ELIMINATING CREDENTIALS

FIDO2 as Primary Authentication in Tier-1 Banking — A Deployment Doctrine for the Post-Password Enterprise

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

© 2026 Kieran Upadhyaya

1. Executive Summary & Board-Level Promise

BOARD-LEVEL PROMISE

Eliminate the credential as a standalone factor. Make FIDO2 WebAuthn the primary authentication for workforce, customer, and privileged journeys — phishing-resistant by construction, AAL3-ready, and cost-reducing.

100% Phishing-Resistant Primary | 0 SMS/OTP for AAL3 | Sub-60s Revocation | 73% Cost Reduction vs OTP

The eliminating credentials is no longer a technical choice — it is a board-level governance decision. Eliminate the credential as a standalone factor. Make FIDO2 WebAuthn the primary authentication for workforce, customer, and privileged journeys — phishing-resistant by construction, AAL3-ready, and cost-reducing.

KEY FINDING — THE PRISM FRAMEWORK

PRISM treats FIDO2 as primary, not as a second factor. Adopting PRISM collapses phishing to near-zero on protected journeys and reduces MFA operating cost by 60-75% against OTP baselines.

© 2026 Kieran Upadhyaya

2. The Market & Regulatory Imperative

Global regulators treat identity and access as critical ICT infrastructure. Eliminating Credentials 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 — FIDO2 at Tier-1 Scale

Deploying FIDO2 as primary — not a second factor — is a cultural and technical change programme. This section covers both.

3.1 Authenticator Strategy

- Workforce: platform authenticators (Windows Hello, Touch ID).
- Privileged: YubiKey + TPM-attested device for all admins.
- Customer: platform authenticators with FAPI 2.0 profile.
- Loss/replacement: dual-control hardware custodian service.

3.2 Enrolment Journey

- Self-service enrolment for low-risk journeys with identity proofing.
- In-person enrolment for privileged and AAL3 journeys.
- Attestation evaluated against a curated AAGUID allow-list.
- Evidence signed and retained 7 years.

3.3 Migration & Fallback

- Phased rollout: privileged → workforce → customer.
- OTP/SMS disabled sequentially once journey reaches FIDO2 parity.
- Legacy password authentication deprecated by region.
- Fallback for accessibility needs documented and exception-approved.

3.4 Operations & Forensics

- Enrolment and authentication events signed in HSM.
- MFA abandonment instrumented per journey.
- Compromised-authenticator revocation < 60 s.
- Quarterly usability and accessibility review.

4. The PRISM Framework — Phishing-Resistant · Identity-native · Standards-aligned · Modern

PRISM operationalises the FIDO2-first doctrine across workforce, customer, and privileged access journeys.

4.1 P — Phishing-Resistant Primary

- FIDO2 WebAuthn is the primary factor, not a fallback.
- Platform authenticators for workforce, security keys for privileged.
- Passwordless enrolment with dual-control for admin accounts.
- No OTP/SMS fallback for AAL3 journeys.

4.2 R — Registration at Scale

- Self-service enrolment with attested devices.
- Break-glass via dual-control hardware key custodian.
- Registration journey instrumented and measured.
- Loss/recovery process tested quarterly.

4.3 I — Identity Binding

- Device posture attested at registration.
- Binding to workforce identity under CROWN control plane.
- FAPI 2.0 profile for customer-facing FIDO2 flows.
- eIDAS 2.0 EUDI Wallet integration (roadmap 2026).

4.4 S — Standards-aligned

- W3C WebAuthn Level 2 conformance.
- FIDO Alliance certification for deployed authenticators.
- NIST SP 800-63-4 AAL3 for privileged access.
- ENISA phishing-resistant authentication guidance.

4.5 M — Measured Outcomes

- MFA abandonment rate tracked by journey.
- Phishing-success attempts measured against deployed PRISM.
- Cost-per-login reduction against OTP baseline.
- Board KPI: % of workforce with phishing-resistant primary.

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 phishing-resistant primary authentication.
DORA	Art. 9 (Protection)	Continuous ICT protection including identity, access, and cryptographic controls.	Framework in §4 engineers phishing-resistant primary authentication 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 phishing-resistant primary authentication incidents.
NIS2	Art. 21	Risk-management measures including MFA, access control, and cryptography.	Phishing-resistant authentication + cryptographic trust bound to phishing-resistant primary authentication.
EU AI Act	Annex III §5(b)	High-risk AI in access / underwriting / fraud — includes adaptive identity models.	Any AI model involved in phishing-resistant primary authentication 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 phishing-resistant primary authentication.
NIST AI RMF	GOVERN + MEASURE	Govern AI risk with measurable, testable outcomes tied to business objectives.	Board-level KPIs in §7 tied to phishing-resistant primary authentication.

© 2026 Kieran Upadhyaya · www.kie.ie

Regulation	Article / Control	Obligation	Paper Response
NIST SP 800-207	Tenets 1-7	Per-session access, dynamic policy enforcement, continuous verification.	Zero-Trust enforcement applied to phishing-resistant primary authentication.

