

TOKEN ISSUANCE AS A SECURITY BOUNDARY

Engineering OAuth2 and OIDC Pipelines for Financial-Grade Systems — A Control-Plane Doctrine for Issued Identity

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 · 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

Treat every issued token as a security boundary. Engineer issuance, exchange, and binding for financial-grade systems — with integrity, provenance, and auditability that satisfies the most exacting regulator.

**Sender-Constrained Every Token | FAPI 2.0 Compliant | 0 Bearer-Only Secrets |
Replayable 7 Years**

The token issuance as a security boundary is no longer a technical choice — it is a board-level governance decision. Treat every issued token as a security boundary. Engineer issuance, exchange, and binding for financial-grade systems — with integrity, provenance, and auditability that satisfies the most exacting regulator.

KEY FINDING — THE AXIOM FRAMEWORK

AXIOM turns token issuance from a functional concern into a security boundary. Sender-constrained tokens, scope minimisation, and cryptographic evidence make bearer-token theft a structurally low-impact attack.

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Token Issuance as a Security Boundary 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 — Engineering the Token Pipeline

Tokens are security boundaries. AXIOM engineers them as such — with integrity, exchange, and minting disciplines worthy of Tier-0 financial systems.

3.1 Authorisation Server Hardening

- Modern OAuth 2.0 profile (RFC 9700) as the baseline.
- PAR endpoint enforced for confidential clients.
- PKCE for all public clients; DPoP-bound for mobile.
- Client registration reviewed by architecture board.

3.2 Token Binding & Sender Constraint

- mTLS-bound access tokens for server-to-server calls.
- DPoP proof-of-possession for mobile and SPA.
- JWT signing keys rotated quarterly.
- Refresh-token rotation with reuse detection.

3.3 Token Exchange Patterns (RFC 8693)

- Delegation with audience narrowing.
- Actor chain preserved in act claim.
- On-behalf-of flows with explicit policy checks.
- Cross-domain exchange through mutually authenticated gateways.

3.4 Observability & Forensics

- Every issuance event signed by HSM and streamed to SIEM.
- Replay harness reconstructs any token issuance.
- Anomaly detection on issuance patterns.
- Board dashboard: issuance rate, rejection rate, scope creep.

4. The AXIOM Framework — Attested · eXchange · Issuance · OAuth · Minted

AXIOM treats every issued token as a security boundary. Each dimension engineers issuance, exchange, and binding for financial-grade systems.

4.1 A — Attested at Source

- Every token carries attested identity and device claims.
- Signing via FIPS 140-3 Level 3 HSM.
- Claim provenance captured at issuance.
- Issuance evidence retained 7 years.

4.2 X — eXchange over Secret Sharing

- Token exchange (RFC 8693) for delegation.
- No bearer secrets crossing service boundaries.
- Downstream systems receive scope-narrowed tokens.
- Exchange events logged and correlated.

4.3 I — Issuance with Integrity

- PAR + PKCE mandatory for confidential clients.
- Sender-constrained tokens via DPOP or mTLS.
- JWT issuance with tight expiration (default 5 min).
- Refresh rotation with reuse detection.

4.4 O — OAuth 2.0 Done Correctly

- Modern profile per RFC 9700 (OAuth 2.0 Security BCP).
- Implicit flow disallowed.
- Client assertions via private_key_jwt.
- JWKS endpoint cached at edge with ETags.

4.5 M — Minted with Meaning

- Every token carries exactly one purpose.
- Scope minimisation enforced at mint.
- Audience restriction is mandatory.
- Consent registered with provenance for customer-facing flows.

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 token issuance as a security boundary.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers token issuance as a security boundary 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 token issuance as a security boundary incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to token issuance as a security boundary.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in token issuance as a security boundary 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 token issuance as a security boundary.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to token issuance as a security boundary.
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to token issuance as a security boundary.

6. Board-Level Governance

The bank's OAuth/OIDC pipeline is a primary attack surface. Bearer-token theft remains one of the most common breach patterns.

6.1 Essential Board Questions

- Are all our access tokens sender-constrained (mTLS or DPoP)?
- Do we enforce PAR and PKCE for all confidential and public clients respectively?
- Is our authorisation server profile aligned to FAPI 2.0 for financial APIs?
- Do we rotate JWT signing keys on a fixed cadence via HSM?
- Can we replay any token issuance event from the last 7 years?
- What is our concentration risk on the authorisation server vendor?

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.
- Bearer tokens in transit are a textbook DORA Art. 9 control failure.

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
Sender-constrained token rate	100% (Tier-1)	FAPI 2.0
p99 issuance latency	< 90 ms	Engineering SLO
Signing key rotation cadence	Quarterly	Crypto policy
Issuance rate observable at board	Yes	Governance
Token TTL (Tier-1)	< 5 min access / < 24 h refresh	Internal SLO

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
Bearer-only tokens in Tier-1 flows	0	FAPI 2.0
Refresh-token reuse detection	100% coverage	OAuth BCP
Implicit flow usage	0	OAuth Security BCP
Client assertion usage	private_key_jwt for all confidential	RFC 7521
Mean time to revoke token	< 60 s	NIST SP 800-207

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
FAPI 2.0 certification	Current	OpenID
RFC 9700 OAuth BCP alignment	100%	IETF
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 2.0 implementation failed the FAPI 2.0 conformance suite; client-credentials secret-shared; no PAR; bearer tokens.

Solution — AXIOM: FAPI 2.0 profile; PAR + PKCE + mTLS; private_key_jwt; JWKS at edge.

Outcome — Passed FAPI 2.0 conformance on first deadline; API fraud reduced 43%; cited as reference in EBA thematic review.

8.2 Sender-constrained tokens for 2,400 internal APIs

SECTOR: Tier-1 Bank — Internal API Estate

Sender-constrained tokens for 2,400 internal APIs

Challenge — Internal APIs used bearer tokens with long TTLs; stolen-token incidents happened quarterly; DORA Art. 9 gap.

Solution — AXIOM: mTLS-bound tokens for server-to-server; DPoP for mobile; rotation policy; observability.

Outcome — Stolen-token incidents eliminated; DORA Art. 9 gap closed; audit evidence produced automatically.

8.3 Token exchange for delegated broker access

SECTOR: Wealth Platform — Customer Journeys

Token exchange for delegated broker access

Challenge — Broker access used shared API keys; regulatory pressure to tighten delegation; audit trail gaps.

Solution — AXIOM: token exchange with audience narrowing; signed attestations; consent registered with provenance.

Outcome — Delegated access governed end-to-end; audit closed; broker turnover workflow automated.

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 token issuance as a security boundary 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 token issuance as a security boundary.
- Inventory bearer-token usage in the target; test for FAPI 2.0 compliance for any financial API.

9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk:** target relies on a single vendor for 90%+ of token issuance as a security boundary. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in token issuance as a security boundary:** 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 token issuance as a security boundary 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 token issuance as a security boundary: systems, vendors, cryptographic dependencies.
- Baseline current KPIs — latency, availability, coverage, exposure.
- DORA Art. 9 gap analysis and regulatory-obligation-to-control map for token issuance as a security boundary.
- Board briefing: impact tolerances, concentration risk, liability framing.

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

- Target topology for token issuance as a security boundary 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 token issuance as a security boundary 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 token issuance as a security boundary 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

Tokens are security boundaries. AXIOM engineers issuance, exchange, and binding for financial-grade systems — with integrity, provenance, and the evidence trail regulators now demand.

INSTITUTIONAL DOCTRINE SERIES

**Paper No. 08 of XXI — Token Issuance as a Security Boundary
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

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)

