POSTRSA ADVISORY | DEGAUS LTD

DOC ID: ADV-20261129-864245
GENERATED: 2026-11-29T00:01:51Z
DATASET: v2026.11.29-aa9ea8fb
SHA-256: aa9ea8fbfe7fcb6f...
SCENARIO: NONE · NO CONFIRMED BREAK

Meridian Clearing Ltd (Sample)

POST-RSA EXPOSURE & REMEDIATION BOARD BRIEF

VENDORS ASSESSED	HYBRID PQ KEX	RSA AUTH / SIGNING	BLOCKED (SCEN. B)
6	**2 / 6**	**4 / 6**	**3**
6 reviewed / 0 slots	TLS 1.3 ML-KEM documented	TLS, JWT/SAML, DKIM or KMS	Public Web PKI / upstream

1. Executive Posture & Post-RSA Readiness Priorities

This point-in-time executive brief summarizes the documented asymmetric cryptography posture of **6 selected third-party providers** used by **Meridian Clearing Ltd (Sample)** as of **2026-11-29T00:01:51Z**. No primary source (NIST, NCSC, CISA, IACR or arXiv) has confirmed a practical break of RSA or elliptic-curve cryptography; this is a preparedness brief describing what would change if one were confirmed. This brief separates **traffic confidentiality (key exchange)** from **identity & authentication (certificates, tokens, signing keys)** across two clear migration horizons:

Horizon 1 — Immediate RSA Removal (Scenario A):
Every RSA TLS certificate/CA chain, RSA JWT/SAML assertion (`RS256`, XML-DSig), RSA SSH key, RSA DKIM key, and RSA KMS key should be inventoried now with a rotation plan ready, so it could be rotated quickly if RSA factoring were confirmed. Classical ECC would contain an RSA-only break but is not post-quantum.

Horizon 2 — Full Post-Quantum Migration (Scenario B):
Transitions both RSA and classical ECC (`ECDSA`, `Ed25519`, `X25519`) to NIST-standardized post-quantum algorithms. Hybrid TLS key exchange (`X25519MLKEM768`, RFC 10024) protects transport confidentiality today, while public Web PKI authentication tracks browser/CA ML-DSA rollout.

Regulatory & Governance Alignment: Structured cryptographic inventories and documented vendor remediation plans align directly with **PCI DSS v4.0.1 Req. 12.3.3**, **EU DORA RTS (EU) 2024/1774 Arts. 6–7**, **NIST IR 8547 Final (27 Oct 2026)**, and the **Bank of England / PRA / FCA Effective Practices on Quantum Resilience (19 Nov 2026)**.

Signal Legend (4-Channel Encoding — Legible in Color & Monochrome Print)

[PQ]	NIST-standardized PQ or hybrid PQ documented (`X25519MLKEM768`, `ML-DSA`, `SLH-DSA`, `ML-KEM`).	[ECC]	Classical ECC (`ECDSA`, `Ed25519`, `X25519`) or symmetric HMAC. Resilient to Scenario A; exposed in Scenario B.
[RSA]	Classical RSA (`RSA-2048/4096`, `RS256`, RSA CA/DKIM/SAML). Exposed under Scenarios A and B.	[UNK]	Undisclosed in public docs, unreviewed catalogue slot, not applicable, or ecosystem-blocked.

2. Action Ownership Split: Customer-Controllable vs. Upstream Dependencies

CUSTOMER-CONTROLLABLE ACTIONS (EXECUTE NOW)	UPSTREAM VENDOR / ECOSYSTEM DEPENDENCIES (TRACK)
• **JWT & Application Auth:** Plan the move of internal token issuers/verifiers off `RS256`: `ES256`/`EdDSA` would contain an RSA-only break; RFC 9964 (`ML-DSA-65`, `kty: "AKP"`) is the post-quantum destination for controlled service-to-service paths. • **Cloud KMS / Vault Keys:** Inventory asymmetric RSA keys in AWS KMS, GCP KMS, Azure Key Vault, and Vault Transit; test FIPS 204 `ML-DSA` / FIPS 203 `ML-KEM` where supported without silently downgrading HSM custody requirements. • **TLS Origin & Edge Policies:** Enable TLS 1.3 hybrid PQ key exchange (`X25519MLKEM768`) on Cloudflare, AWS ALB/CloudFront, Azure Front Door, and Vercel; inventory certificate chains for RSA leaves, intermediates and cross-signs. • **SSH & Git Operations:** Inventory RSA host keys, user keys and commit-signing keys; `Ed25519` would be RSA-only containment, and `mlkem768x25519-sha256` key exchange protects sessions today.	• **Public Web PKI Authentication:** Browser-trusted `ML-DSA` TLS certificates depend on CA/Browser Forum standards, root-store programs, and public CA rollout (ecosystem-blocked for Scenario B). • **Enterprise SAML 2.0 & OIDC IdPs:** Okta, Auth0, Entra ID, and SaaS SAML relying parties predominantly sign assertions with `RSA-SHA256`; monitor vendor release notes for ECC and RFC 9964 support. • **Email DKIM Ecosystem:** Transactional mail providers (Postmark, SendGrid) rely on RSA DKIM keys; dual-signing with Ed25519 (RFC 8463) does not remove RSA exposure while mail receivers accept RSA. • **Vendor Internal HSMs & Closed Clients:** SaaS vault key-wrapping and internal service HSM custody cannot be modified directly by customers; request formal PQC roadmaps at renewal.

