REF AGY-20261129-64681B
WEB northbridge.example
MAIL advisory@northbridge.example
UTC 2026-11-29T15:02:57Z

Post-RSA exposure across your client portfolio

Prepared by **Northbridge Managed IT Ltd** for the 6 organisations under management, as at 29 November 2026.

CLIENTS ASSESSED	HIGH EXPOSURE	PARTIAL	PROTECTED
6	3	3	0
domains in this brief	score below 40 · act this week	score 40 to 74 · bounded rotation	score 75 and above · evidence

3 of 6 clients sit in the high-exposure band and should get a rotation plan first; 3 have bounded rotation work; 0 are protected and need evidence rather than engineering. The table below ranks every client by exposure so the first call of the morning is obvious.

Method: each client's named providers are scored from their public cryptographic documentation across four surfaces. The badges show the weakest provider on each surface; the score averages the whole stack. The score is a planning indicator for Northbridge Managed IT Ltd and its clients, not a scan or audit of client systems.

01 Portfolio table — every client, one line, sorted by exposure

#	CLIENT	DOMAIN	SCORE	BAND	KEX	CHAIN	AUTH	KMS	FIRST ACTION
1	SAMPLE — Fenwick & Co Solicitors	fenwick-law.example	25	HIGH	UNK	RSA	RSA	RSA	Plan token signing off RSA
2	SAMPLE — Harrow Dental Group	harrowdental.example	25	HIGH	UNK	RSA	RSA	RSA	Plan token signing off RSA
3	SAMPLE — Castleford Engineering	castleford-eng.example	28	HIGH	UNK	RSA	RSA	RSA	Plan token signing off RSA
4	SAMPLE — Marlow Boutique Hotels	marlowhotels.example	40	PARTIAL	UNK	RSA	RSA	UNK	Plan token signing off RSA
5	SAMPLE — Oakridge Primary Academy	oakridge-academy.example	40	PARTIAL	UNK	RSA	RSA	UNK	Plan token signing off RSA
6	SAMPLE — Bramble Logistics	bramblelogistics.example	51	PARTIAL	UNK	RSA	RSA	UNK	Plan token signing off RSA

Score is a 0 to 100 readiness indicator derived from the documented posture of each client's named providers across four surfaces: TLS key exchange (KEX), certificate chain (CHAIN), application authentication (AUTH) and key management (KMS). PQ: post-quantum or hybrid documented. ECC: classical elliptic curve, survives RSA failure but not quantum. RSA: exposed now. UNK: undocumented or not applicable. The score reflects public provider documentation at the snapshot date and is not a scan of the client's own systems.

What to tell each client, and what to sell them next

Each sheet is written to be lifted straight into a client meeting. The executive summary is plain English for the client's leadership; the next steps are the remediation work Northbridge Managed IT Ltd can deliver and invoice.

CLIENT 1 OF 6

SAMPLE — Fenwick & Co Solicitors

fenwick-law.example

Legal · providers: Microsoft Azure, Atlassian, 1Password

25

HIGH EXPOSURE

UNK RSA RSA RSA

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Fenwick & Co Solicitors is in the high-exposure band. At least one provider the business depends on still uses RSA where customers, staff or auditors can see it. No practical RSA break has been confirmed; if one were, RSA-signed tokens, certificates or keys in this environment would be treated as untrusted until they were rotated. No breach is implied; the point is to have the rotation plan ready before it is needed.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- Microsoft Azure: RSA in certificate chain, token or SAML signing, key management.
- Atlassian: RSA in certificate chain, token or SAML signing.
- 1Password: RSA in token or SAML signing.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Inventory and re-wrap RSA keys in the cloud KMS or vault; schedule deletion dates for the residue.
4. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
5. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.

CLIENT 2 OF 6

SAMPLE — Harrow Dental Group

harrowdental.example

Healthcare · providers: Microsoft Azure, Okta, SendGrid

25

HIGH EXPOSURE

UNK RSA RSA RSA

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Harrow Dental Group is in the high-exposure band. At least one provider the business depends on still uses RSA where customers, staff or auditors can see it. No practical RSA break has been confirmed; if one were, RSA-signed tokens, certificates or keys in this environment would be treated as untrusted until they were rotated. No breach is implied; the point is to have the rotation plan ready before it is needed.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- Microsoft Azure: RSA in certificate chain, token or SAML signing, key management.
- Okta: RSA in certificate chain, token or SAML signing.
- SendGrid: RSA in certificate chain.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Inventory and re-wrap RSA keys in the cloud KMS or vault; schedule deletion dates for the residue.
4. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
5. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.

