- OWASP ASVS v4.0 and OWASP API Security Top 10
- MITRE ATT&CK and MITRE ATLAS for AI

Industry Research & Technical Documentation

- PingIdentity — PingFederate 12.x Administrative Guide
- PingIdentity — PingOne Protect Risk Engine Whitepaper (2025)
- CISA Zero Trust Maturity Model v2.0
- NCSC Cloud Security Principles and Identity & Authentication Guidance
- ENISA — Threat Landscape for AI (2025)
- Gartner — Access Management Magic Quadrant (2025)
- Forrester — The State of Phishing-Resistant Authentication (2025)
- PRA SS2/21 — Outsourcing and Third-Party Risk Management
- EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04)

- DORA RTS on Threat-Led Penetration Testing (Commission Delegated Regulation)

© 2026 Kieran Upadrasta. All rights reserved. This document is governed by the Institutional Doctrine Series copyright framework.