3. Selected Vendor Cryptographic Surface Matrix (6 Vendors)

Each vendor is assessed independently across five cryptographic surfaces. Key exchange (confidentiality) is never collapsed into authentication (integrity). Footnote indices [N] reference verbatim primary documentation in Section 4.

VENDOR / CAT	TLS EDGE KEX	TLS AUTH / CHAIN	APP AUTH (JWT/ SAML)	KMS / HSM	SSH / GIT	REF
Cloudflare cloudflare.com CDN & Edge VERIF 2026-11-27	[PQ] X25519MLKEM768 documented / default	[UNK] ECDSA / RSA chains unverified / mixed	[UNK] Access JWT signing unverified unverified / not-disclosed	[UNK] Keyless SSL / Edge unverified / not-applicable	[UNK] Access SSH proxy unverified / not-applicable	[1] [2]
AWS aws.amazon.com Cloud & Compute VERIF 2026-11-27	[PQ] X25519MLKEM768 documented / opt-in	[UNK] ACM ECDSA / RSA unverified / configurable	[RSA] Cognito RS256 documented / default	[PQ] ML-DSA & ML-KEM documented / opt-in	[ECC] EC2/CodeCommit Ed25519 documented / configurable	[3] [4]
Stripe stripe.com Payments & Fintech VERIF 2026-11-29	[UNK] TLS 1.2+ documented unverified / not-disclosed	[RSA] api.stripe.com RSA-2048 leaf observed / mixed	[PQ] Symmetric HMAC-SHA256 webhooks documented / symmetric	[UNK] Internal HSM Custody unverified / not-disclosed	[UNK] Not applicable unverified / not-applicable	[5] [6]
GitHub github.com Code & CI/CD VERIF 2026-11-29	[UNK] TLS 1.2/1.3 edge unverified / not-disclosed	[UNK] Public Web PKI TLS unverified / default	[RSA] GitHub Actions OIDC RS256 observed / default	[UNK] Internal Secret Store unverified / default	[ECC] Ed25519/ECDSA/ RSA documented / configurable	[7] [8]
Okta okta.com Identity & Auth VERIF 2026-11-29	[UNK] TLS 1.2/1.3 edge unverified / not-disclosed	[RSA] login.okta.com RSA-2048 leaf observed / default	[RSA] RS256 OIDC & SAML documented / default	[UNK] Tenant Signing Keys unverified / not-disclosed	[UNK] ASA / PAM separate unverified / not-applicable	[9] [10]
Let's Encrypt letsencrypt.org Security & PKI VERIF 2026-11-27	[UNK] CA / ACME Service unverified / not-applicable	[UNK] ECDSA X2 & RSA X1 unverified / configurable	[ECC] ACME JWS (ECDSA/ RSA) documented / configurable	[ECC] Offline Root HSMs documented / default	[UNK] Not applicable unverified / not-applicable	[11]

4. Primary-Source Citations & Explicit Limitations Appendix

[1] **Cloudflare — Cloudflare Post-Quantum Cryptography Documentation** Retrieved 2026-11-27T15:00:00Z
"Cloudflare has deployed support for ML-KEM, the post-quantum key agreement selected by the US National Institute of Standards and Technology (NIST)... Cloudflare has deployed support for ML-DSA, the post-quantum digital signature algorithm selected by NIST (FIPS 204)."
https://developers.cloudflare.com/ssl/post-quantum-cryptography/

