Encryption: who can decrypt your data, and what must you start for post-quantum?

Automate renewal of every public TLS certificate before the maximum lifetime drops to 100 days on 15 March 2027[1], and inventory your cryptography this quarter so data that must stay secret for ten years or more gets hybrid post-quantum key exchange first. Then judge each measure by who can use the key, and whether you could still decrypt if it were deleted.

Reviewed **4 Nov 2026** | Next review **4 Dec 2026** | Version **1.0**

Written for
IT, security and platform teams in EU organizations that run TLS, certificates, disk and database encryption, cloud key management and secrets

Latest version
sheets.einblick.dev/encryption/

If you only do five things

1. **Automate certificate renewal by March 2027.** Public TLS certificates issued from 15 March 2027 may last at most 100 days[1]. Renew with ACME and let ACME Renewal Information (ARI) set the timing, not a fixed interval[2]. Alert a week before any expiry.
2. **Inventory your cryptography.** List TLS endpoints, certificates, keys and who holds them, algorithms and trust stores. The EU roadmap calls this a no-regret first step that needn't be complete before you set priorities[9].
3. **Turn on hybrid post-quantum key exchange.** Recorded traffic can be decrypted once a large quantum computer exists, so BSI recommends hybrid key agreement for long-term secrets[5] and accepts `X25519MLKEM768` in TLS 1.3[7]. Chrome, Firefox and Apple's version 26 systems offer it[11,12,13].
4. **Separate who manages keys from who uses them.** AWS KMS key administrators can't use a key but can rewrite its policy to grant themselves access[19]. Activate key admin roles just in time, with approval[17].
5. **Get secrets out of code and into a vault.** Give apps managed identities, not stored credentials, and one vault per app and environment[17]. Rotate any exposed secret at once. For CI tokens, see the supply-chain sheet.

Build a first cryptographic inventory

1. **Which data must stay secret for ten years or more?** The EU roadmap counts it as high-risk and wants it protected from quantum attacks by the end of 2030[8]. Think of health and HR records, contracts, designs and their backups.
2. **Where does it travel and where is it stored?** Follow it through load balancers, VPNs, SSH, APIs, databases and backups, including systems your managed service providers run.
3. **What protects it, and who holds the key?** Record the protocol and key exchange, the certificate and issuer, where the key lives (HSM, cloud KMS or a file) and who can use it. AWS load balancer connection logs record the negotiated key exchange[16].
4. **Which trust stores do your systems rely on?** List the CA bundle in each runtime, container image and appliance, and how each one gets updated. For Python, see the secure-python sheet.
5. **What can't be upgraded?** Ask suppliers when they will support ML-KEM. BSI strongly recommends that products expected to run beyond 2030 can be upgraded to quantum-safe methods[5].

TLS baseline

- **Offer TLS 1.3 and 1.2 only.** BSI prefers TLS 1.3, recommends TLS 1.2 only until the end of 2031 and doesn't recommend TLS 1.0 or 1.1[6].
- **Put hybrid groups first.** List `X25519MLKEM768` ahead of `X25519`, as OpenSSL 3.5 does by default[14]. Recent Windows 11 and Server 2025 builds support it in Schannel but leave it off; enable it with the ECC Curve Order group policy[15]. On AWS load balancers, pick `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09`[16].
- **Meet BSI key lengths.** Prefer ECDSA P-256 keys. BSI wants RSA keys of at least 3000 bits, so the usual RSA 2048 falls short[6].

Who holds the keys

- **Encryption at rest stops disk thieves, not logins.** It protects against someone with the hardware but not the key[18]. S3 decrypts for any authenticated request with permission[23].
- **Platform-managed keys suit most data,** Microsoft says[18]. Choose customer-managed keys for specific regulatory or security needs; their availability becomes your job.
- **Make deletion slow and keep backups.** Turn on Key Vault soft delete and purge protection, back up keys that can't be recreated and test the restore[17].

What changed in 2026

- **A certificate authority lost its keys.** In October 2026 eight eMudhra intermediate CA keys proved recoverable. Mozilla dropped trust in eMudhra's emSign ECC Root CA - G3 and Chrome committed to do the same[4]. Update the trust store in every runtime and image, and keep a second ACME CA ready.
- **Public certificates are becoming server-only.** Chrome requires public certificates issued from 15 March 2027 to be for server authentication only[3]. Move mutual TLS to a private CA.
- **BSI and NIST set end dates for classical cryptography** in TR-02102 2026-01 and the final IR 8547 (dates below)[5,10].

Dates that set your schedule

Public TLS certificates

Maximum lifetime and domain validation reuse, binding on every public CA[1].

15 Mar 2026
200 days; reuse 200 days

15 Mar 2027
100 days; reuse 100 days

15 Mar 2029
47 days; reuse 10 days

Post-quantum migration

EU roadmap milestones[8], with BSI and NIST dates.