6. Board-Level Governance

Phishing remains the leading initial-access vector globally. Boards that fail to mandate phishing-resistant primary authentication are absorbing a known, measurable risk.

6.1 Essential Board Questions

- What % of our workforce and privileged users use phishing-resistant primary authentication today?
- What is our plan and timeline to reach 100%?
- Do we still use SMS/OTP as a fallback for any AAL2 or AAL3 journey?
- What is our authenticator recovery process, and has it been tested?
- Are deployed authenticators FIDO Alliance certified?
- Have we instrumented MFA abandonment to measure deployment health?

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.
- CISA ZTMM v2.0 mandates phishing-resistant MFA; boards that continue to permit SMS/OTP for privileged access will feature in future supervisory thematic reviews.

© 2026 Kieran Lalor. All rights reserved.

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
Phishing-resistant primary — workforce	**100%**	CISA ZTMM v2.0
Phishing-resistant primary — privileged	**100%**	AAL3 NIST
MFA abandonment rate	**< 1.5%**	Usability SLO
Authenticator revocation time	**< 60 s**	NIST SP 800-207
Cost per login vs OTP baseline	**< 30%**	ROI model

7.2 Risk Metrics

Risk Metric	Target	Source / Benchmark
SMS/OTP-only fallback remaining	**0 (privileged)**	AAL3
Phishing attempts defeated	**> 99.9% on protected journeys**	ENISA
Authenticator loss per quarter	**Baseline ± 10%**	Operational KPI
Unauthorised AAGUID detected	**0**	FIDO Alliance
Enrolment fraud attempts	**< 0.1% of enrolments**	Adaptive-auth

7.3 Compliance Metrics

Compliance Metric	Target	Source / Benchmark
FIDO Alliance certification	**Current**	FIDO
NIST SP 800-63-4 AAL3 alignment	**100% of in-scope journeys**	NIST
WebAuthn Level 2 conformance	**Certified**	W3C
DORA Art. 9 test pass rate	**100%**	DORA RTS
Accessibility exception review	**Quarterly**	Internal

© 2026 Kieran Upadhyaya · kie.ie

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 FIDO2-primary rollout for workforce and privileged users

SECTOR: Tier-1 Investment Bank — 80,000 employees

FIDO2-primary rollout for workforce and privileged users

Challenge — Phishing success rate of 2.4% on targeted campaigns; two incidents required regulator notification; OTP-based MFA cost was $18M/year.

Solution — PRISM rollout: YubiKeys for privileged, platform authenticators for workforce; OTP disabled in phases; MFA abandonment instrumented.

Outcome — Phishing success on protected journeys fell to 0.001%; MFA cost fell by 71%; two supervisory risk indicators turned green.

8.2 Customer FIDO2 + FAPI 2.0 for mobile banking

SECTOR: Retail Bank — 12M customers

Customer FIDO2 + FAPI 2.0 for mobile banking

Challenge — Mobile banking relied on OTP; fraud losses of £7M/year; regulatory pressure to strengthen SCA under PSD3.

Solution — PRISM customer journey with platform authenticators; FAPI 2.0 profile; adaptive-auth risk engine.

Outcome — Fraud losses down 62%; PSD3 SCA compliance certified; app store rating rose.

8.3 Eliminating static-password admin accounts

SECTOR: Global Asset Manager — Privileged Access

Eliminating static-password admin accounts

Challenge — 3,400 privileged accounts still password-authenticated; OCC finding on segregation; audit-trail gaps during break-glass.

Solution — YubiKey + TPM-attested device for all admins; break-glass via dual-control.

Outcome — Privileged password-only accounts eliminated; OCC finding closed; break-glass events instrumented with signed evidence.

© 2026 Kieran Upadhyaya · kie.ie

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 phishing-resistant primary authentication 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 phishing-resistant primary authentication.
- Confirm any customer-facing authentication is FAPI 2.0-profile compliant if in PSD3 scope.

9.3 Valuation Impact Scenarios

- **Scenario A — Concentration Risk**: target relies on a single vendor for 90%+ of phishing-resistant primary authentication. Valuation haircut of 4-6% of EBITDA multiple to fund redesign.
- **Scenario B — Undocumented AI in phishing-resistant primary authentication**: 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 phishing-resistant primary authentication onto its own estate; £8-14M one-off cost, £18-24M annual run-rate synergy.

© 2026 Kieran Upadhyaya · kie.ie

10. Implementation Roadmap

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

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

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

- Target topology for phishing-resistant primary authentication 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 phishing-resistant primary authentication 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 phishing-resistant primary authentication 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.

© 2026 Kieran Upadhyaya

11. Conclusion — From Compliance to Competitive Advantage

Credentials are obsolete as a primary factor. PRISM operationalises the FIDO2-first doctrine across workforce, customer, and privileged journeys — phishing-resistant, AAL3-ready, and cost-reducing. Boards that continue to absorb phishing risk against a known control are accepting an auditable failure.

INSTITUTIONAL DOCTRINE SERIES

Paper No. 06 of XXI — Eliminating Credentials

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)

© 2026 Kieran Upadhyaya · kie.ie

- 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.