[2] **Cloudflare — Cloudflare PQC to Origin Guide** Retrieved 2026-11-27T15:00:00Z
"Automatic origin key exchange is enabled for zones; ML-DSA support applies to Authenticated Origin Pulls and Custom Origin Trust Store with compatible origin TLS."
https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-to-origin/

[3] **AWS — AWS KMS Asymmetric Key Specs (ML-DSA and ML-KEM)** Retrieved 2026-11-27T15:00:00Z
"AWS KMS supports ML-DSA KMS keys and ML-KEM KMS keys (a KMS key with an ML-KEM key pair for encapsulating and decapsulating shared secrets), alongside RSA and ECC key specs."
https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

[4] **AWS — AWS Certificate Manager — Certificate Characteristics** Retrieved 2026-11-27T15:00:00Z
"ACM supports requested RSA-2048 and ECDSA P-256/P-384 certificates with managed renewal and deployment subject to service compatibility."
https://docs.aws.amazon.com/acm/latest/userguide/acm-certificate-characteristics.html

[5] **Stripe — Stripe Security Documentation** Retrieved 2026-11-27T15:00:00Z
"Stripe requires use of at least TLS 1.2 on external requests. All Stripe internal server-to-server communication is encrypted using mutual transport layer security (mTLS)."
https://docs.stripe.com/security

PREVIEW — WA

[6] **Stripe — Stripe Webhook Signatures** Retrieved 2026-11-27T15:00:00Z
"Stripe signs webhook events using a hash-based message authentication code (HMAC) with SHA-256 via the Stripe-Signature header."
https://docs.stripe.com/webhooks/signature

[7] **GitHub — GitHub SSH Key Fingerprints** Retrieved 2026-11-27T15:00:00Z
"GitHub publishes SHA256 host key fingerprints for ECDSA, Ed25519, and RSA (with DSA retired) for ~/.ssh/known_hosts verification."
https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/githubs-ssh-key-fingerprints

[8] **GitHub — GitHub — About SSH** Retrieved 2026-11-27T15:00:00Z
"SSH connections to GitHub support Ed25519, ECDSA, and RSA user authentication keys as well as SSH commit signature verification."
https://docs.github.com/en/authentication/connecting-to-github-with-ssh/about-ssh

[9] **Okta — Okta OAuth 2.0 and OpenID Connect Overview** Retrieved 2026-11-27T15:00:00Z
"Okta implements OAuth 2.0, OpenID Connect, and OAuth 2.0 SAML 2.0 Assertion flows with asymmetric JWT/JWKS token verification."
https://developer.okta.com/docs/concepts/oauth-openid/

[10] **Okta — Okta OpenID Connect & OAuth 2.0 API Reference** Retrieved 2026-11-27T15:00:00Z
"Okta authorization servers publish public signing keys via the /keys JWKS endpoint for asymmetric RS256 signature verification."
https://developer.okta.com/docs/reference/api/oidc/

[11] **Let's Encrypt — Let's Encrypt Chains of Trust** Retrieved 2026-11-27T15:00:00Z
"ISRG Root X2: Key type ECDSA P-384, trusted until 2035-09-04. ISRG Root X1: Key type RSA 4096, trusted until 2030-06-04. ECDSA and RSA intermediates and alternate chains are published."
https://letsencrypt.org/certificates/

EVIDENCE BOUNDARY, NON-RELIANCE & NON-CERTIFICATION NOTICE

Basis: Point-in-time factual summary compiled solely from cited public vendor documentation recorded in PostRSA Status snapshot v2026.11.29-aa9ea8fb (dataset SHA-256 aa9ea8fbfe7fcb6f69d77bc300fc926d29d74a079472f15519af30c1d78d9c73). Unreviewed slots represent scheduled catalogue placeholders and are not adverse findings.
Non-Certification & Non-NCSC Notice: This advisory is an engineering planning indicator only. It is **not** legal, regulatory, or compliance advice; **not** a security audit, penetration test, or cryptographic validation; and **does not** constitute UK NCSC Assured Cyber Security Consultancy (ACSC), FCA, PRA, PCI QSA, or FIPS 140 certification or endorsement. Note that NIST FN-DSA (future FIPS 206) is not claimed finalized.
Third-Party Reliance Excluded: Provided "as is" by Degaus Ltd (England and Wales) for internal planning by Meridian Clearing Ltd (Sample). Primary-source corrections with an official documentation URL may be submitted to corrections@postrsa.com.

PREVIEW WATERMARKED