End 2026
Plans and pilots started[8]

End 2030
High-risk uses migrated[8,5]

End 2031
BSI: TLS 1.2 and classical-only key exchange end[5,6]

End 2035
Medium-risk migrated[8]; NIST bars RSA and ECC[10]

What you can skip

- **Re-keying everything to AES-256 for quantum.** NIST believes approved symmetric algorithms with at least 128-bit security meet its lowest post-quantum security category[10]. Use AES-256 for new long-term secrets, as BSI advises[5].
- **Post-quantum TLS certificates now.** Classical signatures stay trustworthy until a quantum computer exists, and BSI recommends them until the end of 2035[5]. Firmware signing can't wait that long[8].
- **Cloud keys in an external key store.** AWS says their availability and latency risks exceed the perceived benefit for most customers[22].
- **Rotating KMS keys more than yearly.** Wrapping keys are almost never used enough to wear out[21].

Mistakes that cost the most

- **Deleting a key something still uses.** A deleted AWS KMS key leaves its data unrecoverable. Disable it first and alarm on use during the 7 to 30 day waiting period[20].
- **Trusting infrastructure-as-code defaults.** AWS load balancer listeners created from the CLI, CloudFormation or CDK without a named policy get `ELBSecurityPolicy-2016-08`, which allows TLS 1.0 and 1.1[16].
- **Turning off post-quantum key exchange for a middlebox.** Firefox warns this removes protection against later decryption of recorded traffic[12], and Chrome's policy to do so ended with version 146[11]. Fix the middlebox.

What this looks like at your size

Small team, no security staff

- Use your host's or CDN's managed certificates, or an ACME client with ARI, and turn on expiry alerts.
- Keep the cloud's default encryption, and keep passwords and API keys in a vault, not in code.
- Ask your IT provider and SaaS vendors when they will support hybrid post-quantum TLS.

Growing, with IT or security staff

- Build the inventory from load balancer logs, certificate transparency and config scans; give every certificate and key an owner.
- Enable hybrid ML-KEM on internet-facing TLS and SSH, and watch logs for clients that fall back.
- Run a private CA for client certificates and put key admin roles behind just-in-time access.

Enterprise or regulated

- Write the cryptography policy NIS2 requires. For cloud and other digital providers, Regulation 2024/2690 sets its content, from algorithms to key destruction[24].
- Keep the inventory in a standard format such as CBOM[8] and report quantum risk to the board.
- Start with the PKI, the slowest to migrate, and put PQC support into supplier contracts.

Version history

4 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which fixed the AWS policy name and narrowed 10 statements to what the sources say.

Sources

1. Baseline Requirements, v2.3.1. CA/Browser Forum, 4 Oct 2026. cabforum.org
2. Decreasing Certificate Lifetimes to 45 Days. Let's Encrypt, 2 Dec 2025. letsencrypt.org
3. Chrome Root Program Policy, v1.8. Google, 5 Feb 2026. googlechrome.github.io
4. Bug 2083449: eMudhra: Private key compromise of Intermediate Certificates. Mozilla, opened 18 Oct 2026. bugzilla.mozilla.org
5. TR-02102-1, version 2026-01. BSI, 23 Jan 2026. bsi.bund.de
6. TR-02102-2 (TLS), version 2026-01. BSI, 27 Jan 2026. bsi.bund.de
7. TR-02102 page, note on TLS 1.3. BSI, checked 4 Nov 2026. bsi.bund.de
8. Coordinated Implementation Roadmap for the Transition to PQC. NIS Cooperation Group, 23 Jun 2025. digital-strategy.ec.europa.eu
9. EU Roadmap on PQC: FAQ. NIS Cooperation Group, 15 Apr 2026. ec.europa.eu
10. IR 8547: Transition to PQC Standards. NIST, Oct 2026. csrc.nist.gov
11. Chrome Enterprise policy list: PostQuantumKeyAgreementEnabled. Google, checked 4 Nov 2026. chromeenterprise.google
12. PostQuantumKeyAgreementEnabled. Mozilla, updated 4 Nov 2026. firefox-admin-docs.mozilla.org
13. Prepare your network for quantum-secure encryption in TLS. Apple, 18 Jun 2026. support.apple.com
14. OpenSSL 3.5 release notes. OpenSSL, 8 Apr 2025. openssl-library.org
15. TLS Supported Groups in Windows. Microsoft Learn, 20 May 2026. learn.microsoft.com
16. Security policies for your Application Load Balancer. AWS, checked 4 Nov 2026. docs.aws.amazon.com
17. Secure your Azure Key Vault. Microsoft Learn, 10 Jul 2026. learn.microsoft.com
18. Azure data encryption at rest. Microsoft Learn, 8 Jul 2026. learn.microsoft.com
19. Default key policy. AWS, checked 4 Nov 2026. docs.aws.amazon.com
20. Delete an AWS KMS key. AWS, checked 4 Nov 2026. docs.aws.amazon.com
21. Rotate AWS KMS keys. AWS, checked 4 Nov 2026. docs.aws.amazon.com
22. External key stores. AWS, checked 4 Nov 2026. docs.aws.amazon.com
23. Protecting data with server-side encryption. AWS, checked 4 Nov 2026. docs.aws.amazon.com
24. NIS2 technical implementation guidance, v1.0. ENISA, 26 Jun 2025. enisa.europa.eu