CLIENT 3 OF 6

SAMPLE — Castleford Engineering castleford-eng.example

Manufacturing · providers: Microsoft Azure, GitHub, Datadog

28 HIGH EXPOSURE

UNK RSA RSA RSA

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Castleford Engineering is in the high-exposure band. At least one provider the business depends on still uses RSA where customers, staff or auditors can see it. No practical RSA break has been confirmed; if one were, RSA-signed tokens, certificates or keys in this environment would be treated as untrusted until they were rotated. No breach is implied; the point is to have the rotation plan ready before it is needed.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- Microsoft Azure: RSA in certificate chain, token or SAML signing, key management.
- GitHub: RSA in token or SAML signing.
- Datadog: RSA in certificate chain.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Inventory and re-wrap RSA keys in the cloud KMS or vault; schedule deletion dates for the residue.
4. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
5. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.

CLIENT 4 OF 6

SAMPLE — Marlow Boutique Hotels marlowhotels.example

Hospitality · providers: Stripe, SendGrid, Vercel

40 PARTIAL

UNK RSA RSA UNK

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Marlow Boutique Hotels is in the partial band. Traffic is largely protected by modern TLS, but RSA cryptography still signs or wraps something customers can reach. The work is bounded and well understood: inventory, plan the rotation, and collect evidence. This is the right moment to fix it before a customer or insurer asks.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- Stripe: RSA in certificate chain.
- SendGrid: RSA in certificate chain.
- Vercel: RSA in token or SAML signing.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.
- key management: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
4. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.
5. Issue supplier migration-date requests to every provider on SAMPLE — Marlow Boutique Hotels's behalf and track responses at renewal.

CLIENT 5 OF 6

SAMPLE — Oakridge Primary Academy

oakridge-academy.example

Education · providers: Google Cloud, Slack

40

PARTIAL

UNK RSA RSA UNK

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Oakridge Primary Academy is in the partial band. Traffic is largely protected by modern TLS, but RSA cryptography still signs or wraps something customers can reach. The work is bounded and well understood: inventory, plan the rotation, and collect evidence. This is the right moment to fix it before a customer or insurer asks.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- Google Cloud: RSA in token or SAML signing.
- Slack: RSA in certificate chain, token or SAML signing.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.
- key management: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
4. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.
5. Issue supplier migration-date requests to every provider on SAMPLE — Oakridge Primary Academy's behalf and track responses at renewal.

CLIENT 6 OF 6

SAMPLE — Bramble Logistics

bramblelogistics.example

Logistics · providers: AWS, Cloudflare, Stripe, Twilio

51

PARTIAL

UNK RSA RSA UNK

EXECUTIVE SUMMARY FOR THE CLIENT

SAMPLE — Bramble Logistics is in the partial band. Traffic is largely protected by modern TLS, but RSA cryptography still signs or wraps something customers can reach. The work is bounded and well understood: inventory, plan the rotation, and collect evidence. This is the right moment to fix it before a customer or insurer asks.

WHERE RSA STILL SITS, OR IS UNDOCUMENTED

- AWS: RSA in token or SAML signing.
- Stripe: RSA in certificate chain.
- Twilio: RSA in certificate chain.
- TLS key exchange: not documented by at least one provider; treat as RSA until confirmed.
- key management: not documented by at least one provider; treat as RSA until confirmed.

RECOMMENDED NEXT STEPS · NORTHBRIDGE MANAGED IT LTD

1. Plan the move of application and single sign-on token signing off RS256: ES256 or EdDSA would contain an RSA-only break, and ML-DSA-65 (RFC 9964) is the post-quantum destination where the client controls issuer and verifier.
2. Inventory internal and customer-facing TLS certificates on RSA chains and prepare a re-issue plan, including RSA cross-signs.
3. Enable TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) at the edge and confirm origin-side TLS 1.3.
4. Run a cryptographic inventory workshop with the client's team and deliver a dated register of every certificate, token key and SSH key.
5. Issue supplier migration-date requests to every provider on SAMPLE — Bramble Logistics's behalf and track responses at renewal.

BASIS AND LIMITS

This brief was prepared by Northbridge Managed IT Ltd from public provider documentation as at 29 November 2026 for planning and client advisory use. It is not legal, regulatory or compliance advice, not a security audit, and not a certification. Scores reflect documented provider posture, not the configuration of each client's own systems, which should be verified before remediation is scoped. Clients should seek qualified counsel on any notification duty.